SafeScrypt CA

CERTIFICATION PRACTICE STATEMENT

VERSION 3.0

Date of Publication: 26/12/2016

sify safescrypt

Sify Technologies Ltd

2nd Floor, Tidel Park, No. 4, Rajiv Gandhi Salai,
Taramani, Chennai -600113, Tamil Nadu, India.
Tel: +91-44-2254 0770, Fax: +91-44-2254 0771
Email: enquires@sifycorp.com
Website: www.safescrypt.com

SafeScrypt CA Certification Practice Statement

This Certification Practice Statement describes the practices followed by SafeScrypt CA for managing Digital Signature Certificates and related services as per the requirement of The Information Technology Act, 2000

IMPORTANT NOTE:

This CPS (as amended from time to time) is intended to be an all-encompassing CPS that covers all the hierarchy components, classes, certificate types etc. However, not all services and products may be commercially available at all points in time. SafeScrypt CA reserves the sole right to decide when and to whom to offer which type of service.

SafeScrypt CA reserves the right and discretion not to accept the request for issue of any Certificate or the class of the Certificates requested for. The verification and validation processes for different classes will be at the discretion of SafeScrypt CA which is in conformance with the CCA Office Orders. For example such processes for Class 3 certificate under the SafeScrypt CA Hierarchy may be more extensive and detailed than Class 2 certificate under the same hierarchy.

SafeScrypt CA assert that all Certificates issued under CCA hierarchy are as per the CCA Digital Signature Certificate Interoperability Guidelines (IOG) published at http://www.cca.gov.in In the event of any inconsistency between this document and that CCA orders/IOG, that CCA orders/IOG takes precedence over this document.

Trademark Notices

SafeScrypt CA
Sify Technologies Limited
2nd Floor, Tidel Park,
No. 4, Rajiv Gandhi Salai
Taramani, Chennai 600113
Tel: +91-44-2254 0770
Fax: +91-44-2254 0777
Email: enquires@sifycorp.com

Table of Contents

1. Introduction

This document is the SafeScrypt CA Certification Practice Statement (CPS). It states the practices that SafeScrypt CA employs in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of the Indian Information Technology Act 2000 (IT Act 2000), its amendments and rules and regulations framed therein.

Sify Technologies Limited has been awarded a CA license by the Controller of Certifying Authorities (CCA) (see http://www.cca.gov.in) appointed under the IT Act 2000 and operates under the brand name SafeScrypt CA (SafeScrypt). SafeScrypt focus exclusively on Internet Trust and Security Services and Solutions (see https://www.safescrypt.com). As part of these services, SafeScrypt offers Certifying Authority (CA) and PKI Services.

Under this CA license, SafeScrypt offers a range of CA Services that enable individuals and organizations to obtain Digital Signature Certificates that qualify as Digital Signature Certificates under the IT Act 2000. SafeScrypt services and solutions offer individuals and organizations the choices of becoming Subscribers or Registration Authorities (RA) – thus catering to varied market requirements.

1.1 Overview

The SafeScrypt CA Hierarchy is based on the India PKI Certificate Policy (“India PKI CP”). The requirements established via this CP protect the security and integrity of the India PKI Hierarchy and apply to all India PKI Hierarchy Participants. More information concerning the India PKI CP is available at www.cca.gov.in.

The SafeScrypt CA is certified by the Root Certifying Authority of India (RCAI). This root is envisaged to serve as the basis for cross-certification amongst various licensed CA’s in India for consumer applications. Under this hierarchy, the following Classes of Certificates are available:

- Class 1
- Class 2
- Class 3

The SafeScrypt CA Hierarchy components are explained in detail in the rest of the CPS. Each component of SafeScrypt CA hierarchy is governed by the SafeScrypt CA CPS and its own unique policies and requirements – hence each of these is outlined separately in each section /sub-section of this CPS. The individual Subscribers and Relying Parties are required to take cognizance of the sections / subsections relevant to them

This Certification Practice Statement (CPS) is applicable to CA, RA’s, Subscribers and Relying Parties within the SafeScrypt CA Hierarchy.

Thus, the CPS, as a single document, covers practices and procedures concerning the issuance and management of all certificate classes within SafeScrypt CA Hierarchy.

1.1.1 Role of the SafeScrypt CA CPS and Other Practices Documents

The CPS describes, among other things:

- Obligations of Certifying Authority, Registration Authorities (RA’s), Subscribers, and Relying Parties within the SafeScrypt CA Hierarchy,
- Legal matters that are covered in Subscriber Agreements and Relying Party Agreements within the SafeScrypt CA Hierarchy,
- Audit and related security and practice’s review

- Methods used within the SafeScrypt CA Hierarchy to confirm the identity of Certificate Applicants for each Class of Certificate,
- Operational procedures for Certificate lifecycle services undertaken in the SafeScrypt CA Hierarchy: Certificate Applications, issuance, acceptance, revocation, and renewal,
- Operational security procedures for audit logging, records retention, and disaster recovery used within the SafeScrypt CA Hierarchy,
- Physical, personnel, key management, and logical security practices of the SafeScrypt CA Hierarchy,
- Certificate and Certificate Revocation List content within the SafeScrypt CA Hierarchy, and
- Administration of the CPS, including methods of amending it.

The CPS, however, is only one of a set of documents relevant to the SafeScrypt CA Hierarchy. These other documents include:

Ancillary security and operational documents that supplement the CPS by providing more detailed requirements, such as:

- The SafeScrypt CA Security Policy which sets forth the Security Principles governing the SafeScrypt CA Public Key Infrastructure
- The Security and Audit Requirements Guide, which describes detailed requirements for SafeScrypt CA concerning personnel, physical, telecommunications, logical, and cryptographic key management security,
- The SafeScrypt CA Security Policy and Guide, which describes detailed requirements for Customers concerning personnel, physical, telecommunications, logical, and cryptographic key management security, and
- SafeScrypt CA Key Management Guide, which presents detailed key management operational requirements.

In many instances, the CPS refers to these ancillary documents for specific, detailed practices implementing specific standards where including the specifics in the CPS could compromise the security of the SafeScrypt CA Hierarchy

Table 1 is a matrix showing various practices documents, whether they are publicly available, and their locations. The list in Table 1 is not intended to be exhaustive. Note that documents not expressly made public are confidential to preserve the security of the SafeScrypt CA.

Documents	Status	Where Available to the Public
Ancillary Security and Operational Documents		
SafeScrypt CA Security Policy	Confidential	N/A
Security and Audit Requirements Guide	Confidential	N/A
SafeScrypt CA Key Management Guide	Confidential	N/A
SafeScrypt CA hierarchy-Specific Documents		
SafeScrypt Certification Practice Statement	Public	SafeScrypt Repository per CPS 3.0. See https://www.safescrypt.com/drupal/?q=Repository
SafeScrypt CA's ancillary agreements (Subscriber Agreements and Relying Party Agreements)	Public	SafeScrypt Repository per CPS 3.0. See https://www.safescrypt.com/drupal/?q=Repository

Table 1 – Availability of Practices Documents

1.1.2 Compliance with Applicable Standards

The practices specified in this CPS have been designed to meet the requirements of the Indian IT Act 2000, its amendments associated Rules and Regulations as well as generally accepted and developing industry standards related to the operation of CAs and derived from India PKI Certificate Policy (“India PKI CP”). More information concerning the India PKI CP is available at www.cca.gov.in.

1.2 Document Name and Identification

This document is the Certification Practice Statement of the SafeScrypt CA has assigned following OID to this document.

- OID: 2.16.356.100.1.1.2

1.3 PKI Participants

The following are roles relevant to the administration and operation of the SafeScrypt CA.

1.3.1 Certifying Authority

The term “Certifying Authority” is used in several contexts globally. This section clarifies its use in this CPS.

When the term “Certifying Authority” or CA is used in a standalone manner in this CPS, it refers to SafeScrypt CA operated by Sify Technologies Ltd. as the entity that holds the CA licence from the Controller of Certifying Authorities (CCA), Government of India.

Sify Technologies Limited shall provide CA services and issue digital signature certificates usually with several “classes” of certificates and in turn each class is associated with different level of trust. In order to differentiate between certificates corresponding to each of these classes, the SafeScrypt CA usually creates different standalone key pairs from which a digital signature certificate of a particular class is issued.

1.3.1.1 CA Obligations

CAs performs the specific obligations appearing throughout this CPS. The provisions of the CPS specify obligations of SafeScrypt CA (in its role as Service Provider)

In addition, SafeScrypt CA uses commercially reasonable efforts to ensure that Subscriber Agreements and Relying Party Agreements bind Subscribers and Relying Parties within SafeScrypt’s subdomain. Examples of such efforts include, but are not limited to, requiring assent to a Subscriber Agreement as a condition of enrolment or requiring assent to a Relying Party Agreement as a condition of receiving Certificate status information. Similarly, RA’s(where required by contract) must use Subscriber Agreements and Relying Party Agreements in accordance with the requirements imposed by SafeScrypt CA. The Subscriber Agreements and Relying Party Agreements used by SafeScrypt, and RA’s must include the provisions required by CPS 9.6-9.9

1.3.2 Registration Authorities (RA)

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 submits the applicant’s request for certificate issuance to CA. RA should have legally enforceable agreement with CA.

1.3.2.1 RA Obligations

RA facilitate verification of subscriber credentials, entering subscriber information and verifies correctness and securely communicating requests to and responses from the CA. CA assumes all responsibility for verification carried out by RA.

1.3.3 Subscribers

A Subscriber is a named individual who applies for and is issued a digital signature certificate.

A Subscriber must follow request and retrieve the certificate from a specified website of the SafeScrypt CA in accordance with the procedure identified in this CPS and Subscriber Agreement.

1.3.3.1 Subscriber Obligations

Subscriber obligations in the CPS apply to Subscribers within SafeScrypt's subdomain, through this CPS, by way of Subscriber Agreements. The Subscriber Agreements in force within SafeScrypt's Subdomain appear at: https://www.safescrypt.com/drupal/?q=Repository.

