SAFESCRYPT INDIA™ CPS

SAFESCRYPT INDIA CERTIFICATION PRACTICE STATEMENT

IN SUPPORT OF SAFESCRYPT'S INDIA PUBLIC CERTIFICATION SERVICES

VERSION 1.2

DATE OF PUBLICATION: 01/02/2002
PROPOSED EFFECTIVE DATE: 04/02/2002

Safescrypt Ltd,
667-668, Keshava Towers,
11th Main, 4th Block, Jayanagar,
Bangalore – 560 011.
Tel : +91-80-6555093 / +91-80-6555104

WARNING: THE USE OF SAFESCRYPT LTD'S INDIA PUBLIC CERTIFICATION SERVICES ARE SUBJECT TO VARIOUS INDIAN LAWS AND JURISDICTION OF COURTS, TRIBUNALS AND AUTHORITIES IN INDIA AND WHEREVER THERE ARE TRANSBORDER OR MULTI-NATIONAL IMPLICATIONS, THE USE SHALL ALSO BE SUBJECT TO APPROPRIATE LAWS, JURISDICTION AND COURTS, TRIBUNALS AND AUTHORITIES OF THE RELEVANT COUNTRY AND U.S. FEDERAL AND STATE CRIMINAL LAWS, WHICH MAY INCLUDE BUT ARE NOT LIMITED TO: THE INFORMATION TECHNOLOGY ACT, 2000 (IT ACT) AND RULES AND REGULATIONS FRAMED THEREUNDER, INDIAN PENAL CODE, 1860, THE CODE OF CRIMINAL PROCEDURE, 1973, FOREIGN EXCHANGE MANAGEMENT ACT, 1999, FOREIGN CONTRIBUTION (REGULATION) ACT, 1976, FOREIGN TRADE (DEVELOPMENT AND REGULATION) ACT, 1962, CONSERVATION OF FOREIGN EXCHANGE AND PREVENTION OF SMUGGLING ACTIVITIES ACT, 1974, SMUGGLERS AND FOREIGN EXCHANGE MANIPULATORS (FORFEITURE OF PROPERTY) ACT, 1976 AND ANY STATUTORY MODIFICATIONS OR RE-ENACTMENT OF THE ABOVE,

THIS CERTIFICATION PRACTICE STATEMENT SHALL BE READ WITH ANY STATEMENT WITH SUCH PARTICULARS AS THE CONTROLLER OF CERTIFICATION AUTHORITIES (CCA) MAY SPECIFY BY REGULATION IN EXERCISE OF HIS POWERS UNDER THE INFORMATION TECHNOLOGY ACT, 2000.

WRONG USE OF THE DIGITAL CERTIFICATES OR PUBLIC CERTIFICATION SERVICES IN INDIA SHALL BE LIABLE TO BE PROCEEDED WITH CONSEQUENCES CIVIL AND CRIMINAL AND SUBJECTED TO PENALTIES AND PUNISHMENT UNDER THE ABOVE AND OTHER ACTS. THE INFORMATION TECHNOLOGY ACT, 2000 AND RULES PROVIDE FOR SPECIFIC DUTIES OF SUBSCRIBERS AS CONTAINED IN CHAPTER VIII OF THE ACT.

SAFESCRYPT RESERVES THE RIGHT TO SEEK AND ASSIST IN THE PROSECUTION OF ANY PERSON WHO ALLEGEDLY COMMITS A CRIME DIRECTLY AFFECTING 'S PUBLIC CERTIFICATION SERVICES. SAFESCRYPT WILL OFFER A REWARD OF A SUM WHICH IT CONSIDERS APPROPRIATE FOR INFORMATION LEADING TO THE ARREST AND CONVICTION OF ANYONE COMMITTING SUCH A CRIME.

QUICK SUMMARY OF IMPORTANT CPS RIGHTS AND OBLIGATIONS

PLEASE SEE THE TEXT OF THIS CPS FOR DETAILS. THIS SUMMARY IS INCOMPLETE. MANY OTHER IMPORTANT ISSUES ARE DISCUSSED IN THE CPS.

NOTE :
Safescrypt offers two categories of Public Certification Services :

- The **India** Public Certification Services ("**India PCS**")
- The **VTN** (VeriSign Trust Network) Public Certification Services ("**VTN PCS**")

This CPS, known as the "India CPS" is solely for the India PCS. The VTN PCS has its own CPS , known as the "VTN CPS", which is a separate document. The reader is requested to take cognizance of this and accordingly refer to the appropriate CPS as per his or her requirements.

1. This India Certification Practice Statement (*see* definitions) controls the provision and use of Safescrypt's India public certification services (*see* definitions) – including certificate (*see* definitions) application § 4, application validation § 5, certificate issuance § 6, acceptance § 7, use § 8, and suspension and revocation § 9.

2. You (the user) acknowledge that (i) you have been advised to receive proper training in the use of public key techniques prior to applying for a certificate and that (ii) documentation, training, and education about digital signatures, certificates, PKI, and the India PCS are available from Safescrypt § 1.6.

3. Safescrypt offers different classes of certificates § 2.4. You must decide which class(es) of certificate are right for your needs.

4. Before submitting a certificate application § 4.2, you must generate a key pair §§ 2.5.3, 4.1 and keep the private key secure § 4.1 from compromise (*see* definitions) in a trustworthy (*see* definitions) manner § 4.1.1. Your software system should provide this functionality.

5. You must accept (*see* definitions) a certificate § 7.1 before communicating it to others, or otherwise inducing their use of it. By accepting a certificate (*see* definitions), you make certain important representations § 7.2.

6. If you are the recipient of a digital signature or certificate, you are responsible for deciding whether to rely on it. Before doing so, Safescrypt recommends that you check the Safescrypt repository (*see* definitions) to confirm (*see* definitions) that the certificate (*see* definitions) is valid (*see* definitions) and not revoked (*see*

definitions), or suspended (*see* definitions) and then use the certificate to verify § 8.1 that the digital signature (*see* definitions) was created during the operational period of the certificate by the private key (*see* definitions) corresponding to the public key (*see* definitions) listed in the certificate (*see* definitions), and that the message (*see* definitions) associated with the digital signature (*see* definitions) has not been altered.

7. You agree to notify § 12.10 the applicable issuing authority (*see* definitions) upon compromise (*see* definitions) of your private key (*see* definitions).

8. This India Certification Practice Statement (*see* definitions) provides various warranties made by Safescrypt and the issuing authorities § 11.2. Safescrypt also has a refund policy § 11.1. Otherwise, warranties are disclaimed and liability is limited by Safescrypt and issuing authorities §§ 11.3, 11.4, 11.5, 4.3.

9. The India Certification Practice Statement (*see* definitions) contains various miscellaneous provisions § 12, requires compliance with applicable export regulations § 12.2, and prohibits infringement § 12.14.

For more information, see Safescrypt's website at **https://www.safescrypt.com** *or contact customer service at* **customer_service@safescrypt.com**.

COMMENTS AND SUGGESTIONS

Editorial comments and suggestions for future revisions of this CPS are solicited from the user community. Please send your comments to:
practices@safescrypt.com or, to Safescrypt Ltd, 667-668, Keshava Towers, 11th Main, 4th Block, Jayanagar, Bangalore – 560 011. *Attn: Practices and External Affairs.* Tel : +91-80-6555093 / +91-80-6555104 Fax: 91-80-6555300.

TABLE OF CONTENTS

1. PREFATORY MATERIAL

This section introduces the Safescrypt India Certification Practice Statement (CPS) and describes its structure and underlying conventions. It concludes with a list of acronyms and abbreviations used in the CPS.

1.1 Executive Summary

This Safescrypt India Certification Practice Statement presents the practices that Safescrypt, its issuing authorities (IA's), and authorized non-Safescrypt IA's participating in the provision of Safescrypt's India public certification services (India PCS) employ in issuing and managing certificates and in maintaining a certificate-based public key infrastructure (PKI). It details and controls the certification process, from establishing IA's, commencing IA and repository operations, to enrolling subscribers. The India PCS provide for issuing, managing, using, suspending, revoking, and renewing of certificates. The India CPS is intended to legally bind and provide notice to all parties that create, use, and validate certificates within the context of the India PCS. As such, the India CPS plays a central role in governing the India PCS.

This India CPS governs only a portion of the complement of services offered by Safescrypt. Other Safescrypt services may neither require nor invoke a hierarchy of IA's. This India PCS will inevitably evolve to accommodate other structures in response to market demand. This India CPS is periodically updated to reflect new services and to improve the India PCS infrastructure in general. See CPS § 12.1

1.2 Structure of the CPS

The CPS takes a life cycle, or "cradle-to-grave," approach to describing certification processes. It begins with IA establishment and start-up procedures and then covers general IA operations; enrollment; use of certificates; and certificate suspension, revocation, and expiration.

1.3 Citing the CPS

This Certification Practice Statement should be cited in other documents as the "Safescrypt India CPS" or the "Safescrypt India Certification Practice Statement." It is internally cited as the "India CPS," or as "India CPS § *" and its appendices as "Appendix § 13.*" The India CPS is updated periodically. Versions of the India CPS are denoted by a version number following "CPS" (*e.g.*, "version 1.2" or "CPS 1.2").

1.5 Underlined Text

Underlined text in the on-line version of this India CPS represents the first instance in which defined terms (*see* Appendix 13.1 - Definitions) are used in this India CPS. The WWW-based version(s) of this India CPS use hypertext-linked underlined text (using HTML) for cross-referencing within the India CPS and for quick reference to definitions and other relevant documents.

1.6 Publication

This India CPS is published:

(1) in electronic form within the Safescrypt repository at https://www.safescrypt.com/India-Repository

(ii) in electronic form via E-mail from **CPS-requests@safescrypt.com**, and

(iii) in paper form from Safescrypt Ltd, 667-668, Keshava Towers, 11th Main, 4th Block, Jayanagar, Bangalore – 560 011. Tel : +91-80-6555093 / +91-80-6555104 Attn: Practices and External Affairs.

• Each of the referenced Safescrypt World Wide Web URLs is intended to invoke the HTTP with the Secure Sockets Layer (SSL) security protocol to facilitate "secure mode" record retrieval (when using a browser supporting SSL). Each such record is also available in "unsecure mode" by replacing *https://* with *http://*. The secure mode must be used to access the official version of all Web-accessed documents contained within the Safescrypt repository.

• Certain URLs cited in this India CPS point to directories rather than to actual messages. This facilitates maintaining such messages in multiple formats for the convenience of the reader. Much of the information referenced by Safescrypt URLs in the CPS is also available as records in electronic and paper form by E-mail request to **customer_service@safescrypt.com**.

1.6 Customer Service Assistance, Education, and Training

This India CPS assumes that the reader is generally familiar with digital signatures, PKIs, and Safescrypt's India PCS. If not, we advise some training in the use of public key techniques before the reader applies for a certificate. Educational and training information is accessible from Safescrypt at **https://www. safescrypt.com** and **https://digitalID. safescrypt.com**. Additional assistance is available from Safescrypt customer service representatives (**customer_service@safescrypt.com**).

ALL INDIA PCS APPLICANTS AND SUBSCRIBERS ACKNOWLEDGE THAT (i) THEY HAVE BEEN ADVISED TO RECEIVE PROPER TRAINING IN THE USE OF PUBLIC KEY TECHNIQUES PRIOR TO APPLYING FOR A CERTIFICATE AND THAT (ii) DOCUMENTATION, TRAINING, AND EDUCATION ABOUT DIGITAL SIGNATURES, CERTIFICATES, PKI, AND THE PCS ARE AVAILABLE FROM SAFESCRYPT.

1.7 Table of Acronyms and Abbreviations

CA	Certification authority
CK	common key
CRL	certificate revocation list
CSR	certificate signing request
DAM	draft amendment (to an ISO standard)
DPE	Distinguished Panel of Experts
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IA	issuing authority
India CPS	Safescrypt India Trust Network Certification Practice Statement
India PCS	Safescrypt's India public certification services
LRA	local registration authority
LRAA	local registration authority administrator
NSI	nonverified subscriber information
PCA	primary certification authority
PIN	personal identification number
PKCS	Public Key Cryptography Standards
PKI	public key infrastructure
RDN	Relative Distinguished Name
RPA	Relying Party Agreement
RSA	a cryptographic system (*see* definitions)
SAFESCRYPT	Safescrypt Ltd
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
SSP	Safescrypt Security Procedures
URL	uniform resource locator
WWW or Web	World Wide Web
X.509	the ITU-T standard for certificates and their corresponding authentication framework

2. SAFESCRYPT CERTIFICATION INFRASTRUCTURE

This section explains the regulatory environment in India, the architecture underlying the distribution of Safescrypt's India public certification services, as well as certificate classes, certificate extensions, time stamping, and the Safescrypt repository.

2.1 Regulatory Background in India:

India has enacted and brought into force the Indian Information Technology Act 2000 ("IT Act") <www.mit.gov.in>> in June 2000 thereby providing the required impetus for the growth of ecommerce in India. Among numerous issues, the IT Act awards evidentiary status to Digital Signatures in the Indian Courts of Law in lieu of physical signatures. The Digital Signature certificates that enjoy evidentiary status have to be issued by a Certifying Authority (CA) licensed under the IT Act..

To award licenses to CA's and manage the associated functions, amongst other things, the Controller of Certifying Authorities (CCA) has been set up as a statutory authority under the IT Act. An integral part of the CCA's function is to certify the various public keys used by licensed CA's to offer their services. For this purpose, the CCA is in the process of creating his own set of keys, known as the Controller's keys, that he will use to certify every CA's public keys. The Licensed CA's shall operate and conduct the activities of issue of Digital Signature Certificates including through IAs and others in the CA's PKI hierarchy pursuant to the authority vested in the CA's by the Licence granted by the CCA and further the root keys certified by the CCA. The Digital Signature Certificates so issued would enjoy evidentiary value as provided in the IT Act.

It should, however, be noted here that the entire IT Act is related only to signature certificates. However, PKI, in general, is a broader concept and various types of certificates are used for various purposes, not restricted merely to the function of "digital signing". Some certificates are used for encryption, not signing (for example, SSL certificates), while some others are issued to devices and organizations and NOT to individuals. These types of certificates are typically outside the scope of the IT Act and hence outside the process of licensing.

2.2 Trust Infrastructure

Safescrypt's India public certification services (India PCS) are designed to support secure electronic commerce and other general security services to satisfy users' technical, business, and personal needs for digital signatures and other

network security services. To accomplish this, Safescrypt-authorized issuing authorities (IA's – *see* definitions) serve as trusted third parties, issuing, managing, suspending, and revoking certificates in accordance with published practices. The term "IA" is a defined term within Safescrypt's India PCS. Of particular relevance, the term "IA" would cover the Enterprise CA that issue, suspends, or revokes a certificate. With prior approval by Safescrypt, an IA may delegate the responsibility to evaluate and approve or reject certificate applications to one or more LRAs not owned or operated by the IA under CPS § 2.3.3. When such delegation occurs and where the context requires, the term "IA" in this CPS shall include such LRAs with respect to the delegating IA's obligations, representations, warranties, and disclaimers."

The management and administrative functions of Safescrypt's India PCS are established to accommodate a large, public, and widely distributed community of users with diverse needs for communications and information security. To assure users that Safescrypt services are substantially uniform, a general statement of the management and administrative practices used to protect the integrity of Safescrypt's INDIA PCS is described in the CPS. As a result of such practices, Safescrypt's INDIA PCS accommodate a large and geographically dispersed community, enhancing users' trust in these services. *The various logical entities of the system implementation of the INDIA PCS are described in India CPS § 2.7.*

2.2.1 General Discussion of Certificate Issuance and Management

An IA acts as a trusted third party to facilitate the confirmation of the relationship between a public key and a named entity (*see* definition for "naming"). Such confirmation is expressly represented by a certificate – a message which is digitally signed and issued by an IA (*see* India CPS § 2.7). The high-level management of this certification process includes registration, naming, appropriate applicant authentication, issuance, revocation, suspension, and audit-trail generation. Naming may be performed principally by Safescrypt or by another party. Naming of subscribers includes a registration process distinct from that used for certificate management which determines when certificates are valid and operational.