Within SafeScrypt's domain of services, Subscriber Agreements require that Certificate Applicants provide complete and accurate information on their Certificate Applications and manifest assent to the applicable Subscriber Agreement as a condition of obtaining a Certificate.

Subscriber Agreements apply the specific obligations appearing in the CPS to Subscribers in the SafeScrypt CA hierarchy. Subscriber Agreements require Subscribers to use their Certificates in accordance with CPS 1.4, 4.5. They also require Subscribers to protect their private keys in accordance with CPS 6.1-6.2, 6.4. Under these Subscriber Agreements, if a Subscriber discovers or has reason to believe there has been a Compromise of the Subscriber's Private Key or the activation data protecting such Private Key, or the information within the Certificate is incorrect or has changed, that the Subscriber must promptly:

- Notify the entity that approved the Subscriber's Certificate Application, in accordance with CPS 4.9.1. and request revocation of the Certificate in accordance with CPS 3.4, 4.9.3.1, and
- Notify any person that may reasonably be expected by the Subscriber to rely on or to provide services in support of the Subscriber's Certificate or a digital signature verifiable with reference to the Subscriber's Certificate.

Subscriber Agreements require Subscribers to cease use of their private keys at the end of their key usage periods under CPS 6.3.2.

Subscribers should further note that the Indian IT Act 2000 specifies that the responsibility of the private key is solely that of the subscriber

Subscriber Agreements state that Subscribers shall not monitor, interfere with, or reverse engineer the technical implementation of the SafeScrypt CA Hierarchy and shall not otherwise intentionally compromise the security of the SafeScrypt CA Hierarchy CA Services.

1.3.4 Relying Parties

Parties relying on the certificate ("Relying Parties") are application providers who permit the Subscriber to use the certificate to access the applications. Relying parties would be those application providers who provide application services and recognise certificates as per the Information Technology Act 2000.

1.3.4.1 Relying Party Obligations

Relying Party obligations apply to Relying Parties within SafeScrypt's domain of services, through this CPS, by way of SafeScrypt's Relying Party Agreements. Relying Party Agreements in force within SafeScrypt's Sub domain appear at: https://www.safescrypt.com/drupal/?q=Repository.

Relying Party Agreements within SafeScrypt's Sub domain state that before any act of reliance, Relying Parties must independently assess the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose. They state that SafeScrypt and RAs are not responsible for assessing the appropriateness of the use of a Certificate. Relying Party Agreements specifically state that Relying Parties must not use Certificates beyond the limitations in CPS 1.4 and for purposes prohibited in CPS.

Relying Party Agreements further state that Relying Parties must utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain. Under these Agreements, Relying Parties must not rely on a Certificate unless these verification procedures are successful.

Relying Party Agreements also require Relying Parties to check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CPS 4.9.6, 4.9.10, 4.10. If any of the Certificates in the Certificate Chain have been revoked, according to Relying Party Agreements, the Relying Party must not rely on the end-user Subscriber Certificate or other revoked Certificate in the Certificate Chain.

Finally, Relying Party Agreements state that assent to their terms is a condition of using or otherwise relying on Certificates. Relying Parties that are also Subscribers agree to be bound by Relying Party terms under this section, disclaimers of warranty, and limitations of liability when they agree to a Subscriber Agreement.

Relying Party Agreements state that if all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Party Agreements state that Relying Parties must not monitor, interfere with, or reverse engineer the technical implementation of the SafeScrypt Public Hierarchy and shall not otherwise intentionally compromise the security of the SafeScrypt Public Hierarchy CA Services.

1.3.5 Other Participants

Parties other than the CA, RA, subscriber and relying parties would constitute other participants.

1.4 Digital Signature Certificate Usage

1.4.1. Appropriate Digital Signature Certificate Uses

The digital signature certificate usage is issued for the purposed indicated in the key usage field of the certificate. These are to be used in relying party application for the purpose of online authentication and carrying digital signatures on electronic records.

More generally, Certificates shall be used only to the extent use is consistent with all applicable laws, rules and regulations and in particular shall be used only to the extent permitted by applicable laws.

Assurance Level	Assurance	Applicability
Class 1	Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial
Class 3	This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

Table 2 – Certificate Use

1.4.2 Prohibited Certificate Uses

Certificates issued by SafeScrypt CA are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS is administered by the SafeScrypt CA. SafeScrypt CA may be contacted at the following location.

Mail Address:
SafeScrypt CA
Sify Technologies Limited
2nd Floor, Tidel Park,
No. 4, Rajiv Gandhi Salai,
Taramani, Chennai 600113
Tel: +91-44-2254-0770
Fax: +91-44-2254-0777
Email: enquires@sifycorp.com

1.5.2 Contact Person

Address inquiries about the CPS to enquires@sifycorp.com or to the following address:

SafeScrypt CA
Sify Technologies Limited
2nd Floor, Tidel Park,
No. 4, Rajiv Gandhi Salai,
Taramani, Chennai 600113
Attn: Practices Development – CPS
Phone: +91-44-2254-0770
Fax: +91-44-2254-0777

1.5.3 Person Determining CPS Suitability for the Policy

The organization identified in CPS 1.5.1 is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the CP and this CPS in accordance with the guidelines provided by the CCA, India.

1.5.4 CPS Approval Procedures

Amendments to this CPS shall be made by SafeScrypt CA and approved by Controller of Certifying Authorities, India. Amended versions or updates shall be linked to the SafeScrypt CA Repository located at: https://www.safescrypt.com/drupal/?q=Repository. Updates always supersede any designated or conflicting provisions of the referenced version of the CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

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

“**Act**”: Unless otherwise specified the word ‘**Act**’ or ‘**IT Act**’ in this CPS refers to “Information Technology Act 2000” & amendments there to

“**SafeScrypt CA**” is a brand name, refers to the Certifying Authority, owned by Sify Technologies Limited, which is licensed by Controller of Certifying Authorities (CCA), Govt. of India under IT Act 2000, and includes the associated infrastructure as mentioned in this CPS for providing Certification & Trust services.

“**Sify Technologies Limited**” refers to a Matrix company which is a registered Public Company limited by Shares.

“**Applicant**” or “**User**” means a person, entity or organization that has requested for a digital signature certificate to be issued by SafeScrypt CA.

“**Auditor**” means any Audit organizations appointed by SafeScrypt CA or at times by CCA itself and also empanelled by Controller of Certifying Authorities (CCA) for auditing of Licensed CA.

"**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 the IT Act;

“**Digital signature certificate**” means a digital signature certificate issued by SafeScrypt CA under Section 35 of IT Act

“**CA**” refers to SafeScrypt CA, as licensed by CCA, India to issue digital signature certificates.

“**Controller**” means the Controller of Certifying Authorities appointed as per Section 17 of the IT Act.

Certification Practice Statement (CPS) - means a statement issued by Safescrypt CA to specify the practices that SafeScrypt CA employs in issuing Digital Signature Certificates. Unless otherwise specified, the word “**CPS**” used throughout this document refers to Certification Practice Statement of SafeScrypt CA

The “**Certificate Policy**” or **“CP”** is the principal statement of policy governing a PKI hierarchy. It establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing Digital Certificates within the PKI hierarchy and providing associated trust services.

“**Private Key**” means that part of cryptographic key pair generated for creating Digital Signature

“**Registration Authority**” or “**RA**” means 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 submits the applicant’s request for certificate issuance to CA. RA should have legally enforceable agreement with CA.

“Subordinate CA” or **“Sub-CA”** is part of SafeScrypt CA technical infrastructure.

It is to be noted that:

1. The CCA India digitally signs the public keys of the SafeScrypt CA and in turn signs the public keys of sub-CA are – thereby ensuring the authenticity of each of the sub-CA’s that can be verified by any entity.

2. SafeScrypt CA cannot have more than one level of hierarchy under them. Sub-CA comes under the single SafeScrypt CA ambit and under one single CA license. Therefore sub-CA under them in their hierarchy derive their legal licensed status in India from the SafeScrypt CA license

All responsibilities, including liabilities associated with any certificate under any class or any sub CA under any class of any SafeScrypt hierarchy ultimately rests with SafeScrypt CA.

“**Subscriber**” means a person, entity or organization in whose name the Digital Signature Certificate is issued.

Note: The contextual meaning of the terms may be considered for such terms that are used in this CPS but not defined above. In case of any issue / confusion about terms used in this CPS, their original meaning will be prevailed as per defined in the IT Act, 2000 and guidelines issued by CCA

1.6.2 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
eKYC	Electronic- Know Your Customer
ESP	E-Sign Service Provider
DN	Distinguished Name

ITU	International Telecommunications Union
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment
SSL	Secure Socket Layer
SUB-CA	Subordinate Certifying Authority
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

2. Publication and Repository Responsibilities

2.1 Repositories

SafeScrypt is responsible for the repository functions for its own sub-CAs. SafeScrypt CA publishes all Digital Signature Certificates they issue in the repository.

SafeScrypt CA uses directory service following the LDAP protocol for publishing the digital signature certificate issued to its Subscribers. The SafeScrypt CA maintains a certificate revocation list ("CRL"), a lists of all the certificates revoked and made non-operation and is accessible to relying party applications.

The SafeScrypt CA maintains a repository for its CPS and the policies it support. This repository is located at the SafeScrypt CA Website URL https://www.safescrypt.com/drupal/?q=Repository

2.2 Publication of Certification Information

SafeScrypt is responsible for the repository function for:

- All Digital Signature Certificates within the SafeScrypt CA Public Hierarchy

Certificates issued by SafeScrypt CA are published into the directory server. This is accessible over the Internet. Relying parties and subscribers can download certificates through query of the SafeScrypt LDAP directory server at ldap://ldap.safescrypt.com.

2.3 Time or Frequency of Publication

Updates to this CPS are published in accordance with CPS 9.12.1. Updates to Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published upon issuance. Certificate status information is published in accordance with CPS 4.9.7 and 4.9.9.