Safescrypt currently supports two distinct levels of India public certification services. Each level, or class, of certificate provides specific functionality and security features. Certificate applicants choose from this set of service qualities according to their needs; they must specify which class of certificate they desire. Depending on the class of certificate desired, certificate applicants may apply electronically or in writing to an IA, or they may be required to apply in person by contacting a local registration authority (LRA). Each certificate issued by an IA corresponds to a specific PCS trust level. There may be many IA's issuing

certificates for a given trust level; these IA's may be differentiated by value-added services and practices suitable for differing communities.

In response to a certificate application, a certificate is then issued to the certificate applicant, or a draft of the certificate contents is sent to the certificate applicant. The certificate applicant must review the certificate or draft, determine its suitability for the certificate applicant's intended purpose, and, if satisfied, accept the certificate via the certificate registration process. The new subscriber agrees to be bound by the Subscriber Agreement and the continuing obligations of this CPS.

Certificate management also includes the deactivation of certificates and the decommission of the corresponding private keys, through a process involving the revocation and suspension of certificates. Additional IA services may include the listing, distribution, publication, storage, and retrieval of certificates in accordance with their particular intended use.

2.2.2 Security Services

Safescrypt's INDIA public certification services support a variety of security mechanisms to protect communications and information assets. Certificates alone however, do not constitute such a mechanism. Rather, Safescrypt's INDIA PCS provide a framework within which security services may be used by other communicating parties. This framework uses digital signatures and their verification to facilitate the protection of communication and computer-based trade and commerce over open data networks and provides a means for determining whether security services are in fact providing the intended assurances.

Certificate-based security services may be used to counter threats to security in a user-defined environment. Users select security mechanisms, security technology, security service agreements, and INDIA PCS suitable for the users' anticipated levels of risk, to protect users' communications environments from compromise.

Safescrypt's INDIA PCS currently use the RSA public key system for all certification-related purposes. However, Safescrypt is committed to supporting other digital signature standards as market demand materializes for alternatives.

2.2.3 INDIA PCS Domain Administration

Safescrypt's India PCS are administered in such a way that certain India PCS activities may be performed by parties other than Safescrypt. Uniform quality of service is maintained, despite functional and physical distribution of service

provision. The underlying principle of domain administration relies upon a strict delegation of authority. To accomplish this, Safescrypt relies upon decentralized, auditable IA agreement for the performance of specific published practices.

Each IA is authorized by a superior IA to perform certain PCS in a prescribed manner. Each IA also acts as an LRA unless it delegates such responsibility. Some of these functions concern the creation of IA's, while others concern the execution of authorized procedures by an IA once a superior IA has granted approval. To enhance uniformity of INDIA PCS, superior IA's delegate specific duties. Safescrypt's administration policies ensure that autonomous parties agree to execute practices, including the issuance and management of certificates, in a manner that will maintain the uniformity of Safescrypt's INDIA PCS.

2.4 Certificate Classes

Safescrypt currently supports two distinct certificate classes within its India PCS. Safescrypt reserves the right to introduce more classes than what has been specified herein and this India CPS shall be appropriately amended as and when such classes are introduced. Each class provides for a designated level of trust. The following subsections describe each certificate class. Also, further detail is provided in Table 2 (Certificate Attributes Affecting Trust).

THE DESCRIPTIONS FOR EACH CERTIFICATE CLASS (INCLUDING WITHIN TABLE 2, BELOW) REFLECT APPLICATIONS AND COMMUNICATIONS SYSTEMS THAT HAVE BEEN OR ARE IN THE PROCESS OF BEING IMPLEMENTED BY USERS. THEY DO NOT REPRESENT AN ENDORSEMENT OR RECOMMENDATION BY SAFESCRYPT OR BY ANY IA OR ANY OTHER PERSON ACTING IN THE HEIRARCHY FOR ANY PARTICULAR APPLICATION OR PURPOSE, AND THEY MUST NOT BE RELIED UPON AS SUCH. USERS MUST INDEPENDENTLY ASSESS AND DETERMINE THE APPROPRIATENESS OF EACH CLASS OF CERTIFICATE FOR ANY PARTICULAR PURPOSE.

2.4.1 Class B Certificates

Description: Class B certificates are currently issued to individuals only. Class B certificates confirm that the application information provided by the subscriber does not conflict with information in consumer trustworthy databases. Class B certificates are typically used primarily for intraorganizational and interorganizational E-mail; small, "low-risk" transactions; personal/individual E-mail; password replacement; and on-line subscription services. Safescrypt also

supports different types of specialized-use Class B certificates that may also facilitate the provision of special benefits by certain third-party service providers such as Web site hosts when a certificate applicant optionally submits Registration Field Information in the certificate application during enrollment, and such information is then made available to third party service providers via the subscriber's certificate.

Following the on-line submission of a Class B subscriber agreement to a Safescrypt Class B local registration authority (LRA), pertinent certificate applicant enrollment data is confirmed against third-party databases. Based upon such confirmation, the LRA will either approve or reject the application (*see* CPS § 5 – Validation of Certificate Applications). Upon such approval, a postal address confirmation procedure is invoked by the IA (*see* CPS § 5.1.4) **except for certificates issued by non-Safescrypt organizational LRAs.**

Assurance level: Class B certificates may provide reasonable, assurance of a subscriber's identity, based on a process that compares the applicant's name, address, and other personal information on the certificate application against widely referenced or trustworthy proprietary databases. Confirmation may be based upon Safescrypt proprietary matching criteria of third-party databases against the information in the application or alternative procedures that provide a comparable level of assurance.

ALTHOUGH SAFESCRYPT'S CLASS B IDENTIFICATION PROCESS IS A METHOD OF AUTHENTICATING A CERTIFICATE APPLICANT'S IDENTITY, IT DOES NOT REQUIRE THE APPLICANT'S PERSONAL APPEARANCE BEFORE A TRUSTED PARTY (SUCH AS A LOCAL REGISTRATION AUTHORITY OR NOTARY). CONSEQUENTLY, THE DECISION TO OBTAIN, USE, OR RELY UPON A CLASS B CERTIFICATE SHOULD TAKE INTO ACCOUNT ITS RELATIVE BENEFITS AND LIMITATIONS, AND THE CERTIFICATE SHOULD BE USED ACCORDINGLY. FURTHER INFORMATION ABOUT THIS AUTHENTICATION PROCESS IS ACCESSIBLE FROM THE SAFESCRYPT REPOSITORY AT https://www.safescrypt.com/India-Repository

When submitted, Registration Field Information contained in a class B certificate is considered NSI.

SUCH CLASS B CERTIFICATES WILL BE A DIGITAL SIGNATURE CERTIFICATE UNDER THE INFORMATION TECHNOLOGY ACT, 2000 (IT Act) AND THE LEGAL EFFECT, PRESUMPTION AND EVIDENTIARY VALUE OF DIGITAL CERTIFICATES AS PROVIDED IN THE IT ACT WILL BE APPLICABLE TO CLASS B CERTIFICATES.

2.4.2 Class C Certificates

Description: Class C certificates are issued to individuals.

To individuals – Class C certificates provide assurances of the identity of individual subscribers by requiring their personal (physical) appearance before a Class C LRA or its delegate (such as a notary public or a Bank Manager of specified level or designated Safescrypt employee).

SUCH CLASS C CERTIFICATES MENTIONED ABOVE WILL BE A DIGITAL SIGNATURE CERTIFICATE UNDER THE INFORMATION TECHNOLOGY ACT, 2000 (IT Act) AND THE LEGAL EFFECT, PRESUMPTION AND EVIDENTIARY VALUE OF DIGITAL CERTIFICATES AS PROVIDED IN THE IT ACT WILL BE APPLICABLE TO CLASS C CERTIFICATES.

Assurance level: Individual Class C certificate processes utilize various procedures to obtain probative evidence of the identity of individual subscribers. These validation procedures provide stronger assurances of an applicant's identity than Class C certificates. The practical uses and reliability of Class C certificates are bolstered by utilizing notaries public and / or a Bank Manager.

2.5 Certificate Class Properties

Table 2 describes certain properties of each certificate class. Each of the table's headings is described below.

	SUMMARY OF CONFIRMATION OF IDENTITY	IA PRIVATE KEY PROTECTION	CERTIFICATE APPLICANT AND SUBSCRIBER PRIVATE KEY PROTECTION	APPLICATIONS IMPLEMENTED OR CONTEMPLATED BY USERS - *SEE INDIA CPS § 2.4 DISCLAIMER & § 2.5.4.*
CLASS B	Unambiguous name and E-mail address search, plus enrollment information check plus address check	PCA & CA: trustworthy hardware	Encryption software (PIN protected) required	Individual and intra- and inter-company E-mail, on-line subscriptions, and password replacement

CLASS C	Same as Class B, plus personal presence & ID documents plus Class B ID check for individuals;	PCA & CA: trustworthy hardware	Encryption software (PIN protected) required; Hardware token recommended but not required	E-banking, corp. database access, personal banking, membership-based on-line services, content integrity services, E-commerce server, authentication of LRAAs; and strong encryption for certain servers

TABLE 2 - CERTIFICATE PROPERTIES AFFECTING TRUST

Each class of certificate is characterized by a different level of the following properties: confirmation of identity (such as through personal presence or investigation), IA private key protection (and assurance of appropriate use), certificate applicant and subscriber private key protection, and operational controls. While the certificates (and Safescrypt's supporting products and services) possess many other properties, those listed in Table 2 provide a framework for distinguishing some of their aspects that affect their relative trust. Each property is explained below:

2.5.1 Confirmation of Subscriber Identity

This refers to various actions taken by the IA to validate certificate applicants' identity and confirm the information they provide during the application process. The type, scope, and extent of confirmation depends upon the class of certificate, the type of applicant, and other factors. The particular confirmation methods and their rigor depend upon the class of certificate. Confirmation is further described in INDIA CPS § 5.

2.5.2 IA Private Key Protection

Each IA's private key is secured against compromise via trustworthy hardware products. See India CPS § 4.1 (Key Generation and Protection).

2.5.3. Certificate Subscriber (and Applicant) Private Key Protection

The secrecy of the private keys of certificate subscribers (and applicants) must be protected through the use of encryption software or hardware tokens (such as smart cards or PC cards) as specified in this INDIA CPS. *See* INDIA CPS § 4.1 (Key Generation and Protection) and the Key Protection FAQ at **https://www.safescrypt.com/India-Repository/PrivateKey_FAQ**. In this regard the subscribers are notified of the duties of subscribers specified in Sections 40 to 42 of the IT Act, 2000.

As Safescrypt observes new India PCS usage patterns, it will consider providing a specific infrastructure that responds to such patterns.

ISSUING AUTHORITIES NEITHER GENERATE NOR HOLD THE PRIVATE KEYS OF CERTIFICATE APPLICANTS OR SUBSCRIBERS. ALSO, ISSUING AUTHORITIES CANNOT ASCERTAIN OR ENFORCE ANY PARTICULAR PRIVATE KEY PROTECTION REQUIREMENTS OF ANY CERTIFICATE APPLICANT OR SUBSCRIBER.

2.5.4 Operational Controls

Operational controls refer to the organizational, human resources, and other management-oriented controls implemented for each class of certificate. Such controls include limits on who is permitted to obtain certificates, requirements concerning the training and education of IA personnel, policies establishing the separation of duties within IA's, documentation requirements, and prescribed procedures and audits. Many of these controls are identified in CPS § 3 (Foundation for Certification Operations).

2..6 Extensions and Enhanced Naming

2.6.1 Extension Mechanisms and the Authentication Framework

The INDIA PCS facilitate the use of X.509 v1, v2, and v3 certificates. X.509 v3 certificates expand the capabilities of v1 and v2, including the ability to add certificate extensions. This capability, a standard component of Safescrypt's INDIA PCS, augments the standard authentication services model.

2.6.2 Standard and Service-Specific Extensions

The X.509 "Amendment 1 to ISO / IEC 9594-8:1995" defines a number of extensions. These provide various management and administrative controls useful for large-scale and multipurpose authentication. Safescrypt's INDIA PCS exploit a number of these controls for the purposes intended by X.509. (Note: X.509-compliant user software is assumed to enforce the validation requirements of this CPS. IA's and Safescrypt cannot guarantee that such software will support and enforce these controls.)

In addition, this CPS allows users to define additional "private" extensions for purposes or modes of use specific to their application environment. Definitions for service-oriented extensions to and practices for handling such information during certificate application, approval, and issuance, are specified in the SP and in publicly available documents from relevant sponsoring organizations. Examples of private extensions implemented within the INDIA PCS for service-specific purposes include the software validation scheme exploited by some

versions of Microsoft Windows® software and the Netscape Communications Corporation's scheme for SSL security technology. *See* **http://microsoft.com/security**, and **http://home.netscape.com/newsref/ref/netscape-security.html.**

2.6.3 Identification and Criticality of Specific Extensions

The function of each extension is indicated by a standard OBJECT IDENTIFIER value (*see* definition for X.509). Additionally, each extension in a certificate is assigned a "criticality" true/false value. This value is set by the IA, possibly on the basis of information provided by the certificate applicant on the certificate application. This value must conform to certain constraints imposed by the organization responsible for the extension definition.

The presence of a criticality value of *true* upon a specific extension requires all persons validating the certificate to consider the certificate invalid if they lack knowledge of the purposes and handling requirements for any specific extension with criticality value of *true*. If the criticality value of such extension is *false*, all persons shall process the extension in conformance with the applicable definition when performing validation or else ignore the extension.

2.6.4 Certificate Chains and Types of IA's

Safescrypt's India PCS use chains of certificates. Each IA in a Safescrypt certificate chain performs particular procedures according to its assigned role in the Safescrypt PKI (*see* India CPS § 2.7). There are three generic roles an IA may play: root registration authority, IA for another IA, and IA for subscribers. An IA must be a subscriber of another IA. Where an IA is its own root, its self-signed public key shall conform to X.509 v1 format. It can potentially be trusted (based-upon out-of-band authentication mechanisms) without recourse to additional validation during verification of digital signatures (*see* India CPS § 8 – Use of Certificates). When *registered* by a root registration authority, however, the IA's certificate may contain extensions.

2.6.5 End-User Subscriber Certificate Extensions

IA's serving end-user subscribers may issue certificates containing extensions defined both by the X.509 Amendment 1 to ISO/IEC 9594-8:1995 and by sponsoring organizations such as Microsoft and Netscape (*see* CPS § 2.4.2). ISO-defined extensions used in the Safescrypt INDIA PCS, whose content is assigned by the applicable IA, are currently limited to the following extensions:

- basic constraints,
- key usage, and
- certificate policy.

Briefly, the use of these extensions control the process of issuing and validating certificates. Table 3 describes which extensions are present in particular certificates.

2.6.6 ISO-Defined Basic Constraints Extension

The basic constraints extension serves to delimit the role and position an IA or end-user subscriber certificate plays in a chain of certificates. For example, certificates issued to CAs and subordinate CAs contain a basic constraint extension that identifies them as IA certificates. End-user subscriber certificates contain an extension that constrains the certificate from being an IA certificate.

2.6.7 ISO-Defined Key Usage Extension

The key usage extension serves to limit the technical purposes for which a public key listed in a valid certificate may be used within the Safescrypt India PCS. IA certificates may contain a key usage extension that restricts the key to signing certificates, certificate revocation lists, and other data.

2.6.8 ISO-Defined Certificate Policy Extension

The certificate policy extension limits a certificate to the practices required by (or indicated to) relying parties. The certificate policy extension, as implemented in the India PCS, points its users to this India CPS and qualifies appropriate usages (*see* India CPS § 2.6.11).

2.6.9 Enhanced Naming and Safescrypt Extensions

All end-user subscriber certificates, except for certain S/MIME v1 certificates, contain an additional "Organizational Unit" field — an X.520 attribute — that contains a brief statement regarding liability and incorporates by reference the complete CPS, such as "**OU= Terms of use at https://www.safescrypt.com/rpa ©00** "(this references the primary URL of the Relying Party Agreement ("RPA"), notes that liability is limited, and includes a copyright notice). This or comparable information may be present in application-defined X.509 v3 extensions for display to users by "local" (non-Safescrypt vendor controlled) means. Note: the content of this Organizational Unit field is abbreviated because of the X.509 limitation of 64 bytes. This usage of an Organizational Unit field will be retired when functional and consistent use of X.509 v3 extensions become ubiquitous.

When digital signature-verifying software or hardware (collectively, "verifying software") facilitates the acceptance and use of v3 certificate extensions, the verifying software will display both a reference to the RPA and a set of extensions that describe important portions of it. If the verifying software

supports only limited or privately defined v3 extensions, the verifying software may then make use of those application-specific extensions, as appropriate, to equivalently disclose certain critical practice statement sections.

Figure 3 illustrates how Safescrypt has implemented this approach within v3 certificates. Key elements in the figure are explained below.

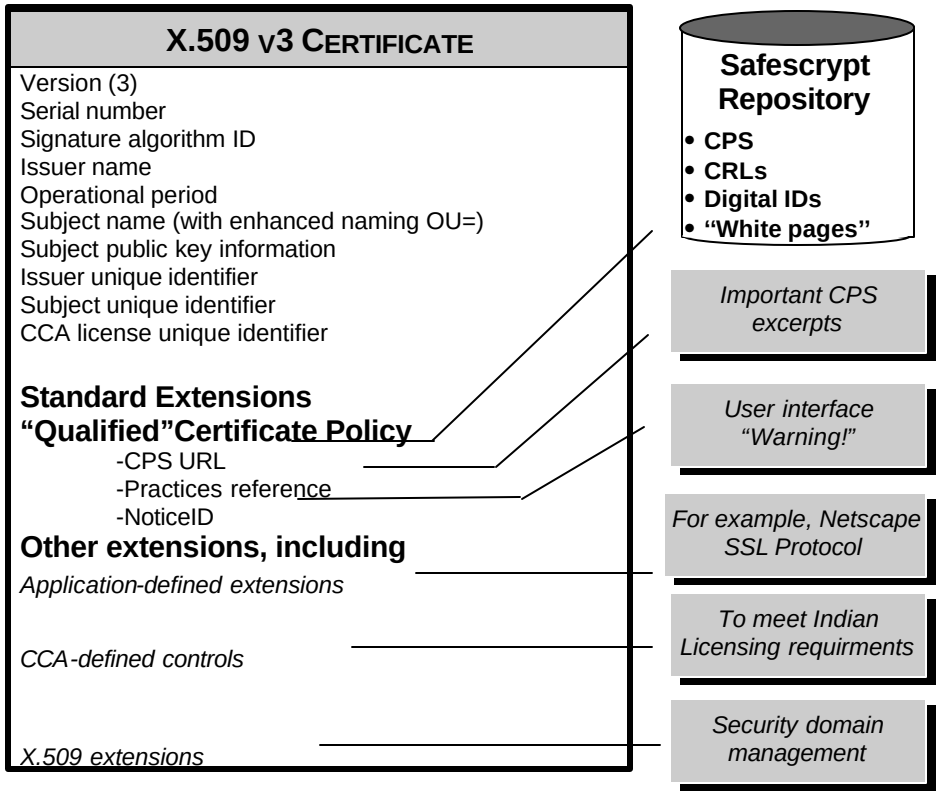

FIGURE 3 – CERTIFICATES AND INFORMATION INCORPORATED BY REFERENCE

2.6.11 Incorporation by Reference

Extensions and enhanced naming are either fully expressed within a certificate or they are at least partially expressed in a certificate with the balance expressed in an external document incorporated by reference in the certificate (*see* definition of **INCORPORATE BY REFERENCE**).

The information contained in the enhanced Organizational Unit field is also present in the **CertificatePolicy** extension, when present in a certificate. This CPS constitutes a "certificate policy" as defined by X.509 Amendment 1 to ISO / IEC 9594-8:1995. Safescrypt, acting as a policy-defining authority, has assigned to the CPS an object identifier value which is present in the **CertificatePolicy** extension. The definition of this "certificate policy" requires the use of a policy qualifier

which Safescrypt has defined to include pointer values, warnings, liability limitations, and warranty disclaimers as described in Table 3 and as follows.

2.6.12 Pointers to CPS

Both computer-based pointers (using URLs or other identifiers and mechanisms) and English (human-readable) text or pointers are used, so that certificate users can easily locate and access the CPS and other relevant information.

2.6.13 Warnings, Liability Limitations, and Warranty Disclaimers

Each certificate includes a brief statement detailing applicable limitations of liability and disclaimers of warranty, with a pointer to the full text of such warnings, limitations, and disclaimers in the India CPS. Alternatively, such information may be displayed by a certificate-viewing function, possibly following a hypertext link to a message accessible by users or agents, rather than being embedded in the certificate. In addition the certificate shall contain such statements and particulars as may be required under the IT Act, 2000 and Rules and Regulations issued thereunder.

The methods of communicating information (to be displayed by a user) are as follows: an enhanced naming organizational unit attribute; a Safescrypt standard qualifier to a Safescrypt–registered certificate policy (using a standard v3 extension); and other vendors' registered extensions (such as a Netscape–registered "Comment" extension).

An "enhanced" organizational unit attribute contains the string "**OU= Terms of use at https://www.safescrypt.com/rpa (c)02**", or similar string.

Table 3 describes the typical contents of certificate extensions and the qualifier types defined for the Safescrypt CPS certificate policy identifier.

NAME/CERT. EXTENSION FIELDS	PURPOSE & DESCRIPTION	ACCOMPANYING ENGLISH (OR OTHER HUMAN-READABLE) TEXT
General Extensions for CA and Subordinate CA: ----------		
basicConstraints	*See* India CPS § 2.6.6	Non Critical cA = TRUE
keyUsage	*See* India CPS § 2.6.7	Non Critical KeyCertSign (Bit 5 set) cRLSign (Bit 6 set)
General Extensions for End-User Subscriber: ----------		
basicConstraints	*See* India CPS § 2.6.6	Non Critical cA = FALSE
certificatePolicy	*See* India CPS § 2.6.8	Non Critical *See* CPS § 2.6.13
Safescrypt standard qualifier – Practices Reference	Contains text referring to the Safescrypt repository (and in future versions of this CPS, certain non-Safescrypt repositories), which holds the Safescrypt CPS, CRL, and other information.	"**This certificate incorporates by reference, and its use is strictly subject to, the Safescrypt Certification Practice Statement (CPS), available in the Safescrypt repository at: https://www.safescrypt.com; by E-mail at CPS-requests@safescrypt.com; or by mail at Safescrypt ltd, 667-668, Keshava Towers, 11th Main, 4th Block, Jayanagar, Bangalore – 560 011. Tel : +91-80-6555093 / +91-80-6555104 Copyright (c)2002 Safescrypt. All Rights Reserved. CERTAIN WARRANTIES DISCLAIMED AND LIABILITY LIMITED."**.
Safescrypt standard qualifier – cpsURLs	A single uniform resource locator indicating the source of this CPS.	**"https://www.safescrypt.com/CPS"** or similar URL
Safescrypt standard	An object identifier referring to a registered	Registered string of value "**WARNING: USE OF THIS CERTIFICATE IS STRICTLY SUBJECT TO THE**

qualifier – NoticeID	string whose content indicates information about warnings, cautions, warranty disclaimers, and limitations of liability regarding the use of Safescrypt INDIA PCS certificates. It is intended to be displayed with every certificate within the user agent (*e.g.*, computer or terminal) certificate viewing function (but it is not embedded in any certificate).	**SAFESCRYPT CERTIFICATION PRACTICE STATEMENT. THE ISSUING AUTHORITY DISCLAIMS CERTAIN IMPLIED AND EXPRESS WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND, WILL NOT BE LIABLE FOR CONSEQUENTIAL, PUNITIVE, AND CERTAIN OTHER DAMAGES. SEE THE CPS FOR DETAILS.**"
Safescrypt standard qualifier – NSINotice	An object identifier referring to a registered string whose content indicates that the certificate contains data for which the IA provides no assurances of accuracy.	Registered string of value "**Contents of the Safescrypt registered nonverifiedSubjectAttribute extension value shall not be considered as information confirmed by the IA.**"

TABLE 3 – SAFESCRYPT CERTIFICATE EXTENSIONS

Alternatively a certificate contains, in a User Notice certificate policy qualifier, a reference to the following text which is displayed by certain products:

> **This certificate incorporates the Safescrypt India Certification Practice Statement (India CPS) by reference. Use of this certificate is governed by the India CPS.**
>
> **The India CPS is available in the Safescrypt repository at** https://www.safescrypt.com/India-Repository**; by E-mail at CPS-requests@safescrypt.com; and by mail at Safescrypt Ltd, 667-668, Keshava Towers, 11th Main, 4th Block, Jayanagar, Bangalore – 560 011. Attn: Practices and External Affairs. Tel : +91-80-6555093 / +91-80-6555104 Fax: 91-80-6555300. THE CPS DISCLAIMS AND LIMITS CERTAIN LIABILITIES, INCLUDING CONSEQUENTIAL AND PUNITIVE DAMAGES. THE CPS ALSO INCLUDES CAPS**

ON LIABILITY RELATED TO THIS CERTIFICATE. SEE THE CPS FOR DETAILS.

This CPS and this certificate are copyrighted.

2.7 Safescrypt PKI Hierarchy

Safescrypt's India public certification services are implemented within a PKI-entity hierarchy composed of the following IAs:

- Public primary certification authorities (PCAs) – that serve as the core self - signed root keys that help Safescrypt offer the India PCS. **These are Self Signed Root Keys.**
- Safescrypt CAs (CA under each PCA), and
- other CAs (including subordinate CAs) authorized by Safescrypt or an authorized IA to operate within the Safescrypt INDIA PCS, consistent with this CPS.

Note : many components of this hierarchy are yet to be implemented.

Within the PKI-entity hierarchy, IA's are interrelated via the relationship of "location subordinate to," which indicates that one IA serves on behalf of another. An IA shall issue IA certificates using either general or enhanced authentication procedures (for IA validation), depending upon the certificate class of the end-user subscriber certificates issued by the last IA in the hierarchy.

In addition, IA's may delegate certain registration functions to one or more LRAs. The Safescrypt India PKI also includes the Safescrypt naming authority and Safescrypt repository.

2.7.1 Public Primary Certification Authorities (PCAs)

The PCAs serve as the highest-level active certification entities within the Safescrypt INDIA PCS. The PCAs issue, suspend, and revoke certificates for all CAs within Safescrypt's INDIA PCS. Each PCA is owned and operated by Safescrypt. **Each PCA is a self signed root**

Each third generation PCA's initial key size is 2048 bits. A trustworthy hardware device (FIPS 140-1 Level 3 certifiable) is used to create, protect, and destroy each PCA's private key. The purposes, assurances, services, and obligations of each PCA (and the rights and responsibilities of its certificate applicants, subscribers, certificate recipients, relying parties, and CAs / subordinate CAs within its certification chain) are presented in this CPS.

Cross-certification between Safescrypt PCAs and comparable entities within non-Safescrypt PKIs, as it relates to Safescrypt's INDIA PCS, is permitted if (I) Safescrypt determines that the non-Safescrypt entity provides at least a comparable function and level of assurance and trustworthiness, (ii) cross-certification is expected to enhance the value of Safescrypt's certificates to Safescrypt subscribers, (iii) both entities have executed an appropriate Safescrypt cross-certification agreement, (iv) Safescrypt and the non-Safescrypt entity have issued certificates to the other, (v) each party has accepted such certificate, and (vi) revocation and repository procedures are agreed upon between the parties.

2.7.2 Certification Authorities (CAs)

Each CA is subordinate to one PCA and operates in accordance with this CPS and any specific constraints imposed by that PCA (which are consistent with this CPS). Class B and C CAs may issue, manage, and revoke end-user subscriber certificates, as permitted by this CPS. Class B and C CAs may also issue IA certificates to subordinate CAs, at Safescrypt's sole discretion. Subordinate CAs may issue, manage, and revoke end-user subscriber certificates, as permitted by this CPS.

Each CA's (and subordinate CA's) initial key size is 2048 bits. A trustworthy hardware device (FIPS 140-1 Level 3 certifiable) is used to create, protect, and destroy the private keys of Class B, and C CA's. CA's and subordinate CA's are generally owned and operated by Safescrypt, but upon agreement between Safescrypt and the other entity, Safescrypt may authorize non-Safescrypt CA's and their subordinate CAs (or non-Safescrypt subordinate CA's that are subordinate to a Safescrypt CA) to join Safescrypt's INDIA PCS (*see* CPS § 3.1).

2.7.3 Local Registration Authorities (LRAs) and LRA Administrators (LRAAs)

Local registration authorities (LRAs) are entities that evaluate and approve or reject certificate applications. LRAs also have the authority to approve the revocation (or where authorized, suspension) of certificates. LRAs may employ LRA Administrators (LRAAs) to perform the work of the LRA. LRAs operate on behalf of and (within the context of the CPS) under the exclusive authority of a single IA (the PCA or CA that actually issues the certificates). An IA may have more than one LRA.

Without otherwise limiting their authority, LRAs may rely upon the following for confirming certificate applicant information: (I) notarial acts that reasonably appear to be performed in good order if it is coupled with a letter from the Manager or above of the recognised Bank with which the subscriber ordinarily conducts his banking operations. and (ii) well-recognized forms of identification, such as passports and driver's licenses.

Non-Safescrypt organizational LRAs are LRAs not affiliated with Safescrypt that are authorized to approve the issuance and revocation of certificates to affiliated individuals within the LRA's organization. For example, a company may become a non-Safescrypt organizational LRA in order to approve (or disapprove) the issuance of certificates to its own employees and other affiliated individuals and may not approve the issuance of certificates to the general public.

Certificates issued by non-Safescrypt organizational LRAs may only be issued to individuals whose affiliation with the LRA is ascertainable by the LRAA via appropriate internal documentation (such as human Resources (HR) employee and independent contractor rolls). All certificates issued as a result of a non-Safescrypt organizational LRA's approval of a certificate application shall contain a distinguished name that states the affiliation of its subject. Non-Safescrypt organizational LRAs are exclusively responsible for approving or not approving certificate applications.

LRAA requirements are presented in CPS § 3.20, below.

2.7.4 Naming Authority

A naming authority, called the Safescrypt naming authority, coordinates the issuance of relative distinguished names (RDNs) for all Safescrypt IA's. The Safescrypt naming authority may also specify naming conventions for subject names within the Safescrypt repository which may vary by certificate class and by IA. These naming conventions may also vary between issuance and re-issuance / re-enrollment. Non-Safescrypt IA's must either use the Safescrypt naming authority, or establish or otherwise use a naming authority whose procedures are not in conflict with those of the Safescrypt naming authority and do not register RDNs by the Safescrypt naming authority.

2.7.5 Safescrypt Repository

The Safescrypt repository is a publicly available collection of databases for storing and retrieving certificates and other information related to certificates. All IA's must utilize the Safescrypt repository as the primary and official repository for all Safescrypt INDIA PCS purposes. The Safescrypt repository's content includes but is not limited to the following: certificates, CRLs and other suspension and revocation information, current and prior versions of the Safescrypt CPS, and other information as prescribed by Safescrypt from time to time.

The Safescrypt repository will not alter any certificate or any notice of certificate suspension or revocation it receives in specified format from an IA, and it will accurately represent the content of such materials.

2.7.6 Publication by the Safescrypt Repository

The Safescrypt repository will act promptly to publish certificates, amendments to the CPS, notices of certificate suspension or revocation, and other information, consistent with this CPS and applicable law. The Safescrypt repository is accessible at https://www.safescrypt.com/India-Repository and by other communications methods as may be designated by Safescrypt from time to time.

Safescrypt may publish both within and outside of the Safescrypt repository a subscriber's certificate and CRL-related data. This CPS prohibits accessing of any data in the repository (or data otherwise maintained by an IA) that is declared confidential by the CPS and / or by the Safescrypt repository, unless authorized by Safescrypt.

Safescrypt will also replicate from time to time with its repository data with the repository hosted by the CCA for India. The frequency would be as determined by the CCA.

2.8 Banker's Certificate

Outside of Safescrypt's PK I, the subscriber's banker, if any , in his or her official capacity as a banker, do serve a reasonable identity confirming person for the persons banking with him and will be in a position to certify the existence of such person with address, the business engaged in by the person and some other essential details. The Banker will have to be of the grade of a Manager or above in the Bank. Safescrypt reserves the right to recognize and subsequently rely upon the bank and consequently the Bank Manager.