2.4 Access Controls on Repositories

Information published in the repository portion of the SafeScrypt CA web site is publicly accessible information. Read only access to such information is unrestricted. SafeScrypt CA requires persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. SafeScrypt CA has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

SafeScrypt CA Hierarchy Certificates contain X.501 Distinguished Names in the Issuer and Subject fields.

3.1.1.1 SafeScrypt CA

SafeScrypt CA Issuer Distinguished Names consist of the components specified in Table below in accordance with the IOG guidelines of CCA.

Attribute	Value
Common Name (CN)	CCA India {Generation Qualifier} (re-issuance number}
Organization (O)	India PKI
Country (C)	IN

Table 3 - SafeScrypt CA Issuer Distinguished Names

SafeScrypt CA Subject Distinguished Names consist of the components specified in Table below.

Attribute	Value
Common Name (CN)	SafeScrypt CA {Generation Qualifier} {Re-issuance Number}
House Identifier	II Floor, Tidel Park,
Street Address	No. 4 Rajiv Gandhi Salai, Taramani,Chennai,
State / Province	Tamil Nadu
Postal Code	600 113
Organizational Unit (OU)	Certifying Authority
Organization (O)	Sify Technologies Limited
Country (C)	IN

Table 4 - SafeScrypt CA Subject Distinguished Names

3.1.1.2 SafeScrypt Sub-CA

SafeScrypt Sub-CA Certificates Issuer Distinguished Names consist of the components specified in SafeScrypt technical CA Subject Distinguished Names under mentioned under CPS 3.1.1.1

SafeScrypt Sub-CA Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Table below.

Attribute	Value
Common Name (CN)	SafeScrypt sub-CA for “Branding Name” {Generation Qualifier} {Re-issuance Number}
Organizational Unit (OU)	Sub-CA
Organization (O)	Sify Technologies Limited
Country (C)	IN

Table 5 - SafeScrypt Sub-CA Subject Distinguished Name

3.1.1.3 End-User Subscriber

End-user Subscriber Certificates Issuer Distinguished Names consist of the components specified in SafeScrypt Sub-CA Subject Distinguished Names under mentioned under CPS 3.1.1.2

End-user Subscriber Certificates contain an X.501 distinguished name in the Subject name field and consist of the components specified in Interoperability Guidelines (IOG) for Digital Signature Certificates, under End user Certificate – Subject Specifications.

3.1.1.4 Other Type of Certificates

SafeScrypt issues other type of certificate like Device certificate. The Issuer Distinguished Names consist of the components specified in the CCA Interoperability guidelines.

3.1.2 Need for Names to be Meaningful

Subscriber Certificates must contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate. For such Certificates, pseudonyms of end-user Subscribers (names other than a Subscriber's true personal or organizational name) are not permitted.

SafeScrypt CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscribers are required to provide verifiable names to be included in the certificate. A Certificate is used for authentication and hence it is necessary to include only names that can be validated against established credentials like PAN Card, Passport, Driving License or other such documents issued by a competent authority.

3.1.4 Rules for Interpreting Various Name Forms

No Stipulation.

3.1.5 Uniqueness of Names

SafeScrypt CA ensures that Subject Distinguished Names is achieved through Pubic Key uniqueness for all subscribers within the SafeScrypt CA Hierarchy. Subscriber can have multiple digital signature certificates of different class or purpose.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. SafeScrypt, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrates, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. SafeScrypt is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

SafeScrypt CA performs the validation process as per the Identity Verification Guidelines (IVG) of CCA (Refer to link- http://www.cca.gov.in).

3.2.1 Method to Prove Possession of Private Key

SafeScrypt CA verifies the Certificate Applicant's possession of a private key through the use of a digitally signed certificate request pursuant to PKCS #10, another cryptographically equivalent demonstration, or another SafeScrypt-approved method.

3.2.2 Authentication of Organizational Person Identity

SafeScrypt CA confirms the identity of Class 2 and Class 3 organizational end-user Subscribers and other enrolment information provided Certificate Applicants in accordance Identity Verification

Guidelines (IVG) - of CCA (Refer to link- http://www.cca.gov.in). In addition to the procedures below, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS 3.2.1.

3.2.2.1 Authentication of the Identity of Organizational End-User Subscribers

3.2.2.1.1 Authentication for Organizational Person Digital Signature Certificates

SafeScrypt confirms the identity of a Certificate Applicant for an organizational person Digital signature Certificate by:

- Verifying that the organization person entity and as per the Identity Verification Guidelines (IVG) of CCA (Refer to link: http:\www.cca.gov.in)
- Where a domain name is included in the certificate SafeScrypt CA authenticates the Organization's right to use that domain name as a fully qualified Domain name.

.

3.2.2.2 Authentication of the Identity of Sub-CAs

For SafeScrypt sub CA Certificate Applications, certificate requests are created, processed and approved by authorized SafeScrypt CA personnel using a controlled process that requires the participation of multiple trusted SafeScrypt employees.

3.2.3 Authentication of Individual Identity

For all Classes of individual Certificates, SafeScrypt CA confirms that:

- the Certificate Applicant is the person identified in the Certificate Application,
- the Certificate Applicant rightfully holds the private key corresponding to the public key to be listed in the Certificate in accordance with CPS 3.2.1, and
- the information to be included in the Certificate is accurate.

In addition, SafeScrypt CA performs the more detailed procedures described below for each Class of Certificate.

3.2.3.1 Class 1 Certificates

Class 1 certificates are validated as per the Identity Verification Guidelines (IVG) of CCA. (Refer to link: http://www.cca.gov.in)

3.2.3.2 Class 2 Certificates

Class 2 certificates are validated as per the Identity Verification Guidelines (IVG) of CCA. (Refer to link: http://www.cca.gov.in)

3.2.3.3 Class 3 Certificates

Class 3 certificates are validated as per the Identity Verification Guidelines (IVG) of CCA. (Refer to link: http://www.cca.gov.in)

3.2.3.4 Other Type of Certificates and Services

SafeScrypt CA issues other types of certificates as per as per the Identity Verification Guidelines (IVG) of CCA. (Refer to link: http://www.cca.gov.in)

3.2.3.4.1. Device/System Certificate

Certificates need to be issued to computer systems for the purpose of machine to machine authentication; it is of paramount importance that the certificate contains a unique identification relating to the systems. At the same time, it is essential that the applications making use of such certificates are designed to verify the system with the digital certificate being used. Device/ system Certificate are validated as per the Identity Verification Guidelines (IVG) of CCA. (Refer to link: http://www.cca.gov.in)

3.2.3.4.2. Document Signer Certificate

The Document Signer Certificates are issued to organisational software applications for operating automatically to authenticate documents/information attributed to the organisation by using Digital Signature applied on the document documents/Information. Document Signer Certificate is validated as per the Identity Verification Guidelines (IVG) of CCA. (Refer to link: http://www.cca.gov.in)

3.2.4 Validation of Authority

Wherever a person is authorised to receive a certificate on behalf of an organization, then a certificate from an authorised person of the organization is used to validate the same. The authorised person should be an employee of an organisation with the designation Manager and above.

3.2.5 Criteria for Interoperation

Interoperability guidelines (Refer to link: http://www.cca.gov.in) issued by the CCA, India would be considered in establishing the criteria to recognize interoperation.

3.3 Identification and Authentication for Re-key Requests

Currently re-key requests are not provided as a part of the SafeScrypt CA services. Certificate re-key is not included in the guidelines provided by the office of CCA

3.3.1 Identification and Authentication for Routine Re-key

Not applicable please refer cps 3.3

3.3.2 Identification and Authentication for Re-key after Revocation

Not applicable please refer cps 3.3

3.4 Identification and Authentication for Revocation Request

Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber submit the Subscriber’s Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

SafeScrypt CA Administrators are entitled to request the revocation of end-user Subscriber Certificates within SafeScrypt CA’s Sub-domain. SafeScrypt CA authenticates the identity of

Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Certificate Applications for End-User Subscriber Certificates

For SafeScrypt CA Certificates, all end-user Certificate Applicants shall undergo an enrolment process consisting of:

- completing a Certificate Application and providing the required information,
- generating, or arranging to have generated, a key pair in accordance with CPS 6.1,
- the Certificate Applicant delivering his, her, or its public key, directly or through RA to SafeScrypt CA, in accordance with CPS 6.1.3,
- demonstrating to SafeScrypt CA pursuant to CPS 3.2.1 that the Certificate Applicant has possession of the private key corresponding to the public key delivered to SafeScrypt, and
- manifesting assent to the relevant Subscriber Agreement.

Certificate Applications are submitted either to SafeScrypt CA for processing, either approval or denial. The entity processing the Certificate Application and the entity issuing the Certificate pursuant to CPS 4.2 may be two different entities as shown in the following table.

Certificate Class/Category	Entity Processing Certificate Applications	Entity Issuing Certificate
Class 1 Certificate	SafeScrypt or RA	SafeScrypt
Class 2 Certificate	SafeScrypt or RA	SafeScrypt
Class 3 Certificate	SafeScrypt or RA	SafeScrypt

Table 6 – Entities Receiving Certificate Applications

4.1.2 Sub-CA Certificate

Sub-CA Certificate is processed as per the IOG guidelines of CCA (Refer to link: http://www.cca.gov.in)

4.1.3 Who can submit a Digital Signature Certificate Application

The subscriber can submit a digital signature certificate application. However, for Class 3 digital signature certificates the subscriber should present himself or herself to CA for issuance of digital signature certificate.

4.1.4 Enrolment Process and Responsibilities

The subscriber should enrol for the digital signature certificate. The subscriber is responsible for the correctness of information provided in the enrolment and key pair generation and safe keeping of private key. The subscriber should further receive the digital signature certificate upon intimation.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Registration Authority (RA) facilitate verification of subscriber credentials, entering subscriber information and verifies correctness and securely communicating requests to and responses from the CA. CA assumes all responsibility for verification carried out by RA.

4.2.2 Approval or Rejection of Digital Signature Certificate Applications

Based on the validation requirement for different classes of Digital Signature Certificates as per the Identity Verification Guidelines (IVG) (Refer to link http://www.cca.gov.in) of CCA, Trusted validation executive of SafesScrypt CA approves or rejects the applications for Digital Signature Certificates.