3. FOUNDATION FOR CERTIFICATION OPERATIONS

This section establishes the foundation and controls for trustworthy INDIA PCS operations. It includes the operating requirements for Safescrypt's INDIA PCS, including record keeping, auditing, and personnel requirements. It also presents the obligations of an IA upon the termination or cessation of its operations.

NOTE: CERTIFICATE APPLICATION PROCEDURES ARE PRESENTED IN CPS § 4, BELOW.

3.1 Prerequisites for Approval as a Non-Safescrypt CA within the INDIA PCS

Safescrypt's INDIA PCS are founded upon IA's operated by Safescrypt. In Safescrypt's discretion, other trustworthy entities may participate in Safescrypt's INDIA PCS as CAs or subordinate CAs. To achieve uniform levels of trustworthiness throughout the INDIA PCS, non-Safescrypt CAs and subordinate CAs agree to follow the various control requirements of this CPS.

3.1.1 Non-Safescrypt CA's

Enterprise Customers of Safescrypt, which are subscribers of CA Certificates, are not required to complete formal Certificate Applications. Instead, they enter into a contract with Safescrypt. CA Certificate Applicants are required to provide their credentials as required by CPS § 3.1.2 to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create Customer's CA key pair, the applicant shall cooperate with Safescrypt to determine the appropriate distinguished name and the content of the Certificates to be issued to the applicant. For these CAs, certificate requests are created and approved by authorized Safescrypt personnel through a controlled process that requires the participation of multiple trusted individuals.

3.1.2 Authentication of the Identity of CAs

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

Enterprise Customers enter into an agreement with SafeScrypt before becoming CAs. SafeScrypt authenticates the identity of the prospective Enterprise Customer before final approval of its status as CA by performing the checks required for the confirmation of the identity of organizational end-user

Subscribers specified in this CPS, except that instead of a Certificate Application, the validation is of an application to become an Enterprise Customer. Optionally, SafeScrypt may require the personal appearance of an authorized representative of the organization before authorized SafeScrypt personnel.

3.2 Safescrypt's Right to Investigate Compromises

IA's, Safescrypt, and any other entity designated by Safescrypt, may, but are not obligated to, investigate all compromises to the furthest extent of the law. By submitting a CA application (*see* INDIA CPS § 3.1) or certificate application (*see* INDIA CPS § 4), all applicants authorize the undertaking and scope of such investigations and agree to assist in determining all facts, circumstances, and other pertinent information that the IA, Safescrypt, and and any other entity designated by Safescrypt deem appropriate and consistent with the INDIA CPS, provided that such investigations comply with all applicable privacy and data protection laws. Investigations of IA's may include but are not necessarily limited to interviews, the review of applicable books, records, and procedures, and the examination and inspection of relevant facilities. Investigations of certificate applicants and subscribers may include but are not necessarily limited to interviews and requests for and evaluation of documents. IA, Safescrypt and any other entity designated by SafeScrypt may require the applicant to provide such additional identification and documents for the investigation and verification as they may be deemed appropriate and the applicant shall make available the same.

3.3 Conformance to this CPS

IA's, LRAs, and the Safescrypt repository shall conform to this INDIA CPS in performing their respective services.

3.4 Trustworthiness

IA's, LRAs, and the Safescrypt repository shall utilize only trustworthy systems in performing their respective services.

3.5 Financial Responsibility

IA's shall have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the risk of liability to subscribers and recipients of certificates and other persons who may rely on the certificates and time stamps they issue. IA's shall also maintain insurance coverage for errors and omissions.

3.6 Records Documenting Compliance

IA's shall maintain and make available to Safescrypt upon request, records in a trustworthy fashion, including

(i) documentation of their own compliance with the CPS, and

(ii) documentation of actions and information that is material to each certificate application and to the creation, issuance, use, suspension, revocation, expiration, and renewal or re-enrollment of each certificate it issues. These records shall include all relevant evidence in the IA's possession regarding

- the identity of the subscriber named in each certificate
- the identity of persons requesting certificate suspension or revocation
- other facts represented in the certificate,
- time stamps, and
- certain foreseeable material facts related to issuing certificates.

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete. An IA may require a subscriber or its agent to submit documents to enable the IA to comply with this section.

3.7 Time Stamping

Time stamping is intended to enhance the integrity of Safescrypt's INDIA PCS and the trustworthiness of certificates and to contribute to the nonrepudiation of digitally signed messages. Time stamping creates a notation that indicates (at least) the correct date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation. All time stamps reflect Greenwich mean time (GMT) and adopt the Universal Time Conventions (UTC). For purposes of this CPS, any two-digit year in the range 00-69 means 2000-2069, and in the range 70-99 means 1970-1999.

The following data shall be time stamped, either directly on the data or on a correspondingly trustworthy audit trail, by the applicable IA's:

- certificates,
- CRLs and other suspension and revocation database entries,
- each version of the CPS,
- customer service messages, and
- other information, as prescribed by this CPS.

Note: Cryptographic-based time stamping will be incrementally implemented by Safescrypt IA's for all relevant messages.

3.8 Records Retention Schedule

IA's shall retain in a trustworthy fashion records associated with Class B certificates for at least five (5) years and records associated with Class C certificates for at least thirty (30) years after the date a certificate is revoked or expires. Such records may be retained as either retrievable computer-based messages or paper-based documents.

3.9 Audit

IA's shall implement and maintain trustworthy systems to preserve an audit trail for all material events, such as key generation and certificate application, validation, suspension, and revocation. A certified public accountant with demonstrated expertise in computer security or an accredited computer security professional shall audit the operations of each IA and corresponding LRAs at least annually, at the sole expense of the audited entity, to evaluate its compliance with this India CPS and other applicable agreements, guidelines, procedures, and standards. Non-Safescrypt IA's shall promptly submit audit reports concerning such audits to Safescrypt.

Safescrypt's receipt of such third-party audit reports constitutes neither endorsement nor approval on the part of Safescrypt of the content, findings, and recommendations of such reports. Safescrypt may review such reports to protect Safescrypt's India PCS. Since Safescrypt is not the author of such audit reports and is therefore not responsible for their content, Safescrypt does not express any opinion on such audit reports and shall not be held responsible for any damages to anyone resulting from Safescrypt's reliance on such audit reports.

3.10 Contingency Planning and Disaster Recovery

IA's shall implement, document, and periodically test appropriate contingency planning and disaster recovery capabilities and procedures, consistent with this India CPS.

3.11 Availability of IA Certificates

IA's shall make copies of their own certificates (*i.e.*, those in which the IA is the subject) and any revocation data (where applicable) available to any person who has and desires to duly verify a digital signature that is verifiable by reference to such a certificate.

3.12 Publication by Issuing Authorities

IA's must publish their certificate, revocation data, and this India CPS.

3.13 Confidential Information

The following information shall be considered received and generated in confidence by Safescrypt and the applicable IA and may not be disclosed except as provided below:

- CA application records, whether approved or disapproved,
- Subscriber agreements and certificate application records (except for information placed in a certificate or repository per this CPS),
- transactional records (both full records and the audit trail of transactions),
- INDIA PCS audit trail records created or retained by Safescrypt or an IA,
- INDIA PCS audit reports created by Safescrypt, an IA, the Safescrypt repository (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- contingency planning and disaster recovery plans, and
- security measures controlling the operations of IA hardware and software and the administration of certificate services and designated enrollment services.

Neither IA's nor Safescrypt shall disclose or sell applicant names or other identifying information, and neither shall share such information, except in accordance with this CPS. Note, however, that the Safescrypt repository shall contain certificates, as well as revocation and other certificate status information (*see* CPS §§ 2.7.5, 2.76 regarding the Safescrypt repository).

Voluntary Release / Disclosure of Confidential Information.
Neither IA's nor Safescrypt shall release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release from (a) the person to whom the IA or Safescrypt owes a duty to keep such information confidential and if such a request is made in addition thereto from the person requesting confidential information (if not the same person); or (b) pursuant to an order from the Court or Tribunal or any Government or public authority having the power to compel the disclosure. The IA or Safescrypt may require that the requesting person pay a reasonable fee before disclosing such information.

3.14 Personnel Management and Practices

IA's shall formulate and follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. Such practices shall be consistent with this India CPS.

3.14.1 Trusted Positions

All employees, contractors, and consultants of an IA (collectively, "personnel") that have access to or control over cryptographic operations that may materially affect the IA's issuance, use, suspension, or revocation of certificates, including access to restricted operations of the Safescrypt repository, shall, for purposes of this India CPS, be considered as serving in a trusted position. Such personnel include, but are not limited to, customer service personnel, system administration personnel, designated engineering personnel, and executives who are designated to oversee the IA's trustworthy system infrastructures.

3.14.2 Investigation and Compliance

IA's shall conduct an initial investigation of all personnel who are candidates to serve in trusted positions to make a reasonable attempt to determine their trustworthiness and competence. IA's shall conduct periodic investigations of all personnel who serve in trusted positions to verify their continued trustworthiness and competence in accordance with Safescrypt's personnel practices or equivalent.

3.14.3 Removal of Persons in Trusted Positions

All personnel who fail an initial or periodic investigation shall not serve in a trusted position. The removal of any person serving in a trusted position shall be at the sole discretion of the applicable IA (or Safescrypt, in the case of Safescrypt personnel).

3.15 Accreditations

3.15.1 Approval of Software and Hardware Devices

All INDIA PCS-related hardware and software shall be approved by Safescrypt, an authorized Safescrypt consultant, or other recognized authority (as designated from time to time by Safescrypt), as appropriate.

3.15.2 Personnel in Trusted Positions

All personnel serving in trusted positions shall be accredited by a recognized external accreditation organization, as appropriate. This provision does not include members of the board of directors of Safescrypt or of any IA, except for such persons serving in an operational capacity in the INDIA PCS.

3.15.3 Organizational Good Standing

An IA shall be in good standing with (and, where applicable, accredited, certified, or licensed by) applicable agencies and authorities whose rules and regulations materially affect IA trustworthiness and as required by law or contract.

3.16 IA Key Generation

An IA shall securely generate and protect its own private key(s), using a trustworthy system, and take necessary precautions to prevent its loss, disclosure, modification, or unauthorized use.

3.17 Secret Sharing

An IA shall use secret sharing (*see* definitions), using authorized secret share holders, to enhance the trustworthiness of their private key(s) and provide for their key's recovery, as described below.

ENTITY	REQUIRED SECRET SHARES TO ENABLE IA'S PRIVATE KEY TO SIGN END-USER SUBSCRIBER CERTIFICATES	REQUIRED SECRET SHARES TO SIGN IA'S CERTIFICATE	TOTAL SECRET SHARES DISTRIBUTED	DISASTER RECOVERY SHARES* NEEDED | TOTAL	
Class B PCA	n / a	5	9	3	4
Class C PCA	n / a	5	9	3	4
Class B CA and subordinate Cas	2 (+1 CK)	3 (+1 CK)	6	2 (+1 CK)	3 (+1 CK)
Class C CA and subordinate Cas	2 (+1 CK)	3 (+1 CK)	6	2 (+1 CK)	3 (+1 CK)

*****In addition to the above-listed number of assigned secret shares required for CAs and subordinate CAs, a *common key* ("CK") is required (thus effectively increasing by one the total number of keys required for all CAs and subordinate CAs for secret sharing purposes). However, an assigned secret share can be used as a substitute for a common key. Common keys are used to keep certain hardware cryptomodules in operational mode without the security risk that results from leaving assigned secret shares in such cryptomodules (other than to enable them).

TABLE 4 – SECRET SHARE DISTRIBUTION

3.17.1 Hardware Protection

IA's must use approved trustworthy hardware cryptomodules for all operations requiring the use of their private key. The procedure for creating such private keys may be published in the Safescrypt repository.

3.17.2 Representations by IA

IA's must use approved trustworthy hardware cryptomodules for all operations requiring the use of their private key. The procedure for creating such private keys may be published in the Safescrypt repository.

3.17.3 Acceptance of Secret Shares by Secret Share Holders

For a secret share holder to accept a secret share, a majority of the designated secret share holders must have personally observed the creation, re-creation, and distribution of the share and its subsequent chain of custody.

Each secret share holder must receive the secret share within a physical medium, such as a Safescrypt-approved hardware token. Once the secret share holder is

satisfied that his or her inspection of the delivered secret share is complete, he or she shall acknowledge acceptance of the secret share by signing and returning to the applicable IA a secret share acceptance form provided by that IA.

3.17.4 Safeguarding the Secret Share

The secret share holder shall use trustworthy systems to protect the secret share against compromise. Except as provided in this India CPS, the secret share holder agrees that he or she shall not

- divulge, disclose, copy, make available to third parties, or make any unauthorized use whatsoever of the secret share,
- reveal (expressly or implicitly) that he or she, or any other secret share holder, is a secret share holder, or
- store the secret share in a location that fails to provide for its recovery in the event the secret share holder becomes incapacitated or unavailable (except when the secret share is being used for authorized purposes).

3.17.5 Availability and Release of Secret Shares

The secret share holder shall make the secret share available to authorized entities (listed in the secret share holder acceptance form) only when provided with proper authorization by an authenticated record (see next paragraph). In the event of a disaster situation (when declared by the secret share issuer), the secret share holder shall report to a disaster recovery site in accordance with instructions from the secret share issuer. Prior to traveling to any contingency / disaster recovery site and releasing the secret share, the secret share holder shall authenticate the declaration of the secret share issuer as specified on the secret share acceptance form (except where prohibited by law or legal process, such as concerning certain criminal investigations). This procedure will include the use of a challenge phrase (communicated from the secret share issuer to the secret share holder) to ensure that the secret share holder is not tricked into traveling to the wrong location thereby incapacitating the secret share issuer's ability to recover. At the disaster recovery site, the secret share holder shall physically deliver (in person) the secret share in order to participate in the disaster recovery procedure.

The secret share holder may rely upon any instruction, document, message, record, instrument, or signature he or she reasonably believes to be genuine, provided he or she authenticates such declaration of the secret share issuer in the manner provided by the preceding paragraph. The secret share issuer will provide the secret share holder with a sample set of all signatures to be used to authenticate the instructions of the secret share issuer.

3.17.6 Record Keeping by Secret Share Issuers and Holders

Secret share issuers and holders shall keep records of activities pertaining to all secret share materials. The secret share holder shall provide information regarding the status of the secret share to the secret share issuer or its designee upon authenticated request.

3.17.7 Secret Share Holder Liability

The secret share holder shall perform his or her obligations under this India CPS and must act in a reasonable and prudent manner in all respects. The secret share holder shall notify the secret share issuer of any loss, theft, improper disclosure, or compromise of the secret share immediately upon learning of it. The secret share holder is not responsible for failure to fulfill his or her obligations due to causes beyond his or her reasonable control but shall be liable for improper disclosure of secret shares or failure to notify the secret share issuer of improper disclosure or compromise through his or her fault, including negligence or recklessness.

3.17.8 Indemnity by Secret Share Issuer

The secret share issuer agrees to indemnify and hold harmless the secret share holder from all claims, actions, damages, judgments, arbitration fees, expenses, costs, attorney's fees, and other liabilities incurred by the secret share holder related to the secret share that are not caused or contributed to by the secret share holder's fault, including negligence, or recklessness.

3.18 Conformance to Operational Period Constraints

The CA applicant shall ensure that the operational period assigned to an IA certificate conforms to the restrictions imposed on that IA by the superior IA that establishes operational periods.

3.19 Security Requirements

3.19.1 Communication Security Requirements

All communications pursuant to this CPS among Safescrypt and the other parties in the INDIA PCS must use an application that provides appropriate security mechanisms commensurate with the attendant risks. Without limiting the generality of the foregoing, computer-based notices, corresponding notice acknowledgments, and any other communications affecting the security of the INDIA PCS shall also be appropriately secured.

3.19.2 Facilities Security Requirements

An IA shall operate trustworthy facilities that are in substantial conformance with the SP, or equivalent.

3.20 Local Registration Authority Administrator Requirements

LRAAs serve in trusted positions (*see* CPS § 3.14 – Personnel Management and Practices). The minimum requirements for an LRAA depend upon the class and affiliation of the certificates issued, based on the applications that an LRAA is authorized to approve. Note that certain non-Safescrypt organizational LRA requirements are less rigorous than requirements for a normal LRAA because the former does not issue certificates to the general public and therefore requires less experience in the general validation of identification documents. Rather, the non-Safescrypt organizational LRA bases its certificate approval decisions upon a simplified, internal list of authorized employees and other "affiliates" or other business records. LRAA requirements are presented in Table 5.

	Non-Safescrypt Organizational LRAA CLASS B	LRAA CLASS C
EDUCATION	No less than requirements for the company's human resources personnel handling company confidential employee records	At least 2 years of college or equivalent experience
TRAINING	Successful completion of on-line LRAA demonstration program and must be employed by the LRA for at least 3 months	Two weeks of LRAA apprenticeship and must be employed by the LRA for at least 3 months
ACCREDITATIONS	n/a - Must be an employee in good standing with his/her LRA	Must be an employee in good standing with his/her employer and LRA
INITIAL INVESTIGATION	Per applicable *trusted position* requirements (*see* CPS § 3.14.1)	Per *trusted position* requirements (*see* CPS § 3.14.1)
ONGOING INVESTIGATIONS	Annually (recommended)	Annually
BONDING	No	Yes
RECORD KEEPING	Yes, per CPS § 3.6. LRAAs not associated with a Safescrypt-owned or operated IA shall independently retain applicable records per CPS § 3.6	Yes, per CPS § 3.6

TABLE 5 – LRAA REQUIREMENTS

3.21 Termination or Cessation of IA Operations

The following obligations are intended to reduce the impact of a termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, and certain remedies.

3.21.1 Requirements Prior to Cessation

Before ceasing to act as an IA, an IA must:

(i) Notify its superior IA (and also Safescrypt, if the superior IA is not owned and operated by Safescrypt) of its intention to cease acting as an IA. Such

notice shall be made at least ninety (90) days before ceasing to act as an IA. The superior IA may require additional statements in order to verify compliance with this provision.

(ii) Provide to the subscriber of each unrevoked or unexpired certificate it issued ninety (90) days notice of its intention to cease acting as an IA.

(iii) Revoke all certificates that remain unrevoked or unexpired at the end of the ninety (90) day notice period, whether or not the subscribers have requested revocation.

(iv) Give notice of revocation to each affected subscriber, as detailed in India CPS § 9.

(v) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding certificates.

(vi) Make reasonable arrangements for preserving its records.

(vii) Pay reasonable restitution (not to exceed the certificate purchase price) to subscribers for revoking their certificates before their expiration date.

3.21.2 Reissuance of Certificates by a Successor IA

To provide uninterrupted IA services to its certificate applicants and subscribers, a discontinuing IA must arrange with another such authority, subject to the other IA's prior written approval, for reissuance of its outstanding subscriber certificates. In reissuing a certificate, the succeeding IA (not to be confused with a subordinate IA) is subrogated to the rights and defenses of the discontinuing IA and, to the extent agreed in writing between the discontinuing and succeeding IA, assumes all of its obligations and liabilities regarding outstanding certificates. Unless a contract between the discontinuing IA and a subscriber provides otherwise, and subject to the succeeding IA's written approval, the INDIA CPS will remain in effect under the succeeding IA as under the original IA.

The requirements of this subsection may be varied by contract, provided such modifications affect only the contracting parties.

3.22 Compliance with IT Act

The IA shall also duly comply with the requirements under the INFORMATION TECHNOLOGY ACT, 2000, the Rules and Regulations framed thereunder including and in particular the Information Technology (Certifying Authorities) Rules, 2000, Information Technology (IT) Security Guidelines and Security Guidelines for Certifying Authorities being Schedules II and III in the above Rules.

4. CERTIFICATE APPLICATION PROCEDURES

This section describes the certificate application process. It includes the requirements for key pair generation and protection and lists the information required for each class of certificate.

All persons (other than an IA) desiring a certificate shall contemporaneously complete the following general procedures for each certificate application:

- generate a key pair and demonstrate to the applicable IA that it is a functioning key pair,
- protect the private key (of this key pair) from compromise,
- determine a proposed distinguished name, and
- submit a certificate application (and subscriber agreement), including the public key of this key pair, to the applicable IA.

4.1 Key Generation and Protection

The following procedures are applicable to all entities generating keys as provided in this CPS.

4.1.1 Holder Exclusivity; Controlling Access to Private Keys

Unless otherwise permitted by this INDIA CPS, each certificate applicant shall securely generate his, her, or its own private key, using a trustworthy system, and take necessary precautions to prevent its compromise, loss, disclosure, modification, or unauthorized use. It is understood that subscribers (and certificate applicants) will generally use non-Safescrypt products that provide appropriate protection to keys. *See* the Subscriber Private Key Protection FAQ at **https://www. safescrypt.com/India-Repository/ PrivateKey_FAQ**.

EACH CERTIFICATE APPLICANT (AND, UPON APPROVAL, EACH SUBSCRIBER) ACKNOWLEDGES THAT SUCH PERSON, AND NOT SAFESCRYPT (OR THE APPLICABLE IA), IS EXCLUSIVELY RESPONSIBLE FOR PROTECTING HIS, HER, OR ITS PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE.

Users and IA's agree not to monitor, interfere with, or reverse engineer the technical implementation of the INDIA PCS except as explicitly permitted by this CPS or upon prior written approval from Safescrypt.

4.1.2 Delegation of Responsibilities for Private Keys

Delegation, if it occurs, does not relieve the delegator of his, her, or its responsibilities and liabilities concerning the generation, use, retention, or proper destruction of his, her, or its private key.

4.2 Certificate Application Information and Communication

Certificate application information includes the items listed in the following Table 6. *Not all of the following information will appear in a certificate (see* Figure 3 - Certificates and Information Incorporated by Reference). *Notes*: The items of such information not included in the certificate will be kept confidential by the IA (*see* CPS § 3.13). Certain Class B information for affiliated individuals of non-Safescrypt organizational LRAs may be not be required in an application but instead made generally available through such LRAs.

CLASS OF CERTIFICATE	REQUIRED CERTIFICATE APPLICATION INFORMATION
CLASS B	**Individuals:** ***Required Information*** (a) Legal name (in the form of a common name) (b) Proposed distinguished name (c) Street, city, state, postal / zip code, country (of residence) (d) Voice telephone numbers (of residence) (e) E-mail address (f) Subject public key (g) Credit card information (h) Spouse's first name (if applicable) (i) Date of birth (j) Employer (if applicable) (k) Challenge phrase (to later authenticate subscriber to the IA) (l) Executed subscriber agreement (m) Previous address (if changed within last two years) (n) Driver's license information (if applicable) (o) *Election Identity* Card (if applicable) (p) Authentication by the Bank Manager where the applicant maintains the account (if applicable) (q) Other information as prescribed by the IA or Safescrypt (if applicable) (r) Other information as may be required under the Information Technology Act, 2000 or any Rule or Regulations framed thereunder. (if Applicable) ***Optional*** (a) Demographic data (Registration Field Information) ***Method of Communicating Application****: Same as Class 1.* ***Agents/Authorized Representatives*****:** n / a **Business Entities:** Class 2 certificates are issued to individuals only.
CLASS C	**Individual** ***Required Information*** *– Same as Class B, plus:* (a) Subscriber agreement acknowledged by a notary or LRA and further authenticated by the Bank Manager where the applicant maintains the account (to fulfill the "personal presence" requirement) upon presentation of three (3) forms of identification by the certificate applicant.

	Optional **–** (b) Previous employer

TABLE 6 – REQUIRED CERTIFICATE APPLICATION INFORMATION

5. VALIDATION OF CERTIFICATE APPLICATIONS

This section presents the requirements for validation of certificate applications to be performed by the applicable IA or by an authorized local registration authority. It also explains the procedures for applications that fail validation.

5.1 Validation Requirements for Certificate Applications

Upon receipt of a certificate application (per CPS § 4 – Certificate Application Procedures) the IA shall perform all required validations as a prerequisite to certificate issuance (per CPS § 6 – Issuance of Certificates), as follows.

The IA shall confirm that

(a) the certificate applicant has agreed to be bound by the terms and conditions of a Subscriber Agreement;

(b) the certificate applicant is the person identified in the request (in accordance with and only to the extent provided in the certificate class descriptions, *see* CPS § 2, and as further described below),

(c) the certificate applicant rightfully holds the private key corresponding to the public key to be listed in the certificate (this obligation may be satisfied by a statement to this effect from the certificate applicant),

(d) the information to be listed in the certificate is accurate, except for nonverified subscriber information (NSI), and

Once a certificate is issued, the IA shall have no continuing duty to monitor and investigate the accuracy of the information in a certificate, unless the IA is notified in accordance with this CPS of that certificate's compromise.

Table 7 (Validation Requirements for Certificate Applications) highlights certain differences between the validation requirements for each certificate class. Safescrypt reserves the right to update these validation procedures to improve the validation process. Further details concerning validations are presented below. Updated validation procedures (when released) are presented in the Safescrypt repository at https://www.safescrypt.com/India-Repository/updates and may also be obtained from **Safescrypt Ltd, 667-668, Keshava Towers, 11th Main, 4th Block, Jayanagar, Bangalore – 560 011. Tel : +91-80-6555093 / +91-80-6555104**

VALIDATION REQUIREMENTS	CLASS B	CLASS C
PERSONAL PRESENCE	No	Yes – Individuals: Before a notary public or LRA (except non-Safescrypt organizational LRA applicants) Organizations: Optional
PERSONAL INVESTIGATION (FOR INDIVIDUALS)	No	Yes – Individuals: By a notary public in conjunction with the notary public's acknowledgment of the certificate application
THIRD-PARTY AUTOMATED CONFIRMATION OF PERSONAL (INDIVIDUAL) DATA	Yes	Yes (*see* description below)
THIRD-PARTY CONFIRMATION OF BUSINESS ENTITIES	n/a	Yes (*see* description below)
POSTAL ADDRESS CONFIRMATION	Yes (*see* below)	n/a
DOMAIN NAME CONFIRMATION	n/a	Yes (*see* description below)

TABLE 7 – VALIDATION REQUIREMENTS FOR CERTIFICATE APPLICATIONS

5.1.1 Personal Presence

In order to effect an appropriate binding between the applicant and the applicant's public key, individuals applying for Class C certificates must appear personally before a trusted entity (such as a notary public or an LRA) to facilitate the confirmation of their identity. A personal presence requirement has many variables (depending upon the class and type of certificate), including but not limited to specified identification documents.

5.1.2 Third-Party Confirmation of Personal Data

Where required, a third party confirms personal information provided by the certificate applicant by comparing it to the third party's databases. Confirmation is achieved if the certificate applicant's data is consistent with the database information, based on Safescrypt's custom matching algorithm or another appropriate determination process.

On-line investigation provides some assurance of identity by comparing certificate applicant identity information against trustworthy third-party

databases. These databases may also provide confirmation of the applicant's address. The scope of on-line investigations is, however, subject to individual countries' data protection laws. Special procedures may also be implemented by an IA, depending on the requirements of the certificate applicant and the class of certificate to be issued.

5.1.3 Third-Party Confirmation of Business Entity Information

Where required, the third party confirms the business entity's name, address, and other registration information through comparison with third-party databases and / or through inquiry to the appropriate government entities. Confirmation of information of companies, banks, and their agents requires certain customized (and possibly localized) procedures focusing on specific business-related criteria (such as proper business registration). The third party also provides telephone numbers that are used for out-of-band communications with the business entity to confirm certain information (for example, to confirm an agent's position within the business entity or to confirm that the particular individual listed in the application is in fact the applicant). If its databases do not contain all the information required, the third party may undertake an investigation, if requested by the IA, or the certificate applicant may be required to provide additional information and proof.

5.1.4 Postal Address Confirmation

Upon issuance of a Class B (provisional) certificate, the IA shall send a corroboration letter (via first class mail) to the postal address submitted in the certificate application and confirmed (via third party database - *see* CPS § 5.1.2). This corroboration procedure provides further confirmation that the subscriber's address matches the address listed in the certificate application and therefore provides further assurances that the subscriber is who he or she purports to be.

The corroboration letter (letter) contains a personal identification number (PIN) that is intended to enhance the authentication of the certificate applicant. The letter instructs the recipient (of the letter) to request cancellation of the application process and revocation of the certificate in the event the certificate application is determined to have been submitted by an imposter. This cancellation procedure is available only during the certificate's provisional period, and is distinct from certificate revocation procedures. If revocation has not occurred during the provisional period, the provisional certificate shall become a normal certificate thereafter. Postal address confirmation does not apply to Class B certificates approved by non-Safescrypt organizational LRAs.

5.1.5 Domain Name Confirmation & Serial Number Assignment

The naming authority used by an IA and Safescrypt shall have sole discretion regarding the assignment of relative distinguished names (RDNs) and certificate serial numbers appearing in the certificates they issue. IA's shall use an appropriate domain name registration service for resolving RDN assignment where appropriate. For information about InterNIC procedures and assurances, *see* **http://ds.internic.net/ds/admin.html**.

5.2 Approval of Class C Certificate Applications

Upon successful performance of all required validations of a Class C certificate application (in accordance with CPS § 5.1), the applicable IA shall approve the application. Approval is demonstrated by issuing a normal certificate according to CPS § 6 (Issuance of Certificates).

5.3 Approval of Class B Certificate Applications

Upon successful performance of all required IA-internal validations of a Class 2 certificate application (in accordance with CPS § 5.1), the applicable IA shall provisionally approve the certificate application.

5.4 Rejection of Certificate Application

If a validation fails, the applicable IA shall reject the certificate application by promptly notifying the certificate applicant of the validation failure and providing the reason code (except where prohibited by law) for such failure. Where such validation failure is caused as a result of third-party database information, the applicable IA shall provide the certificate applicant with the third-party database company's contact information for inquiry and dispute resolution. Such notice shall be communicated to the certificate applicant using the same method as was used to communicate the certificate application to the IA (or LRA).

A person whose certificate application has been rejected may thereafter reapply.

6. ISSUANCE OF CERTIFICATES

This section presents the requirements for the issuance of certificates. It also lists the specific representations issuing authorities make upon issuing certificates.

6.1 Normal Certificates

Upon approving a certificate application (per India CPS § 5), an IA issues a certificate. The issuance of a normal certificate indicates a complete and final approval of the certificate application by an IA. The normal certificate is deemed to be a valid certificate upon the subscriber's acceptance of it (*see* India CPS § 7 regarding acceptance).

6.2 Consent by Subscriber for Issuance of Certificate by IA

An IA shall not issue certificates without the certificate applicant's consent. Consent to issue is given through applicant's submission of an application notwithstanding the fact that acceptance of a certificate has not yet occurred.

6.3 Refusal to Issue a Certificate

An IA may refuse to issue a certificate to any person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Provided that the certifying authority before refusing the certificate shall give a reasonable opportunity to the applicant to show cause against the proposed rejection, consider the representation made by the applicant and decide the issue or rejection of the certificate applied for. Upon an IA's refusal to issue a certificate, the IA shall promptly refund to any certificate applicant any paid certificate enrollment fee, unless the certificate applicant submitted fraudulent or falsified information to the IA.

6.4 IA's Representations Upon Certificate Issuance

6.4.1 IA's Representations to Subscriber

(i) Unless otherwise provided in this India CPS or mutually agreed upon by both the IA and the subscriber in an authenticated record, the IA promises to the subscriber named in the certificate that

(a) there are no misrepresentations of fact in the certificate known to the IA or originating from the IA,

(b) there are no data transcription errors as received by the IA from the certificate applicant resulting from a failure of the IA to exercise reasonable care in creating the certificate, and

(c) the certificate meets all material requirements of this India CPS.

(ii) Unless otherwise provided in this India CPS or mutually agreed upon by both the IA and the subscriber in an authenticated record, the IA promises to the subscriber to make reasonable efforts, consistent with the terms of this India CPS,

(a) to promptly revoke or suspend certificates in accordance with India CPS § 9, and

(b) to notify subscribers of any facts known to it that materially affect the validity and reliability of the certificate it issued to such subscriber.

(iii) The obligations and representations in India CPS §§ 6.5.1 (i) and (ii) are made and undertaken solely for the benefit of the subscriber and are not intended to benefit or be enforceable by any other party. An IA makes reasonable efforts, for purposes of India CPS § 6.5.1(ii), if its conduct substantially complies with this India CPS and applicable law.