4.2.3 Time to Process Digital Signature Certificate Applications

The certificate applications would be taken up for processing and completed within 2 working days.

4.3 Digital Signature Certificate Issuance

SafeScrypt CA issues digital signature certificate to Subscribers and End Entities subject to the following practice details below in the following sections.

4.3.1 Issuance of End-User Subscriber Certificates

After a Certificate Applicant submits a Certificate Application, SafeScrypt CA, RA, attempts to confirm the information in the Certificate Application pursuant to CPS 3.2.2.1, 3.2.3. Upon successful performance of all required authentication procedures pursuant to CPS 3.1, SafeScrypt CA. If authentication is unsuccessful, SafeScrypt CA or denies the Certificate Application.

A Digital Signature Certificate is created and issued following the approval of a Digital Signature Certificate Application to issue the Digital Signature Certificate. SafeScrypt creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application. The procedures of this section are also used for the issuance of Certificates in connection with the submission of a request to replace (i.e., renew or rekey) a Certificate. Class 2, Class 3, Device/System Certificate, Document Signer Certificate, are approved as per the Identity Verification Guidelines (IVG) of CCA (Refer to link: http://www.cca.gov.in).

4.3.3 CA Actions during Digital Signature Certificate Issuance

A Subscriber or End Entity submits digital signature certificate request to the SafeScrypt CA or other SafeScrypt authorised RA along with the prescribed documents. The RA verifies subscriber's information provided in the digital signature request form.
All requests of the RA are forwarded to SafeScrypt CA for the approval and SafeScrypt CA processes all the requests as per the validation process. A Digital Signature Certificate is issued/rejected or kept on hold if there is any discrepancy. If there is no discrepancy, SafeScrypt CA creates and issues a Certificate to the Applicant based on the information in a DSC Request Form

4.3.4 Notification to Subscriber by the CA of Issuance of Certificate

The CA would notify the subscriber through mail of the issuance of certificate and the subscriber is expected to download the certificate as instructed in the mail notification.

4.4 Certificate Acceptance

Upon Certificate generation, SafeScrypt notifies Subscribers that their Digital Signature Certificates are available and notifies them of the means for such Digital Signature Certificates.

Upon issuance, Certificates are made available to end-user Subscribers, either by allowing them to download from a web site or via a message sent to the Subscriber containing the Certificate. For example, SafeScrypt may send the Subscriber a PIN, which the Subscriber enters into an enrolment web page to obtain the Certificate.

4.4.1Publication of the Certificate by the CA

The SafeScrypt CA will publish the certificate in the directory immediately after issuance.

4.4.2 Notification of Certificate Issuance by the CA to Other Entities

The SafeScrypt CA will only notify the subscriber of certificate via email about issuance of the certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Digital Signature Certificate Usage

Usage of a private key and certificate by subscriber are subject to the terms of the subscriber agreement. Subscriber should use private key only after the subscriber has accepted the corresponding certificate. Subscriber must discontinue use of the private key following the expiration or revocation of the certificate.

Subscriber shall safeguard the private key from third party access using hardware crypto token to store it or by password protecting it. Subscriber shall use private key in accordance to constraints set in the certificate extension

- Key Usage
- Extended Key Usage
- Certificate Policy

4.5.2 Relying Party Public Key and Certificate Usage

Usages of a private key and corresponding certificate are subject to the terms of the relying party agreement.

Relying party shall use public key in accordance to constraints set in the certificate extension

- Key Usage
- Extended Key Usage
- Certificate Policy

4.6 Certificate Renewal and Renewal Process

It is compulsory for subscriber to generate new key pair and replace the existing key pair on expiry. Therefore certificate renewal is not permitted.

4.7 Certificate Re-key and Renewal

4.7.1 Circumstance for Certificate Re-key

Prior to the expiration of an existing Subscriber’s Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. SafeScrypt CA generally requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as “rekey”). Table below describes SafeScrypt CA’s requirements for routine rekey (issuance of a new certificate for a new key pair that replaces an existing key pair) and renewal (issuance of a new certificate for an existing key pair).

Generally speaking, both “Re-key” and “Renewal” is commonly described as “Certificate Renewal,” focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated.

Certificate Class and Type	Routine Rekey and Renewal Requirements
Class 1	For these types of Certificates, Subscriber key pairs are browser generated or can be generated & stored in FIPS Certified Hardware as part of the online enrolment process. The Subscriber does not have the option to submit an existing key pair for “renewal.” Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not.
Class 2 & Class 3	For these types of Certificates, Subscriber key pairs can be generated & stored only in FIPS Certified Hardware as part of the online enrolment process. The Subscriber does not have the option to submit an existing key pair for “renewal.” Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not

Table 7 – Routine Re-key and Renewal Requirements

4.7.2 Who May Request Certification of a New Public Key

The subscriber of certificate can request for renewal through the Registration Authority (RA) /CA. On approval of request by CA, a new digital signature certificate would be issued to the subscriber.

4.7.3 Processing Certificate Re-keying Requests

Subscriber should submit the certificate within its validity period for renewal through the SafeScrypt CA services portal/ RA. Certificate which have expired or revoked will not be renewed. However customer has to submit fresh set of documents and undergo all validation process as per Identity Verification Guidelines (IVG) of CCA (Refer to link: http://www.cca.gov.in).

4.7.4 Notification of New Digital Signature Certificate Issuance to Subscriber

On successful processing of application, enrolment and approval by the Certifying authority, the Safescrypt CA issues certificate. The subscriber receives a notification on the email id provided in the enrolment form. No other form of notification of issuance would be made by the CA.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

A subscriber is deemed to have accepted the certificate when they have not explicitly intimated the CA about their refusal to accept the certificate citing reasons within 2 days of receiving certificate issuance intimation from the CA.

4.7.6 Publication of the Re-Keyed Certificate by the CA

The renewal certificate is published in the CA repository.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The CA will only notify the subscriber of certificate issuance and publish the certificate in the repository

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Not supported, subscriber to seek fresh certificate and follow the enrolment process applicable for new certificates.

4.8.2 Who May Request Certificate Modification

Not applicable, please refer CPS 4.7.1.

4.8.3 Processing Certificate Modification Requests

Not applicable please refer CPS 4.7.1

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable please refer CPS 4.7.1

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable please refer CPS 4.7.1

4.8.6 Publication of the Modified Certificate by the CA

Not applicable please refer CPS 4.7.1

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable please refer CPS 4.7.1

4.9 Certificate Revocation and Suspension

An end-user Subscriber Certificate is revoked if:

- SafeScrypt CA or a Subscriber has reason to believe or strongly suspects that there has been a Compromise of a Subscriber’s private key,
- SafeScrypt CA has reason to believe that 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,
- SafeScrypt CA has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by the applicable CPS, the Certificate was issued to a person other than the one named as the Subject of the Certificate, or the Certificate was issued without the authorization of the person named as the Subject of such Certificate,
- SafeScrypt CA has reason to believe that a material fact in the Certificate Application is false,
- SafeScrypt CA determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
- The information within the Certificate is incorrect or has changed, or
- The Subscriber requests revocation of the Certificate in accordance with CPS

SafeScrypt CA Subscriber Agreements require end-user Subscribers to immediately notify SafeScrypt CA of a known or suspected compromise of its private key in accordance with the procedures in CPS

The revocation of the Certificate shall be done after adopting the process prescribed in the India IT Act and rules and regulations made there under.

4.9.1 Who Can Request Revocation

4.9.1.1 Who Can Request Revocation of an End-User Subscriber Certificate

The following entities may request revocation of an end-user Subscriber Certificate:

- Individual Subscribers may request revocation of their own individual Certificates.
- In the case of organizational person Certificates, only a duly authorized representative of the organization is entitled to request the revocation of Certificates issued to the organization.
- A duly authorized representative of SafeScrypt is entitled to request the revocation of a Certificate.

4.9.2 Procedure for Revocation Request

4.9.2.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

An end-user Subscriber requesting revocation is required to communicate the request to SafeScrypt or the Customer approving the Subscriber's Certificate Application, who in turn will initiate revocation of the certificate promptly.

4.9.3 Revocation Request Grace Period

Revocation requests must be submitted and further action will be taken as per 4.9.4 of CPS.

4.9.4 Time within Which CA Must Process the Revocation Request

The CA will process the request for revocation within 01 day time after firmly establishing the genuineness of such request.

4.9.5 Revocation Checking Requirement for Relying Parties

Relying Parties must check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely.

4.9.6 CRL Issuance Frequency

SafeScrypt CA publishes CRLs showing the revocation of certificate issued by SafeScrypt CA and offers status-checking services. CRLs for the end-user Subscriber Certificates are published daily. CRLs for sub-CA Certificates are published annually and whenever such a sub-CA Certificate is revoked. Expired Certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration.

4.9.7 Maximum Latency for CRLs

CRLs will be published every 24 hours by the CA. Download of CRL and validation latencies are network and relying party application dependent and the CA is not responsible for any such latencies.

4.9.8 Online Revocation/Status Checking Availability

In addition to publishing CRLs, SafeScrypt CA provides Certificate status information through in the SafeScrypt CA repository.

SafeScrypt CA also provides OCSP Certificate status information for Relying Parties. Relying parties who contract for OCSP services may check Certificate status with OCSP. The URL for the relevant OCSP Responder is communicated to then subscribing Relying Party. Safescrypt CA follows the OCSP Guidelines for CAs as issued by CCA. (Refer to link- http//www.cca.gov.in)

4.9.9 Online Revocation Checking Requirements

If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party must check Certificate status using one of the applicable methods specified in this CPS.

4.9.10 Other Forms of Revocation Advertisements

No stipulation.

4.9.11 Special Requirements Re-Key Compromise

In addition to the procedures described in CPS, SafeScrypt CA will make commercially reasonable efforts to notify potential Relying Parties of such a compromise.

4.9.12 Circumstances for Suspension

SafeScrypt CA does not offer suspension services for end-user Subscriber’s Digital signature Certificates.

4.9.13 Who Can Request Suspension

Not applicable.

4.9.14 Procedure for Suspension Request

Not applicable.

4.9.15 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

Online certificate status is available to register relying parties and other subscribers. This is standards compliant OCSP responder which provides a standard OCSP response to registered relying parties. Safescrypt CA follows the OCSP Guidelines for CAs as issued by CCA. (Refer to link-http://www.cca.gov.in)

4.10.1 Operational Characteristics

A standards compliant OCSP client can place a request to the SafeScrypt OCSP responder. The OCSP responder would provide a standard response based on the status of the certificate.

4.10.2 Service Availability

The service would be available 24 x 7 to registered relying parties only. The process of registration and details of usage are separately provided under a separate agreement between SafeScrypt CA and the relying party.

4.10.3 Optional Features

Not applicable

4.11 End of Subscription

On expiry of the validity period of the digital signature certificate or on its revocation by the subscriber or by any other authorised body as described in this CPS, the subscription ends.

4.12 Key Escrow and Recovery

Key escrow services are not currently provided by SafeScrypt CA. As and when these services become available the description for the same would be included in the CPS.

5. Facility, Management, and Operational Controls

SafeScrypt CA has implemented the SafeScrypt CA Security Policy, which supports the security requirements of this CPS.

5.1 Physical Controls

5.1.1 Site Location and Construction

SafeScrypt's CA operations are conducted within SafeScrypt's facilities in Chennai, India, which meet the requirements of SafeScrypt Security and Audit Requirements. The facilities also fulfil all criteria specified in the Information Technology (Certifying Authorities) Rules, and Information Technology (Certifying Authorities) Regulations, prescribed under the Information Technology Act, 2000 of India. All SafeScrypt CA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

SafeScrypt's primary facilities have up to seven physical security tiers as described in CPS 5.1.2 with:

- CA functions performed within Tier 4
- Sensitive servers, including the SafeScrypt CA Server, located in Tier 4
- Online CA cryptographic modules stored in Tier 5
- Offline CA cryptographic modules stored in Tier 7.

5.1.2 Physical Access

SafeScrypt CA systems are protected by four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. In addition, the physical security system includes three additional tiers for key management security. The characteristics and requirements of each tier are described in Table 8 below.

Tier	Description	Access Control Mechanisms
Physical Security Tier 1	Physical security tier one refers to the outermost physical security barrier for the facility.	Access to this tier requires the use of a proximity card employee badge. Physical access to tier one is automatically logged and video recorded.
Physical Security Tier 2	Tier two includes common areas including restrooms and common hallways.	Tier two enforces individual access control for all persons entering the common areas of the CA facility through the use of a proximity card employee badge. Physical access to tier two is automatically logged.
Physical Security Tier 3	Tier three is the first tier at which sensitive CA operational activity takes place. Sensitive CA operational activity is any activity related to the lifecycle of the certification process such as authentication, verification, and issuance.	Tier three enforces individual access control through the use of two-factor authentication including biometrics. Individuals approved for unescorted tier three accesses must satisfy the Trusted Employee Policy. Unescorted personnel, except those authorized, including un-trusted employees or visitors, are not allowed into a tier-three secured area. Physical access to tier three is automatically logged.

Tier	Description	Access Control Mechanisms
Physical Security Tier 4	Tier four is the tier at which especially sensitive CA operations occur. There are two distinct tier four areas: the online tier 4 data center and the offline tier 4 key ceremony rooms.	The tier four data center enforces individual access control and the key ceremony room enforces dual control, each through the use of two-factor authentication including biometrics. Individuals approved for unescorted tier four accesses must satisfy the Trusted Employee Policy. Physical access to tier four is automatically logged.
Key Management Tiers 5-7	Key Management tiers five through seven serve to protect both online and offline storage of Cryptographic Signing Unit (CSU) and keying material.	Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with SafeScrypt CA's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers are logged for audit purposes. Progressively restrictive physical access privileges control access to each tier.

Table 8 – Physical Security Tiers

5.1.3 Power and Air Conditioning

SafeScrypt CA's secure facilities are equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

SafeScrypt CA has taken reasonable precautions to minimize the impact of water exposure to SafeScrypt CA systems.

5.1.5 Fire Prevention and Protection

SafeScrypt CA has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. SafeScrypt CA's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information are stored within SafeScrypt 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).

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 zeroized in accordance the manufacturer's guidance prior to disposal. Other waste is disposed of in accordance with SafeScrypt CA's normal waste disposal requirements.

5.1.8 Off-Site Backup

SafeScrypt CA performs routine backups of critical system data, audit log data, and other sensitive information

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or renewal requests, or enrolment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- or the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel,
- cryptographic business operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

SafeScrypt considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements of CPS 5.3.

5.2.2 Number of Persons Required Per Task

SafeScrypt maintains a policy and rigorous control procedures to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (cryptographic signing unit or CSU) and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device. Persons with physical access to modules do not hold “Secret Shares” and vice versa. Requirements for CA private key activation data and Secret Shares are specified in CPS 6.2.7.

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 Trusted Persons performing SafeScrypt CA HR [or equivalent]or security functions and a check of well-recognized forms of identification (e.g., Pan Card, passports and driver’s licenses). Identity is further confirmed through the background checking procedures in CPS 5.3.2.

SafeScrypt 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 SafeScrypt CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Operations Manager, Security Manager, Key Manager, Share Holders and RA's would require role separation.

5.3 Personnel controls

5.3.1 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 5 years for personnel holding Trusted Positions.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, SafeScrypt conducts background checks, which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records (local, state or provincial, and national),
- check of credit/financial records,
- search of driver's license records.

It should be noted here that the term "employment" covers not only those personnel who are employees of SafeScrypt CA but also those who work on a contract basis or as consultants also.

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, SafeScrypt will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

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 unfavourable or unreliable personal references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

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 behaviour 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 laws of India.

5.3.3 Training Requirements

SafeScrypt CA provides its personnel with training upon hire and the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily. SafeScrypt CA periodically reviews and enhances its training programs as necessary.

SafeScrypt CA's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- SafeScrypt CA security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining Frequency and Requirements

SafeScrypt 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 training is provided on an ongoing basis.

5.3.5 Job Rotation Frequency and Sequence

No stipulation

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorized actions or other violations of SafeScrypt 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.

5.3.7 Independent Contractor Requirements

Independent contractors and consultants who have not completed the background check procedures specified in CPS 5.3.2 are permitted access to SafeScrypt's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.

5.3.8 Documentation Supplied to Personnel

SafeScrypt CA personnel involved in the operation of SafeScrypt CA's PKI services are required to read this CPS, and the SafeScrypt CA Security Policy. SafeScrypt CA provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

SafeScrypt CA manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by SafeScrypt personnel
  - Security sensitive files or records read, written or deleted

- Security profile changes
- System crashes, hardware failures and other anomalies
- Firewall and router activity
- CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Identity of the entity making the journal entry
- Kind of entry.

SafeScrypt CA log Certificate Application information including:

- 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's 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 receiving CA or submitting RA, if applicable.

5.4.2 Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, SafeScrypt reviews its audit logs for suspicious or unusual activity in response to alerts generated based on irregularities and incidents within SafeScrypt CA.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also be documented.

5.4.3 Retention Period for Audit Log

Audit logs are retained and archived in accordance with CPS 5.5.2.

5.4.4 Protection of Audit Log

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.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed monthly.

5.4.6 Audit Collection System (Internal vs. External)

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

5.4.7 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.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, monthly, and annual basis in accordance with the requirements of the Security and Audit Requirements Guide. An annual LSVA serves as an input into the annual Compliance Audit.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to the audit logs specified in CPS 5.4, SafeScrypt CA maintains records that include documentation of:

a) SafeScrypt CA's compliance with the CPS and other obligations under its agreements with their Subscribers, and
b) actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation, expiration, and rekey or renewal of all Certificates it issues from the SafeScrypt Processing/Service Center.

SafeScrypt CA's records of Certificate life cycle events include:

- the identity of the Subscriber named in each Certificate,
- the identity of persons requesting Certificate revocation,
- other facts represented in the Certificate,
- time stamps, and
- certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a Compliance Audit under CPS 9.12.

Records may be maintained electronically or in hard copy, provided that such records are accurately and completely indexed, stored, preserved, and reproduced.

5.5.2 Retention Period for Archive

Digital Records associated with a Certificate are retained for at least the time periods set forth below following the date the Certificate expires or is revoked:

SafeScrypt CA Hierarchy:

- Seven (7) years for Class 1 Certificates
- Seven (7) years for Class 2 Certificates, and
- Seven (7) years for Class 3 Certificates

If necessary, SafeScrypt may implement longer retention periods in order to comply with applicable laws for all products.

5.5.3 Protection of Archive

SafeScrypt CA protects its archived records compiled under CPS 5.5.1 so that only authorized Trusted Persons are permitted to access archived data. Electronically archived data is protected against unauthorized viewing, modification, deletion, or other tampering through the implementation of appropriate physical and logical access controls. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archived data can be accessed for the time period set forth in CPS 5.5.2.

5.5.4 Archive Backup Procedures

SafeScrypt CA performs full backup of its issued Certificate information on a daily basis. Copies of paper-based records compiled under CPS 5.5.1 are maintained in an off-site disaster recovery facility in accordance with CPS 5.7.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries contain time and date information.

5.5.6 Archive Collection System (Internal or External)

Data archival happens on two sets of backup media. One is stored on site and the other is sent to the off-site.

5.5.7 Procedures to Obtain and Verify Archive Information

See CPS 5.5.3.

5.6 Key Changeover

SafeScrypt CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in CPS 6.3.2. SafeScrypt CA Certificates may be renewed as long as the cumulative certified lifetime of the CA key pair does not exceed the maximum CA key pair lifetime. New CA key pairs will be generated as necessary, for example to replace CA key pairs that are being retired, to supplement existing, active key pairs and to support new services in accordance with CPS 6.1 and as stipulated in the IT Act and Certificate Policy of India PKI issued by CCA.