6.4.2 IA's Representations to Relying Parties

By issuing a certificate an IA represents to all who reasonably rely on a digital signature verifiable by the public key listed in the certificate that consistent with this India CPS:

(i) all information in or incorporated by reference within the certificate, except nonverified subscriber information (NSI), is accurate, and

(ii) the IA has substantially complied with the India CPS when issuing the certificate.

6.5 IA's Representations Upon Publication

By publishing a certificate (*see* India CPS § 7.5), an IA certifies to the Safescrypt repository and to all who reasonably rely on the information contained in the certificate that it has issued the certificate to the subscriber and that the subscriber has accepted the certificate, as described in India CPS § 7.1.

6.6 Limitations on IA Representations

The foregoing representations in India CPS §§ 6.5 and 6.6 are subject to the disclaimers of warranty and limitations of liability in India CPS §§ 11.3, 11.4, and 11.5.

6.7 Time of Certificate Issuance

IA's shall make reasonable efforts to confirm certificate application information and issue end-user subscriber certificates once all relevant information is received by the IA within the following time periods:

	CLASS B	CLASS C
TIME PERIOD	"Immediately" to 1 business day	1-5 business days

TABLE 8 – CERTIFICATE ISSUANCE DEADLINES

Safescrypt's and IA's satisfaction of these deadlines depends upon a certificate applicant's timely submission of complete and accurate information, and responsiveness to any Safescrypt and IA administrative requests, including the provision of appropriate and accurate payment information and approval.

6.8 Certificate Validity and Operational Periods

All certificates shall be considered valid upon issuance by the applicable IA and acceptance by the subscriber (*see* CPS § 7). The standard operational periods for the various classes of certificates are as follows, subject to earlier termination of the operational period due to suspension or revocation

CERTIFICATE ISSUED BY:	CLASS B	CLASS C
PCA (SELF-SIGNED)	Up to 20 years	Up to 20 years
PCA TO CA	Up to 20 years	Up to 20 years
CA TO SUBORDINATE CA	TBD	TBD
CA TO END-USER/ SUBSCRIBER	1 year	1 year

TABLE 9 – CERTIFICATE OPERATIONAL PERIODS

All certificates begin their operational period at the date and time of issuance, unless a later date and time (no later than sixty (60) days after the date of issue) is indicated in the certificate. The operational period begins at this date and time even if the certificate has not yet been accepted and is therefore not yet valid.

6.9 Restrictions on Issued but not Accepted Certificates

A subscriber must not create digital signatures using a private key corresponding to the public key listed in a certificate (or otherwise use such private key) if the foreseeable effect would be to induce or allow reliance upon a certificate which is invalid (because it has not been accepted).

7. ACCEPTANCE OF CERTIFICATES BY SUBSCRIBERS

This section explains the requirements for certificate acceptance by subscribers, the representations made by subscribers upon acceptance, subscribers' obligations to protect their private keys, and procedures for the publication of certificates.

7.1 Certificate Acceptance

A subscriber is deemed to have accepted a certificate when, following communication of the application per CPS § 4.2, approval is manifested as described in Table 10.

CLASS	MEANS OF ESTABLISHING ACCEPTANCE
CLASS B	**Individuals:** **On-line (via the Web):** The certificate applicant enters his or her PIN to obtain and accept the certificate. Note: The certificate applicant must notify the IA of any inaccuracy or defect in a certificate promptly after receipt of the certificate or publication of the certificate in the repository, or upon earlier notice of informational content to be included in the certificate. Additionally, upon the certificate applicant's receipt of the corroboration letter from the IA, the certificate applicant shall review the letter's content and contact the IA should the letter contain an error, in accordance with CPS § 5.1.4 (Postal Address Confirmation). **E-mail (S/MIME):** The certificate applicant submits a CSR to the IA to accept the certificate. Upon completion of specified validation procedures, the IA then sends the certificate to the E-mail address from which the certificate application originated. Note: The certificate applicant must promptly notify the IA of any inaccuracy or defect in a certificate or publication of the certificate in the repository, or upon earlier notice of informational content to be included in the certificate. **Business Entities:** n / a
CLASS C	**Individuals:**

	On-line (via the Web): *Same as on-line Class b.* **E-mail (S/MIME):** *Same as E-mail Class b.*

TABLE 10 – METHODS OF CERTIFICATE ACCEPTANCE

7.1.2 As provided in Section 41 of the *Information Technology* Act, 2000, a subscriber is also deemed to have accepted a certificate if he publishes or authorises the publication of a Digital Signature Certificate to one or more persons or in a repository or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

7.2 Representations by Subscriber Upon Acceptance

By accepting a certificate issued by an IA or CA, the subscriber certifies to and agrees with the IA and to all who reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber,

(i) 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, suspended or revoked) at the time the digital signature is created,

(ii) no unauthorized person has ever had access to the subscriber's private key,

(iii) all representations made by the subscriber to the IA or CA regarding the information contained in the certificate are true,

(iv) all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and does not promptly notify the IA of any material inaccuracies in such information as set forth in India CPS § 6.1,

(v) the certificate is being used exclusively for authorized and legal purposes, consistent with this India CPS, and

(vi) the subscriber is an end-user subscriber and not an IA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as an IA or otherwise, unless expressly agreed in writing between subscriber and the IA.

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT HE, SHE, OR IT AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS INDIA CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT.

7.3 Subscriber Duty to Prevent Private Key Disclosure

By accepting a certificate, the subscriber assumes a duty to retain control of the subscriber's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use. The subscriber is responsible for and shall duly fulfill his duties listed in IT Act (including and in particular sections 40 to 42) and in the Rules and Regulations framed thereunder.

7.4 Indemnity by Subscriber

BY ACCEPTING A CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD THE IA, SAFESCRYPT, AND THEIR AGENT(S) AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS' FEES, THAT THE IA, SAFESCRYPT, AND THEIR AGENTS AND CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A CERTIFICATE, AND THAT ARISES FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORIZED BY THE SUBSCRIBER); (II) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE THE IA, SAFESCRYPT, OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; OR (III) 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.

When a certificate is issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify the IA, Safescrypt, and their agents and contractors pursuant to this subsection. The subscriber has a continuing duty to notify the issuer of any misrepresentations and omissions made by an agent.

7.5 Publication

Upon the subscriber's acceptance of the certificate, the IA shall publish a copy of the certificate in the Safescrypt repository and in one or more other repositories, as determined by the IA and Safescrypt. Subscribers may publish their Safescrypt PCS certificates in other repositories

8. USE OF CERTIFICATES

This section addresses the rights and obligations of the entities whose rights and obligations are intended to be controlled by this CPS (*see* definition of "parties") regarding the use of digital signatures and digitally signed messages corresponding to Safescrypt-issued certificates.

The parties (IA and the parties who are "users" of the certificate, *i.e.*, the subscriber and the relying parties), are hereby notified of the following rules governing the respective rights and obligations of the parties among themselves, which are also deemed to be agreed by the parties, effective (i) upon publication of this CPS in the case of the IA; (ii) upon submission of an application for a certificate, in the case of an applicant or subscriber; and (iii) upon reliance of a certificate or a digital signature verifiable with reference to a public key listed in the certificate, in the case of a recipient of a certificate or a relying party.

8.1 Verification of Digital Signatures

Verification of a digital signature, is undertaken to determine that (i) the digital signature was created by the private key corresponding to the public key listed in the signer's certificate and that (ii) the associated message has not been altered since the digital signature was created.

Such verification shall be undertaken in a manner consistent with this INDIA CPS, as follows:

• **Establishing a certificate chain for the digital signature** – A digital signature shall be verified with regard to a successful confirmation of certificate chain.

• **Ensuring that the identified certificate chain is the most suitable for the digital signature** – It is possible to have more than one valid certificate chain leading from a given certificate to an acceptable root (such as through cross-certification among other possibilities). If there is more than one certificate chain to an acceptable root, the person verifying the digital signature may have various options in selecting and validating the certificate chain. For instance, a "higher-trust" PCA may have been certified by a "lower trust" PCA. In this case the person verifying the digital signature may prefer to use a certificate chain terminating in the higher-trust PCA rather than the lower-trust PCA.

• **Checking the Safescrypt (or other) repository for revocation or suspension of certificates in the chain** – The recipient must determine if any of

the certificates along the chain from the signer to an acceptable root within the INDIA PCS has been revoked or suspended, because a revocation or suspension has the effect of prematurely terminating the operational period during which verifiable digital signatures can be created. This may be ascertained in two different ways. The Safescrypt repository may be queried for the most up-to-date revocation status. Alternatively, CRLs may have been provided in the certificate chain. These CRLs may be used to determine the revocation status of certificates in the chain.

• **Delimiting data to which digital signatures are attached** – In order to verify a digital signature, it is necessary to know precisely what data has been signed. In the case of public key cryptography standards (PKCS), a standard signed message format is specified to accurately denote the signed data.

• **Indicating digital signature time and date of creation** – In order for a digital signature to support non repudiation, the data to which the corresponding digital signature is attached must include, or reference, a time stamp. The time stamp shall reflect the time at which date and time the digital signature is affixed.

• **Establishing the assurances intended by its signer** – Various technical means may be used to determine the purpose (or meaning) of the digital signature intended by its signer. In formal protocols (such as EDI), digital signatures are classified as specified security services with defined semantics so as to convey their precise meaning. The verifier should also determine whether the certificate is normal or provisional.

• **Ensuring that all certificates in the chain authorize use of an end-user subscriber private key** – An IA may limit the purposes for which a private key corresponding to a certificate it issues may be used. Such limitations are indicated or incorporated by reference in the certificate and provide a means to warn recipients of situations for which reliance upon the certificate would not be considered reasonable. Persons validating certificates must inspect certificate contents for such warnings and limitations to ensure that no certificate in the chain denies appropriate use of an end-user subscriber certificate.

• **Confirmation of a certificate chain** – Each IA is certified by a superior IA and thus inherits the trust associated with its superior IA. Each IA is presumed to be at least as trustworthy as its superior IA. Confirmation of a certificate chain is the process of validating a certificate chain and subsequently validating an end-user subscriber certificate.

8.2 Effect of Validating an End-User Subscriber Certificate

A digital signature is binding against its maker if it (i) was created during the operational period of a valid certificate, (ii) such digital signature can be properly verified by confirmation of certificate chain (iii) the relying party has no knowledge or notice of a breach of the requirements of this India CPS by the signer, and (iv) the relying party has complied with all requirements of this India CPS.

THE USE OF CERTIFICATES DOES NOT CONVEY EVIDENCE OF *AUTHORITY* ON THE PART OF ANY USER TO ACT ON BEHALF OF ANY PERSON OR TO UNDERTAKE ANY PARTICULAR ACT. VERIFIERS OF DIGITALLY SIGNED MESSAGES ARE SOLELY RESPONSIBLE FOR EXERCISING DUE DILIGENCE AND REASONABLE JUDGMENT BEFORE RELYING ON CERTIFICATES AND DIGITAL SIGNATURES. A CERTIFICATE IS NOT A GRANT FROM AN IA OF ANY RIGHTS OR PRIVILEGES, EXCEPT AS SPECIFICALLY PROVIDED IN THIS INDIA CPS.

8.3 Procedures upon Failure of Digital Signature Verification

A person relying on an unverifiable digital signature assumes all risks with regard to it and is not entitled to any presumption that the digital signature is effective as the signature of the subscriber under India CPS §§ 8.4 - 8.6.

8.4 Reliance on Digital Signatures

A recipient of a message signed by a digital signature of the subscriber may rely upon that digital signature as binding against the subscriber if:

(i) the digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate chain, and

(ii) such reliance 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 reasonable.

Additionally, the verifier should consider the class of certificate and the state of a certificate (normal or provisional). The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the verifier.

8.5 Writings

A message bearing a digital signature verified by the public key listed in a valid certificate is as valid, effective, and enforceable as if the message had been written and signed on paper.

8.6 Signatures

Where a rule of law or applicable practice requires a signature or provides for certain consequences in the absence of a signature, that rule is satisfied in relation to a message by a digital signature affixed by a signer with the intention of signing a message and subsequently verified by reference to the public key listed in a valid certificate.

8.7 Security Measures

Any person using or relying upon a Safescrypt INDIA PCS-issued certificate in conjunction with a message shall apply reasonable security measures to the message to provide message authentication and, as required, to support data confidentiality.

8.8 Issuing Certificates

Only authorized IA's may issue certificates.

9. CERTIFICATE SUSPENSION AND REVOCATION

This section explains the circumstances under which a certificate may (or must) be suspended or revoked. It also details the procedures for suspending, revoking, and reinstating certificates.

9.1 Reasons for Suspension or Revocation, Generally

A certificate shall be suspended or revoked if

• there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject,

• the certificate's subject (whether an IA or a subscriber) has breached a material obligation under this India CPS,

• the performance of a person's obligations under this India CPS has been delayed or prevented by an act of God; natural disaster; computer or communications failure; change in statute, regulation, or other law; official government action, including but not limited to acts by agencies responsible for export control administration; or other cause beyond the person's reasonable control, and as a result another person's information has been or may be materially threatened or compromised, or

• the subscriber (or authorized representative) has duly requested it.

- Any other reason provided in the IT Act

9.2 Suspension or Revocation of an IA's Certificate

An IA must make a reasonable effort to suspend or revoke a subordinate IA's certificate, regardless of whether the subordinate IA consents, if it determines any of the following:

• a material fact represented in the certificate is known or reasonably believed by the IA to be false,

• a material prerequisite to certificate issuance was neither satisfied nor waived,

• the subordinate IA's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability, or

• the certificate's subject (here, an IA) has breached a material obligation under this INDIA CPS.

The IA must promptly notify the subordinate IA of any such suspension or revocation.

Note: *Suspension is not currently available for end-user subscriber certificates. It is contemplated to be offered as an added service in the future. Safescrypt will announce its availability in the Practices Updates and Notices section on its website. Revocation is currently available for both end-user subscriber and IA certificates.*

9.3 Suspension at an IA's Request

An IA shall suspend a subordinate IA's certificate upon the request of a duly authorized representative of the subordinate IA or of a person claiming to be the subordinate IA or a person in a position likely to know of a compromise of the subordinate IA's private key, such as an agent or employee of the subordinate IA. Such suspension must be undertaken in accordance with the suspension prerequisites stated in Table 11 as follows.

	PREREQUISITES FOR SUSPENDING AN IA'S CERTIFICATE
PCA AND CA	• Request from the IA. • Request in the form of an authenticated record or a fax or voice message from the subject IA or its agent (authenticated by means of a challenge phrase or recitation of certain presubmitted enrollment information). **Note:** The issuing IA need not further confirm the identity or agency of the person requesting such a suspension. An IA that suspends a subordinate IA's certificate in accordance with India CPS § 9.3 shall not be held liable for the unauthorized suspension of such certificate provided that it acts in good faith upon receiving purportedly authorized instructions.

TABLE 11 – SUSPENSION PREREQUISITES

The IA that suspended a subordinate IA's certificate shall subsequently revoke it if requested to do so and upon confirming the reason for suspension or upon confirming any of the reasons for revocation listed in India CPS § 9.1

9.4 Termination of a Suspension of an IA's Certificate

An IA may terminate a certificate suspension (thereby reinstating the certificate), if (i) the subject IA requests it and the IA confirms his or her identity, (ii) the IA determines that the request for suspension was made without the suspended IA's authorization, or (iii) the IA determines that the reasons for the suspension were unfounded.

9.5 Revocation at Subscriber's Request

An IA must revoke a certificate promptly upon the subscriber's request once it has confirmed that the person requesting the revocation is in fact the subscriber

9.6 Revocation Due to Faulty Issuance

An IA shall revoke a certificate promptly upon discovering and confirming that it was not issued in accordance with the procedures required by this India CPS. A certificate may be suspended while the IA investigates to confirm grounds for revocation. Table 12 details revocation prerequisites.

	PREREQUISITES FOR AN IA REVOKING A CERTIFICATE
PCA AND CA	• Certificate revocation request from a subordinate IA. • Request in the form of an authenticated record or voice message from the subscriber or its agent, authenticated by means of a challenge phrase or recitation of certain presubmitted enrollment information.