5.7 Compromise and Disaster Recovery

SafeScrypt CA maintains its Disaster Recovery facility in its Data Center in Bengaluru, India The facility is replica of the primary SafeScrypt CA centre in terms CA Infrastructure and security architecture. The infrastructure is designed to take over the functions of the CA in the event of disaster.

5.7.1 Key Compromise

Upon the suspected or known Compromise of a SafeScrypt CA, SafeScrypt infrastructure or Customer CA private key, SafeScrypt's Key Compromise Response procedures are enacted by the Compromise Incident Response Team (CIRT). This team, which includes Security, Cryptographic Business Operations, Production Services personnel, and other SafeScrypt management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from SafeScrypt executive management.

If CA Certificate revocation is required, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the SafeScrypt repository in accordance with CPS 4.9.7,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected Participants, and
- The CA will generate a new key pair in accordance with CPS 5.6, except where the CA is being terminated in accordance with CPS 5.8.

5.7.2 Disaster Recovery

SafeScrypt CA has in place a Disaster Recovery (DR) Plan to mitigate the effects of any kind of natural or man-made disaster. SafeScrypt's DR plan is being modelled after the specifications provided in the IT Act 2000 and its associated rules and regulations.

5.7.3 Incident and Compromise Handling Procedures

Incident and compromise handling procedures are stipulated in the SafeScrypt Security Policy documents.

5.7.4 Computing Resources, Software, and/or Data are corrupted

The entire CA and the data can be reconstructed using the backup material available in the event such software / data are corrupted.

5.7.5 Entity Private Key Compromise Procedures

SafeScrypt CA follows the same standard for all subscribers in all its domain of services, irrespective of which hierarchy the subscriber is subscribing to. Subscriber Agreements state that Subscribers failing to meet these Standards are solely responsible for any loss or damage resulting from such failure.

SafeScrypt CA would also like to point out here that the India IT Act and its associated rules and regulations holds the subscriber solely responsible for the protection of his or her private key.

5.7.6 Business Continuity Capabilities after a Disaster

SafeScrypt CA's DR would take over the functions to provide business continuity in the event of a disaster. SafeScrypt CA through its back-up capability and use its best efforts to restore SafeScrypt CA functionality at the disaster recovery location in the event of system failure at SafeScrypt CA.

5.8 CA Termination

In the event that it is necessary for a SafeScrypt CA to cease operation, SafeScrypt makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is required, SafeScrypt will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans may address the following, as applicable in line with the provisions of the IT Act 2000 and rules and regulations made there under:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by SafeScrypt,
- The preservation of the CA's archives and records for the time periods required in CPS 5.5,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services. The revocation of unexpired un-revoked Certificates of end-user Subscribers and subordinate CAs, if necessary. The payment of compensation (if necessary) to Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and

Provisions needed for the transition of the CA's services to a successor CA, if applicable.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and required cryptographic strength for the generated keys. The cryptographic modules used for key generation for all CAs -- including Issuing Root CAs, SafeScrypt CAs,

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the Key Ceremony Reference Guide, the CA Key Management Tool User's Guide, and the Security and Audit Requirements Guide. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by SafeScrypt Management.

Generation of RA key pairs is performed by the RA and Generation of end-user Subscriber key pairs is performed by the Subscriber. For Class 2 Certificates and Class 3 Certificates, Subscriber should /meet use FIPS 140-1/2 Level 2 Validated Hardware Cryptographic tokens for key generation as per the CCA regulations, For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

6.1.2 Private Key Delivery to Subscriber

End-user Subscriber key pairs are typically generated by the end-user Subscriber; therefore in such cases, private key delivery to a Subscriber is not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

End-user Subscribers and RAs submit their public key to SafeScrypt for certification electronically through the use of a PKCS#10 Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL) and a signed certificate is delivered to the subscriber through a secured online session.

6.1.4 CA public Key Delivery to Relying Parties

For its SafeScrypt CA Public hierarchy the certificates on SafeScrypt's repository are at https://www.safescrypt.com/drupal/?q=Repository.

SafeScrypt generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. SafeScrypt CA Certificates may also be downloaded from the SafeScrypt LDAP Directory at ldap://ldap.safescrypt.com.

6.1.5 Key Sizes

SafeScrypt CA key pairs are all 2048 bit RSA. SafeScrypt CA mandated that Registration Authorities and end-user Subscribers generate 2048 bit RSA key pairs to ensure they comply with the requirements of the India IT Act 2000.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Applicable

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

For X.509 Version 3 Certificates, SafeScrypt populates the Key Usage extension of Certificates in accordance with Interoperability guidelines (IOG) of CCA (Refer to link: http://www.cca.gov.in).. SafeScrypt has implemented a combination of physical, logical, and procedural controls to ensure the security of SafeScrypt, Managed PKI Customer, and CA private keys. Logical and procedural controls are described in CPS 6.3. Physical access controls are described in CPS 5.1.2. Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

SafeScrypt CA private keys are generated and used from Hardware Security Module conforming to FIPS Level II standards. These modules are housed in multi-tiered CA centre and do not leave the premises. Access to HSM is always through multi-level authentication.

6.2.2 Private Key (n out of m) Multi-Person Control

SafeScrypt CA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. SafeScrypt uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (n) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (m) is required to activate a CA private key stored on the module.

Table 9 below shows the threshold number of shares required and the total number of shares distributed for the different types of SafeScrypt CAs. It should be noted that the number of shares distributed for disaster recovery tokens is less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with CPS 6.5.

Entity	**Required Secret Shares to Enable CA's Private Key to Sign End-User Subscriber Certificates**	**Required Secret Shares to Sign CA's Certificate**	**Total Secret Shares Distributed**	**Disaster Recovery Shares**	
				Shares Needed	**Total Shares**
Class 1 CA and subordinate CAs	3	3	7	3	7
Class 2 CA and subordinate CAs	3	3	7	3	7
Class 3 CA and subordinate CAs	3	3	7	3	7

Table 9 – Secret Share Distribution and Thresholds

6.2.3 Private Key Escrow

SafeScrypt does not escrow CA, RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement.

6.2.4 Private Key Backup

SafeScrypt creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of CPS 6.2.1. CA private keys are copied to backup hardware cryptographic modules in accordance with CPS 6.2.6.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CPS 5.1, 6.2.1. SafeScrypt does not store copies of RA private keys and Subscriber private keys.

6.2.5 Private Key Archival

When SafeScrypt CA key pairs reach the end of their validity period, such CA key pairs will be archived for a period of at least 5 years. Archived CA key pairs will be securely stored using hardware cryptographic modules that meet the requirements of CPS 6.2.1. Procedural controls prevent archived CA key pairs from being returned to production use. Upon the end of the archive period, archived CA private keys will be securely destroyed in accordance with CPS 6.2.9.

SafeScrypt does not archive copies of RA and Subscriber private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

SafeScrypt generates CA key pairs on the hardware cryptographic modules in which the keys will be used. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

SafeScrypt CA private keys are stored only on HSM conforming FIPS Level III certification. These are tamper proof devices, in the event the HSM is tampered the private key volatilizes.

6.2.8 Method of Activating Private Key

All SafeScrypt Domain Services Participants are required to protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

6.2.8.1 End-User Subscriber Private Keys

Subscribers should use enhanced private key protection mechanisms available today including the use of smart cards, biometric access devices, and other hardware tokens to store private keys. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.2.8.2 Administrators' Private Keys

Use of a password along with a smart card, biometric access device, in accordance with CPS 6.4.1 is recommended to authenticate the Administrator before the activation of the private key.

6.2.8.3 Private Keys Held by SafeScrypt

SafeScrypt CA private keys are activated by a threshold number of Shareholders supplying their activation data (tokens or passphrases) in accordance with CPS 6.2.2. For SafeScrypt's offline CAs, the CA private key is activated for one session (e.g., for the certification of a Subordinate CA or an instance where a PCA signs a CRL) after which it is deactivated and the module is returned to secure storage. For SafeScrypt's online CAs, the CA private key is activated for an indefinite period and the module remains online in the production data centre until the CA is taken offline (e.g., for system maintenance). SafeScrypt Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

6.2.9 Method of Deactivating Private Key

SafeScrypt CA private keys are deactivated upon removal from the token reader. Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers has an obligation to adequately protect their private key(s)

6.2.10 Method of Destroying Private Key

SafeScrypt destroys CA 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. SafeScrypt 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.

6.2.11 Cryptographic Module Rating

SafeScrypt CA uses best in class HSM conforming to FIPS140 -1/2 Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

SafeScrypt CA, RA and end-user Subscriber Certificates are backed up and archived as part of SafeScrypt's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period of a Certificate ends upon its expiration or revocation. The Operational Period for key pairs is the same as the Operational Period for the associated Certificates, except that private keys may continue to be used for decryption and public keys may continue to be used for signature verification. The maximum Operational Periods for SafeScrypt Certificates for Certificates issued on or after the effective date of this CPS are set forth in Table below.

In addition, SafeScrypt CAs stops issuing new Certificates at an appropriate date prior to the expiration of the CA's Certificate such that no Certificate issued by a Subordinate CA expires after the expiration of any Superior CA Certificates.

Certificate Issued By:		
SafeScrypt CA Hierarchy	Class 2	Class 3
CA to Subordinate CA	Up to 10 years	Up to 10 years
CA to end-user Subscriber	Up to 2 years	Up to 2 years

Table 10 – Certificate Operational Periods

Except as noted in this section, SafeScrypt Sub domain Participants shall cease all use of their key pairs after their usage periods have expired.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing SafeScrypt CA private keys is generated in accordance with the requirements of CPS 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

SafeScrypt RAs & Subscribers are required to select strong passwords to protect their private keys. SafeScrypt's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

SafeScrypt strongly recommends that RAs, and end-user Subscribers choose passwords that meet the same requirements. SafeScrypt also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

SafeScrypt Shareholders are required to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities. SafeScrypt strongly recommends that RAs and end-user Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

See CPS 6.5.1 and 6.5.2.

6.5 Computer Security Controls

SafeScrypt performs all CA functions using trustworthy systems that meet the requirements of SafeScrypt's Security and Audit Requirements Guide.

6.5.1 Specific Computer Security Technical Requirements

SafeScrypt ensures that the systems maintaining CA software and data files are trustworthy systems secure from unauthorized access. In addition, SafeScrypt limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

SafeScrypt's production network is logically separated from other components. This separation prevents network access except through defined application processes. SafeScrypt 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.

SafeScrypt require the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. SafeScrypt requires that passwords be changed on a periodic basis.

Direct access to SafeScrypt databases supporting the SafeScrypt repository is limited to Trusted Persons in SafeScrypt's operations group having a valid business reason for such access.

6.5.2 Computer Security Rating

Not Applicable in India.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by the SafeScrypt in accordance with SafeScrypt systems development and change management standards. SafeScrypt also provides software to its Customers for performing RA functions. Such software is developed in accordance with SafeScrypt system development standards.

6.6.2 Security Management Controls

SafeScrypt has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. SafeScrypt creates a hash of all software packages and SafeScrypt software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, SafeScrypt validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

SafeScrypt performs all its CA and RA functions using networks secured in accordance with the Security and Audit Requirements Guide to prevent unauthorized access and other malicious activity. SafeScrypt protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping

This is as per the Interoperability Guidelines for Digital Signature Certificate Certificates issued by CCA India.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

CPS defines SafeScrypt CA's Certificate Profile and Certificate content requirements for SafeScrypt CA Hierarchy Certificates issued under this CPS.

SafeScrypt CA Certificates conform to

a) ITU-T Recommendation X.509 Version 3
b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("RFC 5280")

c) Interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act, issued by CCA India.

7.1.1 Version Number(s)

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2 Certificate Extensions

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.1 Key Usage

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.2 Certificate Policies Extension

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.3 Subject Alternative Names

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.4 Basic Constraints

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.5 Extended Key Usage

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.6 CRL Distribution Points

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.7 Authority Key Identifier

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.8 Subject Key Identifier

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.2.9 Authority Information Access

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.3 Algorithm object identifiers

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.4 Name Forms

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.1.5 Name Constraints

No stipulations

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate Class of Certificate as shown in the table below.

Sr. No.	Certificate Type	Certificate Policies OID
1	CA	2.16.356.100.2
2	Sub-CA	2.16.356.100.2
3	Class 1	2.16.356.100.2.1
4	Class 2	2.16.356.100.2.2
5	Class 3	2.16.356.100.2.3

Table 11 – Certificate Policy Object Identifier

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

SafeScrypt populates X.509 Version 3 Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the SafeScrypt CA CPS. In addition, some Certificates contain a User Notice Qualifier that points to the applicable Relying Party Agreement. This is as per the Interoperability Guidelines for Digital Signature Certificate Certificates issued by CCA India (Refer to link http://www.ccca.gov.in).

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.2.1 Version Number(s)

This is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India.

7.2.2 CRL and CRL Entry Extensions

Must be included when reason code = key compromise or CA compromise. The criticality field of this extension is set to FALSE which is as per the Interoperability Guidelines for Digital Signature Certificates issued by CCA India (Refer to link http://www.ccca.gov.in).

.

7.2.3. Authority Key Identifier

Authority Key Identifier should be composed of the 160-bit SHA-1 hash of value of the BIT STRING Authority Public Key in the certificate (excluding the tag, length, and number of unused bits).
OR
The Authority Key Identifier should be composed of a four-bit type field with value 0100 followed by the least significant 60 bits of SHA-1 hash of the value of the BIT STRING Issuer Public Key (excluding the tag, length, and number of unused bits. This is as per the Interoperability Guidelines for Digital Signature Certificate Certificates issued by CCA India.

7.3 OCSP Profile

SafeScrypt CA provides OCSP services in conformance to RFC 2560 & India PKI Certificate Policy

7.3.1 Version Number(s)

SafeScrypt CA provides OCSP services in conformance to RFC 2560 & India PKI Certificate Policy

7.3.2 OCSP Extensions

SafeScrypt CA provides OCSP services in conformance to RFC 2560 & India PKI Certificate Policy

8. Compliance Audit and Other Assessments

SafeScrypt performs regular audits, annual as well as half yearly internal audits, in compliance with the Specifications in the IT Act 2000, and its associated rules and regulations. These audits are performed by an auditor empanelled with the Controller of Certifying Authorities (CCA), Govt. of India.

This audit is performed for SafeScrypt's CA operations data center operations and key management operations supporting SafeScrypt's services.

In addition to compliance audits, SafeScrypt shall be entitled to perform other reviews and investigations to ensure the trustworthiness of SafeScrypt's domain of services, which include, but are not limited to:

- SafeScrypt or its authorized representative shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself or a Customer in the event SafeScrypt or its authorized representative has reason to believe that the audited entity has failed to meet SafeScrypt Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity's failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of any of the SafeScrypt hierarchy.
- SafeScrypt or its authorized representative shall be entitled to perform "Supplemental Risk Management Reviews" on itself or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

SafeScrypt or its authorized representative shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with SafeScrypt and the personnel performing the audit, review, or investigation.

8.1 Frequency or Circumstances of Assessment

Compliance audits are performed on an annual basis.

8.2 Identity/Qualifications of Assessor

SafeScrypt's compliance audits are performed by an audit firm that is empanelled by the Controller of Certifying Authorities (CCA), Govt. of India.

8.3 Assessor's Relationship to Assessed Entity

Compliance audits of SafeScrypt's operations are performed by an auditing firm that is independent of SafeScrypt.

8.4 Topics Covered by Assessment

The scope of SafeScrypt's annual audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls. The details are available in the CCA Audit criteria and its associated rules and guidelines (Refer to link http://www.cca.gov.in).

8.5 Actions Taken as a Result of Deficiency

With respect to compliance audits of SafeScrypt's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by SafeScrypt management with input from the auditor. SafeScrypt management is responsible for developing and implementing a corrective action plan. If SafeScrypt determines that such exceptions or deficiencies pose an immediate threat to the security or integrity, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, SafeScrypt Management will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communication of Results

Results of the compliance audit of SafeScrypt's operations will be submitted to the CCA and may be released to any other party at the discretion of SafeScrypt management.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Access Fees

SafeScrypt and Customers do not charge a fee as a condition of making a Certificate available in a repository However, SafeScrypt reserves the right to charge such fees, to any of its customers at any given point in time without prior notice.

9.1.2 Revocation or Status Information Access Fees

SafeScrypt does not charge a fee as a condition of making the CRLs required by CPS 4.9.7 available in a repository or otherwise available to Relying Parties at the time of publication of this CPS. However, SafeScrypt reserves the right to charge such fees to any of its customers at any given point in time without prior notice. SafeScrypt does, however, charge a fee, for OCSP services, or other value-added revocation and status information services. SafeScrypt does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilize such Certificate status information without SafeScrypt's prior express written consent.

9.1.3 Fees for Other Services such as Policy Information

SafeScrypt does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, is subject to a license agreement with the entity holding the copyright to the document. This holds true at the time of publication of this CPS. However, SafeScrypt reserves the right to charge such fees, to any of its customers at any given point in time without prior notice.

9.1.4 Refund Policy

Within SafeScrypt's Subdomain, the following refund policy (reproduced at https://www.safescrypt.com/drupal/?q=node/110) is in effect:

SafeScrypt adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber may request that SafeScrypt revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber may request that SafeScrypt revoke the certificate and provide a refund if SafeScrypt has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate. After SafeScrypt revokes the subscriber's certificate, SafeScrypt will promptly credit the subscriber's credit card account (if the certificate was paid for via credit card) or otherwise reimburse the subscriber via cheque, for the full amount of the applicable fees paid for the certificate. To request a refund, please call customer service at +91-44-2254 0863. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

Within SafeScrypt's domain of services, SafeScrypt reserves the sole right to take a decision regarding refunds to subscribers, should any cause for dissatisfaction arise on part of the subscriber.

9.2 Financial Responsibility

No Stipulation

9.2.1 Fiduciary Relationships

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, any fiduciary relationship between SafeScrypt on one hand and a Subscriber or Relying Party on the other hand.

9.2.2 Insurance Coverage

No Stipulation

9.2.3 Other Assets

No Stipulation

9.2.4 Insurance or Warranty Coverage for End-Entities

No Stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers are, subject to CPS 9.3.2, kept confidential:

- CA application records, whether approved or disapproved,
- Certificate Application records (subject to CPS 9.3.2),
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by SafeScrypt or a Customer,
- SafeScrypt audit reports created by SafeScrypt or their respective auditors
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of SafeScrypt hardware and software and the administration of Certificate services and designated enrolment services.

Any other records / data / information mandated to be kept confidential by the IT Act 2000, its associated rules and regulations

9.3.2 Information Not Within the Scope of Confidential Information

Participants of SafeScrypt CA services acknowledge that Certificates, Certificate revocation and other status information, SafeScrypt's repository, and information contained within them are not considered Confidential Information. Information not expressly deemed Confidential Information under CPS 9.3.2 shall be considered confidential.

9.3.3 Responsibility to Protect Confidential Information

Confidential information as mentioned in CPS 9.3.1 provided to the Subscriber, relying party or third parties are to be protected by the respective entities.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

SafeScrypt has implemented a privacy policy, which is located at: (https://www.safescrypt.com/drupal/?q=Privacy%20Policy).

9.4.2 Information Treated as Private

The following records of Subscribers are, subject to CPS 9.4.2, kept private:

- Customer registration information,
- Certificate Application records (subject to CPS 9.4.2),

Any other records / data / information mandated to be kept private by the IT Act 2000, its associated rules and regulations

9.4.3 Information Not Deemed Private

Participants of SafeScrypt CA services acknowledge that Certificates, Certificate revocation and other status information, Information published in Subject DN of the certificate. SafeScrypt's repository, and information contained within them are not considered Private Information. Information not expressly deemed Private Information under CPS 9.4.2 shall be considered private. This section is subject to applicable privacy laws.