TABLE 12 – REVOCATION PREREQUISITES

9.7 Notice and Confirmation upon Suspension or Revocation

Upon suspending or revoking a certificate, an IA must publish notice of the suspension or revocation in the Safescrypt repository. An IA may publish one or more of the following:

• a listing of revoked (and suspended) certificates available through a secure channel,

• a certificate revocation list (CRL) designating both revoked and suspended certificates. An IA must publish a CRL at least daily for Class B and C CAs and subordinate CAs and at least monthly for PCAs, unless otherwise provided in the Safescrypt repository. CRLs shall also be issued on an emergency basis, as determined by the IA, and

• a composite CRL issued by a PCA that has been generated from CRLs deposited in the Safescrypt repository by corresponding IA's.

IA's may also provide the following suspension and revocation notification services upon request and payment of associated fees by the requester:

• confirming that a certificate has been suspended or revoked, if asked to do so by a recipient of a digitally signed message originated by the subject of that certificate, and

• providing a "push service" to provide notice from the IA to the requester upon the suspension or revocation of designated certificates.

9.8 Effect of Suspension or Revocation

9.8.1 On Certificates

During suspension, or permanently upon revocation of a subscriber's certificate, that certificate's operational period shall immediately be considered terminated. Similarly, in the case of a certificate issued to an IA, the termination of the operational period of that IA's certificate withdraws the authority of that IA to issue certificates, but does not affect the validity of certificates issued by that IA, when the IA's certificate was operational.

9.8.2 On Underlying Obligations

Suspension or revocation of a certificate shall not affect any underlying contractual obligations created or communicated under this India CPS

9.9 Safeguarding of Private Key upon Suspension or Revocation

Private keys corresponding to public keys contained in suspended or revoked certificates shall be safeguarded by the subscriber in a trustworthy manner throughout the period of suspension and, upon revocation for the applicable retention period, unless destroyed

10. CERTIFICATE EXPIRATION

This section describes parties' obligations regarding certificate expiration. This is distinct from certificate suspension and revocation (*see* CPS § 9). Certificate validity and operational periods are addressed in CPS § 6.9.

10.1 Notice Prior to Expiration

IA's will make a reasonable effort to notify subscribers, via E-mail, of the impending expiration of their certificates. Such notice is intended solely for the convenience of the subscriber in the re-enrollment or renewal process, whichever is applicable.

10.2 Effect of Certificate Expiration on Underlying Obligations

Expiration of a certificate shall not affect the validity of any underlying contractual obligations created or communicated under this India CPS.

10.3 Re-enrollment and Subscriber Renewal

Subscriber renewal and re-enrollment shall be initiated as follows:

CLASS B	CLASS C
Same process as initial application. However, a certificate applicant need submit only new or changed information.	Same process as initial application. However, a certificate applicant need submit only new or changed information.

TABLE 13 – RENEWAL AND RE-ENROLLMENT REQUIREMENTS

Requirements for renewal and re-enrollment are subject to change at Safescrypt's discretion. Up-to-date requirements for re-enrollment and renewal are accessible (when available) from the Safescrypt repository at https://www.safescrypt.com/India-Repository

11. OBLIGATIONS OF ISSUING AUTHORITIES AND SAFESCRYPT, AND LIMITATIONS UPON SUCH OBLIGATIONS

This section summarizes and provides references to Safescrypt's refund policy, the warranties and promises made by issuing authorities and Safescrypt, and the disclaimers and limitations upon such obligations.

11.1 Refund Policy

Safescrypt adheres to, and stands behind, 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 India 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, for the full amount of the applicable fees paid for the certificate. To request a refund, subscribers shall file a request at **https://www.safescrypt.com/India-Repository/refund**. This refund policy is not an exclusive remedy and does not limit other remedies that may be available to subscribers.

11.2 Limited Warranties and Other Obligations

Issuing authorities (and Safescrypt, to the extent specified in the referenced India CPS sections) warrant and promise to

- provide the infrastructure and certification services, including the establishment and operation of the Safescrypt repository, as delineated in India CPS § 2 (Safescrypt Certification Infrastructure),

- provide the controls and foundation for Safescrypt's PKI, including IA key generation, key protection, and secret sharing procedures, presented in India CPS § 3 (Foundation for Certification Operations),

- perform the application validation procedures for the indicated class of certificate as set forth in India CPS § 5 (Validation of Certificate Applications),

- issue certificates in accordance with India CPS § 6 and honor the various representations to subscribers and to relying parties presented in India CPS § 6.5 (IA's Representations Upon Certificate Issuance),

• publish accepted certificates in accordance with India CPS § 6.6 (IA's Requirements Upon Publication) and India CPS § 7.5 (Publication),

• perform the obligations of an IA and support the rights of the subscribers and relying parties who use certificates in accordance with India CPS § 8 (Use of Certificates),

• suspend and revoke certificates as required by India CPS § 9 (Certificate Suspension and Revocation),

• provide for the expiration, re-enrollment, and renewal of certificates as stated in India CPS § 10 (Certificate Expiration), and

• comply with the provisions contained in India CPS § 12 (Miscellaneous Provisions).

Additionally, IA's and Safescrypt warrant that their own private keys are not compromised unless they provide notice to the contrary via the Safescrypt repository.

ISSUING AUTHORITIES AND SAFESCRYPT MAKE NO OTHER WARRANTIES AND HAVE NO FURTHER OBLIGATIONS UNDER THIS INDIA CPS.

11.3 Disclaimers and Limitations on Obligations of IA's and Safescrypt

EXCEPT AS EXPRESSLY PROVIDED IN THE FOREGOING (CPS § 11.2), ISSUING AUTHORITIES AND SAFESCRYPT DISCLAIM ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED, AND FURTHER DISCLAIM ANY AND ALL LIABILITY FOR NEGLIGENCE, FAILURE TO WARN, AND LACK OF REASONABLE CARE.

Except as expressly stated in the foregoing CPS § 11.2, IA's and Safescrypt

• do not warrant the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of issuing authorities and Safescrypt,

• shall not incur liability for representations of information contained in a certificate, provided the certificate content substantially complies with this CPS,

• do not warrant "nonrepudiation" of any certificate or message (because nonrepudiation is determined exclusively by law and the applicable dispute resolution mechanism), and

• do not warrant any software.

11.4 Exclusion of Certain Elements of Damages

IN NO EVENT SHALL ANY ISSUING AUTHORITY OR SAFESCRYPT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA, OR OTHER INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES, WHETHER OR NOT REASONABLY FORESEEABLE, ARISING FROM OR IN CONNECTION WITH THE USE, DELIVERY, LICENSE, PERFORMANCE, OR NONPERFORMANCE OF CERTIFICATES, DIGITAL SIGNATURES, OR ANY OTHER TRANSACTIONS OR SERVICES OFFERED OR CONTEMPLATED BY THIS CPS, EVEN IF SUCH ISSUING AUTHORITIES OR SAFESCRYPT, OR BOTH, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.5 Damage and Loss Limitations

IN NO EVENT WILL THE AGGREGATE LIABILITY OF AN ISSUING AUTHORITY AND ALL SUPERIOR IA'S IN THE CERTIFICATION CHAIN TO WHICH THE IA's CERTIFICATE BELONGS (AND SAFESCRYPT, AS SPECIFIED) TO ALL PARTIES (INCLUDING WITHOUT LIMITATION A SUBSCRIBER, AN APPLICANT, A RECIPIENT, OR A RELYING PARTY) EXCEED THE APPLICABLE LIABILITY CAP FOR SUCH CERTIFICATE SET FORTH IN TABLE 14, BELOW.

THE COMBINED AGGREGATE LIABILITY OF ALL ISSUING AUTHORITIES AND SAFESCRYPT TO ANY AND ALL PERSONS CONCERNING A SPECIFIC CERTIFICATE SHALL BE LIMITED TO AN AMOUNT NOT TO EXCEED THE FOLLOWING, FOR THE AGGREGATE OF ALL DIGITAL SIGNATURES AND TRANSACTIONS RELATED TO SUCH CERTIFICATE:

	LIABILITY CAPS
CLASS B	To be decided
CLASS C	To be decided

TABLE 14 - LIABILITY CAPS

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages incurred by any person, including without limitation a subscriber, an applicant, a recipient, or a relying party, that are caused by reliance on or use of a certificate an issuing authority or Safescrypt issues, manages, uses, suspends or revokes, or such a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall Safescrypt be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

11.6 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

11.7 No Fiduciary Relationship

IA'S AND SAFESCRYPT ARE NOT THE AGENTS, FIDUCIARIES, TRUSTEES, OR OTHER REPRESENTATIVES OF SUBSCRIBERS OR RELYING PARTIES. The relationship between IA's (or Safescrypt) and subscribers and that between IA's (or Safescrypt) and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind an IA (or Safescrypt), by contract or otherwise, to any obligation. IA's and Safescrypt shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

11.8 Hazardous Activities

Safescrypt's public certification services 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.

12. MISCELLANEOUS PROVISIONS

This section presents general terms and conditions of this CPS that are not covered in the other sections.

12.1 Conflict of Provisions

In the event of a conflict between this India CPS and other guidelines, or contracts, the subscriber shall be bound by the provisions of this India CPS, except as to other contracts either (i) predating the first public release of the India CPS or (ii) expressly superseding this India CPS for which such contract shall govern as to the parties thereto, and except to the extent that the provisions of this India CPS are prohibited by law.

12.2 Compliance with Export Laws and Regulations

Export of certain software used in conjunction with Safescrypt's INDIA PCS may require the approval of appropriate government authorities. The parties shall conform to applicable export laws and regulations.

12.3 Governing 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 users, no matter where they reside or use their certificates.

12.4 Dispute Resolution, Choice of Forum, and Presumptions

12.4.1 Notification Among Parties to a Dispute

Before invoking any dispute resolution mechanism (including litigation or arbitration, as detailed below) with respect to a dispute involving any aspect of this CPS or a certificate issued by an IA, aggrieved persons shall notify Safescrypt, the applicable IA, and any other party to a dispute for the purpose of seeking dispute resolution among themselves.

12.4.2 Distinguished Panel of Experts

If the dispute is not resolved within ten (10) days after initial notice pursuant to CPS § 12.4.1, then a party may submit the dispute in written or electronic form to Safescrypt requesting consideration by its Distinguished Panel of Experts (DPE). In response, Safescrypt will convene a DPE, composed of three PKI experts,

including those from SafeScrypt, to assemble relevant facts with the goal of facilitating dispute resolution. The submitting party must deliver a copy of the submittal to all other parties. Any party that did not submit the matter may provide appropriate information to the DPE within one (1) week after the date the dispute was submitted to the DPE. The DPE shall complete and communicate its recommendations to the parties within three (3) weeks (unless the parties mutually agree to extend this period for a specified additional period) after the matter was initially submitted to the DPE. The DPE will generally operate via E-mail, teleconferencing, courier and postal mail. The recommendations of the DPE shall not be binding upon the parties.

12.4.3 Formal Dispute Resolution

Following the DPE's completion and communication of its recommendations, or the DPE's failure to complete and communicate its recommendations (per CPS § 12.4.2), an aggrieved person may invoke a dispute resolution mechanism as follows. Nothing in CPS § 12.4 shall preclude Safescrypt and the applicable IA from seeking equitable (including injunctive) relief upon alleged compromise or alleged material breach in a manner consistent with governing law and this CPS.

(i) When one of the indispensable parties to a dispute is Safescrypt resident or organization situated or doing business in India, except where each indispensable party to a dispute agrees to an alternative dispute resolution mechanism (such as arbitration), all suits to enforce any provision of this CPS or arising in connection with the CPS or any related business relationship between the parties hereto shall be brought in a court in Bangalore, India . Each person hereby agrees that such court shall have exclusive in personam jurisdiction and venue with respect to such person and each person hereby submits to the exclusive in personam jurisdiction and venue of such court.

(ii) Except for those cases mentioned in CPS § 12.4.3(i), all disputes arising in connection with the CPS shall be finally settled by Arbitration of Indian Council of Arbitration, Federation of Indian Chambers of Commerce and Industry, New Delhi which shall apply the Rules of Conciliation and Arbitration of the International Chamber of Commerce (ICC) modified as necessary to reflect the provisions herein by one or more arbitrators. The place of arbitration shall be in Bangalore, India and the proceedings shall be conducted in English. In cases involving appointment of a single arbiter under the above rules, that single arbiter shall be appointed by mutual agreement of the parties. If the parties fail to agree on an arbiter within fifteen (15) days, the Indian Council of Arbitration shall choose an arbiter knowledgeable in computer software law, information security, and cryptography or otherwise having special qualifications in the field, such as a lawyer, academician, or judge in a common law jurisdiction.

12.5 Successors and Assigns

This CPS inures to the benefit of, and shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. Subject to the provisions of IT Act, Rules Regualtions and other applicable laws the rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with CPS § 3.21, concerning termination or cessation of IA operations; and provided further, that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

12.6 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of Safescrypt or any IA may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

12.7 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so as best to reasonably effect the intent of its parties. IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EACH AND EVERY PROVISION OF THIS CPS THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF OR LIMITATION UPON ANY WARRANTIES OR OTHER OBLIGATIONS, OR EXCLUSION OF DAMAGES IS INTENDED TO BE SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND IS TO BE ENFORCED AS SUCH.

12.8 Interpretation and Translation

Unless otherwise provided, this CPS shall be interpreted consistently with what is commercially reasonable under the circumstances. In interpreting this CPS, regard is to be given to its international scope and application, to the benefits in promoting uniformity in its application, and to the observance of good faith.

12.9 No Waiver

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

12.10 Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

To **Safescrypt Ltd, 667-668, Keshava Towers, 11th Main, 4th Block, Jayanagar, Bangalore – 560 011**.

By Safescrypt or an IA to another person:	To the most recent address of record on file with Safescrypt or IA

Any non-Safescrypt IA shall immediately advise its Safescrypt IA of any legal notice served on the non-Safescrypt IA that might affect its Safescrypt IA or Safescrypt.

12.11 Headings and Appendices of this CPS

The headings, subheadings, and other captions in this CPS are for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS. The appendices, including the definitions to this CPS, are for all purposes an integral and binding part of the CPS.

12.12 Change of Subscriber Information on File with IA; Change to CPS

12.12.1 Change of Subscriber Information Maintained by an IA

Any subscriber may change certain information about itself on file with its IA that does not appear within its certificate (typically, information provided in the subscriber agreement or certificate application) upon giving thirty (30) days notice in accordance with CPS § 12.10 (Notice). Such change in information shall be effective after such thirty (30) day period.

12.12.2 Amendment of CPS

12.12.2.1 Amendments Generally

Safescrypt shall be entitled to amend this CPS from time to time (prospectively and not retroactively). Safescrypt shall be entitled to place amendments in the Safescrypt repository either in the form of an amended version of the CPS or in the Practices Updates and Notices section of the Safescrypt repository.

12.12.2.2 Practices Updates and Notices

Amendments to this CPS that are placed in the Practices Updates and Notices section of the Safescrypt repository (*see* https://www.safescrypt.com/India-Repository/updates) shall have the effect of amending the CPS. Such amendments shall supersede any conflicting and designated provision(s) of the referenced version of the CPS.

12.12.2.3 Material Amendments

A material amendment to the CPS shall become effective fifteen (15) days after Safescrypt publishes the amendment in the Safescrypt repository in accordance with CPS § 12.12.2.1, unless Safescrypt publishes a notice of withdrawal of the amendment in the repository prior to the end of such fifteen (15) day period.

12.12.2.4 Material Amendments Exception

If, notwithstanding CPS § 12.12.2.3, Safescrypt publishes a material amendment to the CPS, it shall become effective immediately upon publication in the Safescrypt repository in accordance with CPS § 12.12.2.1 if failure by Safescrypt to make the amendment may result in a compromise of the INDIA PCS or any portion of it.

12.12.2.5 Non-Material Amendments

An amendment to the CPS that is non-material shall become effective immediately upon publication in the Safescrypt repository in accordance with CPS § 12.12.2.1. Safescrypt's decision to designate an amendment as non-material shall be within Safescrypt's sole discretion.

12.12.2.6 Assent to Amendments

A certificate applicant and subscriber’s decision not to request revocation of his, her, or its certificate within fifteen (15) days following the publication of an amendment shall constitute agreement to the amendment.

12.12.2.7 Consent of the Controller:

In the event the Information Technology Act or Rules or Regulations framed thereunder require the consent or approval of the Controller appointed under the Act to the Amendments to CPS, the Amendments shall take effect subject to such consent or approval of the Controller.