9.4.4 Responsibility to Protect Private Information

Participants of SafeScrypt CA services will protect private information subject to CPS 9.4.2.

9.4.5 Notice and Consent to Use Private Information

Subscriber is deemed to have given consent to use private information by accepting the certificate application form and by accepting subscriber agreement and this CPS accepting registration process online.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Participants of SafeScrypt's domain of services acknowledge that SafeScrypt shall be entitled to disclose Confidential/Private Information if, the disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among Participants of SafeScrypt's domain of services other than Subscribers and Relying Parties is governed by the applicable agreements among such Participants of SafeScrypt's domain of services. The following subsections of CPS 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information

SafeScrypt retains all Intellectual Property Rights in and to the Certificates and revocation information that they issue. SafeScrypt and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of

Certificates is subject to the Relying Party Agreement referenced in the Certificate. SafeScrypt and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS

Participants of SafeScrypt's domain of services acknowledge that SafeScrypt retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of SafeScrypt CAs and end-user Subscribers are the property of the SafeScrypt and end-user Subscribers that are the respective Subjects of these Certificates regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs. Notwithstanding the foregoing, SafeScrypt's CA public keys and the root certificates containing them, including all the SafeScrypt CA public keys and self-signed Certificates, are the property of SafeScrypt. Finally, without limiting the generality of the foregoing, Secret Shares of a technical CA's private key are the property of the SafeScrypt, and retains all Intellectual Property Right in and to such Secret Shares.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

All responsibilities, including liabilities associated with any certificate under any class or any sub CA under any class of any SafeScrypt hierarchy ultimately rests with SafeScrypt CA

The warranties, disclaimers of warranty, and limitations of liability among SafeScrypt, and their respective Customers within SafeScrypt's subdomain are set forth and governed by the agreements among them. This CPS 9.6.1 relates only to the warranties that SafeScrypt must make to end-user Subscribers receiving Certificates from them and to Relying Parties, the disclaimers of warranties they shall make to such Subscribers and Relying Parties, and the limitations of liability they shall place on such Subscribers and Relying Parties. .

SafeScrypt uses, and (where required) shall use, Subscriber Agreements and Relying Party Agreements in accordance with CPS 1.3.1.1. These Subscriber Agreements shall meet the requirements imposed by SafeScrypt. Requirements that Subscriber Agreements contain warranties, disclaimers, and limitations of liability below apply to those that use Subscriber Agreements. SafeScrypt adheres to such requirements in its Subscriber Agreements. SafeScrypt's practices concerning warranties, disclaimers, and limitations in Relying Party Agreements apply to SafeScrypt. Note that terms applicable to Relying Parties shall also be included in Subscriber Agreements, in addition to Relying Party Agreements, because Subscribers often act as Relying Parties as well.

9.6.1.1 Certifying Authority Warranties to Subscribers and Relying Parties

SafeScrypt's Subscriber Agreements include, and other Subscriber Agreements shall include, a warranty to Subscribers that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,

- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to this CPS in all material aspects.

SafeScrypt's Relying Party Agreements contain a warranty to Relying Parties who reasonably rely on a Certificate that:

- All information in or incorporated by reference in such Certificate, is accurate,
- In the case of Certificates appearing in the SafeScrypt repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with CPS 4.4, and
- The entities approving the Certificate Application and issuing the Certificate have substantially complied with this CPS when issuing the Certificate.

9.6.2 RA Representations and Warranties

The warranties, disclaimers of warranty, and limitations of liability between an RA & SafeScrypt CA, it is assisting to issue Certificates, are set forth and governed by the agreements between them. Safescrypt CA assumes all responsibility for verification carried out by RA.

9.6.3 Subscriber Representations and Warranties

SafeScrypt's Subscriber Agreements require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- No unauthorized person has ever had access to the Subscriber's private key,
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true,
- All information supplied by the Subscriber and contained in the Certificate is true,
- The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, and
- The Subscriber is an end-user Subscriber and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL or otherwise.

SafeScrypt would also like to point out here that the Indian IT Act 2000 holds the subscriber solely responsible for the protection of his or her private key.

9.6.4 Relying Party Representations and Warranties

Subscriber Agreements and Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CPS 1.3.5.1.

9.6.5 Representations and Warranties of Other Participants

No warranty is extended by SafeScrypt CA to other parties other than specifically mentioned in this CPS.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements disclaim, and other Subscriber Agreements shall disclaim, SafeScrypt's possible warranties, including any warranty of merchantability or fitness for a particular purpose.

9.8 Limitations of Liability

The issue of Certificates by SafeScrypt are based on verifications done on best practices adopted and on best endeavour basis and it is inherent that neither SafeScrypt or RA performing activities under this CPS can underwrite the conduct or activities of the subscribers or otherwise assure the bonafide of the actions. SafeScrypt and RA do not accept any liability to the Relying Party on this account. Further even in other eventualities to the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements limit, and other Subscriber Agreements shall limit, SafeScrypt's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. They also include the following liability caps limiting SafeScrypt's damages concerning a specific Certificate:

Class	Liability Caps
SafeScrypt Hierarchy:	
Class 1	Indian Rupees Two Hundred
Class 2	Indian Rupees Two Hundred
Class 3	Indian Rupees One Thousand

Table 12 – Liability Caps

9.9 Indemnities

9.9.1 Indemnification by Subscribers and Relying Parties

9.9.1.1 Indemnification by Subscribers

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements require, and other Subscriber Agreements shall require, Subscribers to indemnify SafeScrypt s for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or 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.

9.9.1.2 Indemnification by Relying Parties

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements require, and other Subscriber Agreements shall require, Relying Parties to indemnify SafeScrypt and any non-SafeScrypt for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- 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.

9.10 Term and termination

Not Applicable

9.10.1 Term

Not Applicable

9.10.2 Termination

Not Applicable

9.10.3 Effect of Termination and Survival

Not Applicable

9.11 Individual Notices and Communications with Participants

No specific stipulations

9.12 Amendments

9.12.1 Specification Change Procedures

Amendments to this CPS shall be made by SafeScrypt and approved by the Controller of Certifying Authorities, Government of India. Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be linked to the Practices Updates and Notices section of the SafeScrypt Repository located at: https://www.safescrypt.com/drupal/?q=node/68. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2 Items that Can Change Without Notification

SafeScrypt 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. SafeScrypt's decision to designate amendments as material or non-material shall be within SafeScrypt's sole discretion.

9.12.3 Items that Can Change with Notification

SafeScrypt shall be entitled to make at its absolute discretion material amendments to the CPS in accordance with this CPS 2.2, 2.3

9.12.3.1 List of Items

Material amendments are those changes that SafeScrypt, under CPS 9.12.2, considers to be material.

9.12.4 Notification Mechanism

SafeScrypt's Practices Development group will post proposed amendments to the CPS in the Practices Updates and Notices section of the SafeScrypt Repository, which is located at:

https://www.safescrypt.com/drupal/?q=node/68. SafeScrypt solicits proposed amendments to the CPS from other SafeScrypt Subdomain Participants. If SafeScrypt considers such an amendment desirable and proposes to implement the amendment, SafeScrypt shall provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CPS to the contrary, if SafeScrypt believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security of the SafeScrypt's Subdomain, or any portion of the SafeScrypt CA, SafeScrypt shall be entitled to make such amendments by publication in the SafeScrypt Repository. Such amendments will be effective immediately upon publication.

9.12.5 Comment Period

Except as noted under CPS 9.12.4, the comment period for any material amendments to the CPS shall be fifteen (15) days, starting on the date on which the amendments are posted on the SafeScrypt Repository. Any SafeScrypt Subdomain Participant shall be entitled to file comments with SafeScrypt's Practices Development group up until the end of the comment period.

9.12.5.1 Mechanism to Handle Comments

SafeScrypt's Practices Development group will consider any comments on the proposed amendments. SafeScrypt 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 CPS 9.12.4, or

c) withdraw the proposed amendments. SafeScrypt is entitled to withdraw proposed amendments by providing notice in the Practices Updates and Notices section of the SafeScrypt Repository. Unless proposed amendments are amended or withdrawn, they shall become effective upon the expiration of the comment period under CPS 9.12.5.

9.12.6 Procedure for Amendment

No Specific Stipulation

9.12.7 Notification Mechanism and Period

No Specific Stipulation

9.12.8 Circumstances under Which OID Must Be Changed

Controller of Certifying Authorities, India in consultation with the CA can mandate changes to OID.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among SafeScrypt CA and Customers

Disputes between SafeScrypt and one of its Customers shall be resolved pursuant to provisions in the applicable agreement between the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, a dispute resolution clause.

9.13.3 Role of the Controller of Certifying Authorities

Under the IT Act 2000, the Controller of Certifying Authorities (CCA) is also authorized to resolve disputes arising out of CA services. His role is described in detail in the IT Act 2000 and its associated rules and regulations.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of India shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in India. This choice of law is made to ensure uniform procedures and interpretation for all participants within SafeScrypt's domain of services, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference may have their own governing law provisions, provided that this CPS 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.15 Compliance with Applicable Law

Applicable law in India is the Information Technology Act 2000

9.16 Miscellaneous Provisions

9.16.1 Force Majeure

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements include, and other Subscriber Agreements shall include, a force majeure clause protecting SafeScrypt.

9.16.2 Entire Agreement

Agreements between SafeScrypt CA and the subscriber, relying parties and other entities supersede anything contained in this document.

9.16.3 Assignment

No specific stipulation

9.16.4 Severability

To the extent permitted by applicable law, SafeScrypt's Subscriber Agreements and Relying Party Agreements contain, and other Subscriber Agreements shall contain, 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.

9.16.5 Enforcement (attorneys' fees and waiver of rights)

SafeScrypt CA shall not bear any attorney fee or any other expense that may be incurred by a Subscriber or Relying party.

9.17 Other Provisions

No specific Stipulations