12.13 Property Interests in Security Materials

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

• **Certificates:** Certificates are the personal property of their respective IA. Certificates issued by Safescrypt CAs and Safescrypt subordinate CAs contain a copyright notice similar to: "Copyright (c)2000 Safescrypt, All Rights Reserved" or "(c)00" in connection with Safescrypt. Permission is hereby granted to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates shall not be published in any publicly accessible repository or directory without the express written permission of Safescrypt. This restriction is intended, in part, to protect the privacy of subscribers against unauthorized republication of their certificates. Questions concerning this copyright notice should be sent to Safescrypt as listed in CPS § 12.10 (Notice), or to **practices@safescrypt.com**.

• **CPS:** This CPS is the personal property of Safescrypt Ltd.

• **Distinguished names:** Distinguished names are the personal property of the persons named (or their employer or principal).

• **Private keys:** Private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected.

• **Public keys:** Public keys are the personal property of subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected.

• **Safescrypt public keys:** Safescrypt CA public keys are the property of Safescrypt. Safescrypt licenses relying parties to use such keys only in conjunction with trustworthy hardware or software product in which the root public key is distributed by Safescrypt's authority.

• **Secret shares of private keys:** Secret shares of an IA's private key are the personal property of the applicable IA.

12.14 Infringement and Other Damaging Material

Certificate applicants (and, upon acceptance, subscribers) represent and warrant that their submission (to an IA) and use of a domain and distinguished name (and all other certificate application information) does not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to

their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Certificate applicants (and, upon acceptance, subscribers) shall defend, indemnify, and hold their IA harmless for any loss or damage resulting from any such interference or infringement.

IA's and Safescrypt shall not be responsible for nonverified subscriber information (NSI) submitted to Safescrypt, an IA, or the Safescrypt repository or otherwise submitted for inclusion in a certificate. In particular, subscribers shall be solely responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed. Because laws regarding the transmission and availability of information content are constantly changing and vary widely, certificate applicants' and subscribers' responsibilities are determined not only by laws in existence at the time the IA issues a certificate to a certificate applicant but also by any laws that may be enacted after such date. Certificate applicants and subscribers should be aware that there are many laws regarding the transmission of data, especially data that is encrypted or involves encryption algorithms, and that these laws may vary dramatically from state to state and country to country. Further, it is generally not possible to limit the distribution of content on the Internet or certain other networks based on the locality of the user / viewer, and this may require certificate applicants and subscribers to comply with the laws of each jurisdiction in which the content may be viewed or used.

Certificate applicants and subscribers will not submit to Safescrypt, an IA, or the Safescrypt repository any materials that contain statements that (i) are libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

12.15 Fees

Subject to any direction given by the Central Government under Rule 30 of the Information Technology (Certifying Authorities) Rules, 2000 Safescrypt may charge subscribers fees for their use of Safescrypt's services. A current schedule of such fees is available from the Safescrypt repository at https://www.safescrypt.com/India-Repository . Such fees are subject to change seven (7) days following their posting in the Safescrypt repository.

12.16 Choice of Cryptographic Methods

All persons acknowledge that they (not Safescrypt or any IA) are solely responsible for and have exercised independent judgment in choosing security software, hardware, and encryption / digital signature algorithms, including their respective parameters, procedures, and techniques.

12.17 Survival

The obligations and restrictions contained within CPS §§ 3.9 (Audit), 3.13 (Confidential Information), CPS § 11 (Obligations of Issuing Authorities and Safescrypt, and Limitations Upon Such Obligations), and CPS § 12 (Miscellaneous Provisions) shall survive the termination of this CPS.

12.18 Force Majeure

IA's and Safescrypt shall not be responsible for any breach of warranty, delay, or failure in performance under this CPS that results from events beyond their control, such as acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters.

***

13. APPENDICES

13.1 Definitions

A-B

ACCEPT (A CERTIFICATE)

To demonstrate approval of a certificate by a certificate applicant while knowing or having notice of its informational contents, in accordance with the INDIA CPS.

ACCESS

A specific type of interaction between a submission and communications or information resources that results in a flow of information, the exercise of control, or the activation of a process.

ACCREDITATION

A formal declaration by a Safescrypt–designated approving authority that a particular information system, professional or other employee or contractor, or organization is approved to perform certain duties and to operate in a specific security mode, using a prescribed set of safeguards.

AFFILIATED CERTIFICATE

A certificate issued to an affiliated individual. (*Cf.*, **AFFILIATED INDIVIDUAL**)

AFFILIATED INDIVIDUAL

A human being that is affiliated with an organization (i) as an officer, director, employee, partner, contractor, intern, or other person within the organization, or (ii) as a person maintaining a contractual relationship with the organization where the organization has business records providing strong assurances of the identity of such person. (*Cf.*, **AFFILIATED CERTIFICATE**)

AFFIRM / AFFIRMATION

To state or indicate by conduct that data is correct or information is true.

ALIAS

A pseudonym.

APPLICANT (*See* CA APPLICANT; CERTIFICATE APPLICANT)

ARCHIVE

To store records and associated journals for a given period of time for security, backup, or auditing purposes.

ASSURANCES

Statements or conduct intended to convey a general intention, supported by a good-faith effort, to provide and maintain a specified service by an IA. "Assurances" does not necessarily imply a guarantee that the services will be performed fully and satisfactorily. Assurances are distinct from insurance, promises, guarantees, and warranties, unless otherwise expressly indicated.

AUDIT

A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

AUTHENTICATE (*See* **AUTHENTICATION**)

AUTHENTICATED RECORD

A signed document with appropriate assurances of authentication or a message with a digital signature verified by a valid Class 3 certificate by a relying party. However, for suspension and revocation notification purposes, the digital signature contained in such notification message must have been created by the private key corresponding to the public key contained in the certificate for the applicable certificate class.

AUTHENTICATION

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (*Cf.*, **VERIFY (**a **DIGITAL SIGNATURE)**)

AUTHORIZATION

The granting of rights, including the ability to access specific information or resources.

AVAILABILITY

The extent to which information or processes are reasonably accessible and usable, upon demand, by an authorized entity, allowing authorized access to resources and timely performance of time-critical operations.

BINDING

An affirmation by an IA (or its LRA) of the relationship between a named entity and its public key.

C

CA APPLICATION (NON-SAFESCRYPT CA APPLICATION)

The application submitted to the applicable Safescrypt PCA by a non-Safescrypt entity requesting to become a certification authority or subordinate certification authority, and requesting an IA certificate, within Safescrypt's public certification services. (*See* INDIA CPS § 3.1.1)

CA APPLICANT

A person who submits a CA application to Safescrypt requesting to become a CA or subordinate CA. (*Cf.*, **SUBSCRIBER**)

CERTIFICATE (PUBLIC KEY CERTIFICATE)

A message (*see* definition for **MESSAGE**) that, at least, states a name or identifies the IA, identifies the subscriber, contains the subscriber's public key, identifies the certificate's operational period, contains a certificate serial number, and is digitally signed by the IA. All references to a "Class 1, 2, or 3 certificate" or to a "certificate" without a modifying adjective are intended as references to both "normal" and "provisional" certificates, unless the context requires otherwise. References to a certificate refer exclusively to certificates issued by an IA. (*Cf.*, **PROVISIONAL CERTIFICATE**)

CERTIFICATE APPLICANT

A person or authorized agent that requests the issuance of a public key certificate by an IA. (*Cf.*, **CA APPLICANT; SUBSCRIBER**)

CERTIFICATE APPLICATION

A request from a certificate applicant (or authorized agent) to an IA for the issuance of a certificate. (*Cf.*, **CERTIFICATE APPLICANT; CERTIFICATE SIGNING REQUEST**)

CERTIFICATE CHAIN

An ordered list of certificates containing an end-user subscriber certificate and IA certificates (*See* **VALID CERTIFICATE**)

CERTIFICATE EXPIRATION

The time and date specified in the certificate when the operational period ends, without regard to any earlier suspension or revocation.

CERTIFICATE EXTENSION

An extension field to a certificate which may convey additional information about the public key being certified, the certified subscriber, the certificate issuer, and / or the certification process. Standard extensions are defined in Amendment 1 to ISO / IEC 9594-8:1995 (X.509). Custom extensions can also be defined by communities of interest.

CERTIFICATE HIERARCHY

A Safescrypt INDIA PCS domain of IAs, each categorized with respect to its role in a "tree structure" of subordinate IAs. An IA issues and manages certificates for end-user subscribers and / or for one or more IAs at the next level. Note: an IA in a trust hierarchy must observe uniform practices addressing issues such as naming, maximum number of levels, etc., to assure integrity of the domain and thereby ensure uniform accountability, auditability, and management through the use of trustworthy operational processes.

CERTIFICATE ISSUANCE

The actions performed by an IA in creating a certificate and notifying the certificate applicant (anticipated to become a subscriber) listed in the certificate of its contents.

CERTIFICATE MANAGEMENT

Certificate management includes, but is not limited to, storage, dissemination, publication, revocation, and suspension of certificates. An IA undertakes certificate management functions by serving as a registration authority for subscriber certificates. An IA designates issued and accepted certificates as valid by publication.

CERTIFICATE OF AUTHENTICITY

A document issued by an authorized official of the jurisdiction in which an acknowledgment by a notary was taken, such as the secretary of state of a state (U.S.) to authenticate the status of a notary.

CERTIFICATE REVOCATION (*See* **REVOKE A CERTIFICATE**)

CERTIFICATE REVOCATION LIST (CRL)

A periodically (or exigently) issued list, digitally signed by an IA, of identified certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked

certificates' serial numbers, and the specific times and reasons for suspension and revocation.

CERTIFICATE SERIAL NUMBER

A value that unambiguously identifies a certificate generated by an IA.

CERTIFICATE SIGNING REQUEST (CSR)

A machine-readable form of a certificate application. (*Cf.*, **CERTIFICATE APPLICATION**)

CERTIFICATE SUSPENSION (*See* **SUSPEND A CERTIFICATE**)

CERTIFICATION / CERTIFY

The process of issuing a certificate by an IA.

CERTIFICATION AUTHORITY (CA)

A person (*see* definition for **PERSON**) authorized to issue certificates. Under the Safescrypt INDIA PCS, a CA is subordinate to a PCA. (*Cf.*, **REGISTRATION AUTHORITY; TRUSTED THIRD PARTY**)

CERTIFICATION PRACTICE STATEMENT (INDIA CPS)

This document, as revised from time to time (representing Safescrypt's statement of the practices an IA employs in issuing certificates).

CERTIFIER (*See* **ISSUING AUTHORITY)**

CHALLENGE PHRASE

A set of numbers and / or letters that are chosen by a certificate applicant, communicated to the IA with a certificate application, and used by the IA to authenticate the subscriber for various purposes as required by the INDIA CPS. A challenge phrase is also used by a secret share holder to authenticate himself, herself, or itself to a secret share issuer.

CLASS 1, 2, OR 3 CERTIFICATE

A certificate of a specified level of trust. (*See* INDIA CPS § 2.2)

COMMERCIAL REASONABLENESS

In the context of electronic commerce, the implementation and use of technology, controls, and administrative and operational procedures that reasonably ensure system and message trustworthiness.

COMMON KEY

Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, "common key" refers to this last share. It is not assumed to be secret as it is not continually in an individual's possession.

COMPROMISE

A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. (*Cf.,* **DATA INTEGRITY**)

CONFIDENTIALITY

The condition in which sensitive data is kept secret and disclosed only to authorized parties.

CONFIRM

To ascertain through appropriate inquiry and investigation. (*Cf.,* **AUTHENTICATION; VERIFY A DIGITAL SIGNATURE**)

CONFIRMATION OF CERTIFICATE CHAIN

The process of validating a certificate chain and subsequently validating an end-user subscriber certificate.

CONTROLS

Measures taken to ensure the integrity and quality of a process.

CORRESPOND

To belong to the same key pair. (*See also* **PUBLIC KEY; PRIVATE KEY**)

CROSS-CERTIFICATION

A condition in which either or both a Safescrypt PCA and a non-Safescrypt certificate issuing entity (representing another certification domain) issues a certificate having the other as the subject of that certificate.

CRYPTOGRAPHIC ALGORITHM

A clearly specified mathematical process for computation; a set of rules that produce a prescribed result.

CRYPTOGRAPHY (*Cf.,* **PUBLIC KEY CRYPTOGRAPHY**)

(i) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be

reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

(ii) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and / or prevent its unauthorized uses.

CRYPTOMODULE

A trustworthy implementation of a cryptosystem which safely performs encryption and decryption of data.

D

DATA

Programs, files, and other information stored in, communicated, or processed by a computer.

DATABASE

A set of related information created, stored, or manipulated by a computerized management information system.

DATA CONFIDENTIALITY (*See* **CONFIDENTIALITY**)

DATA INTEGRITY

A condition in which data has not been altered or destroyed in an unauthorized manner. (*See also* **THREAT;** *cf.*, **COMPROMISE**)

DEMO CERTIFICATE

A certificate issued by an IA to be used exclusively for demonstration and presentation purposes and not for any secure or confidential communications. Demo certificates may be used by authorized persons only.

DENIAL OF SERVICE (*See* **AVAILABILITY**)

DIGITAL SIGNATURE

A transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the message has been altered since the transformation was made.

DIRECTORY (*Cf.*, **REPOSITORY**)

DISTINGUISHED NAME

A set of data that identifies a real-world entity, such as a person in a computer-based context. (*e.g.*, countryName=IN, state=Tamil Nadu, organizationName=Electronic Ltd., commonName=Deepak Patel).

DOCUMENT

A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information. (*Cf.*, **MESSAGE; RECORD**)

E-F

ELECTRONIC MAIL ("E-MAIL")

Messages sent, received or forwarded in digital form via a computer-based communication mechanism.

EMPLOYEE IN GOOD STANDING

A non-probationary employee that has not been terminated or suspended, and is not the subject of pending disciplinary action, by his or her employer.

ENCRYPTION

The process of transforming plaintext data into an unintelligible form (ciphertext) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

END-USER SUBSCRIBER

A subscriber which is not also an IA.

ENHANCED NAMING

The use of an extended organization field (OU=) in an X.509 v3 certificate.

ENROLLMENT

The process of a certificate applicant's applying for a certificate.

ENTITY (*See* **PERSON**)

EXTENSIONS

Extension fields in X.509 v3 certificates. (*See* **X.509**)

FILE TRANSFER PROTOCOL (FTP)

The application protocol that offers file system access from the Internet suite of protocols.

FREE CERTIFICATE

A certificate issued by an IA such that the IA does not charge the subscriber a fee for the certificate or otherwise receive compensation.

FTP (*See* **FILE TRANSFER PROTOCOL**)

G-H

GENERATE A KEY PAIR

A trustworthy process of creating private keys during certificate application whose corresponding public key are submitted to the applicable IA during certificate application in a manner that demonstrates the applicant's capacity to use the private key.

GLOBAL SERVER CERTIFICATE

A certificate-based service that allows approved server certificate subscribers to operate in a strong encryption mode, and as a result, allows a browser accessing such a server to also operate in such strong encryption mode.

HASH (HASH FUNCTION)

An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that

i. A message yields the same result every time the algorithm is executed using the same message as input.

ii. It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.

iii. It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

I

IA (*See* ISSUING AUTHORITY)

IA CERTIFICATE

A certificate issued by an authorized superior IA to a subordinate IA. (*See* **SUPERIOR IA; SUBORDINATE IA**; *cf.*, **CERTIFICATE**)

IDENTIFICATION / IDENTIFY

The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of certificates.

IDENTITY

A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

INCORPORATE BY REFERENCE

To make one message a part of another message by identifying the message to be incorporated, with information that enables the receiving party to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message to the extent permitted by law.

INTEGRITY (*See* **DATA INTEGRITY**)

ISSUING A CERTIFICATE (*See* **CERTIFICATE ISSUANCE**)

ISSUER (*See* **ISSUING AUTHORITY**)

ISSUING AUTHORITY (IA)

Within Safescrypt's INDIA PCS, PCA, or CA (or subordinate CA) that issues, suspends, or revokes a certificate. IAs are identified by a distinguished name on all certificates and CRLs they issue. With prior approval by Safescrypt, an IA may delegate the responsibility to evaluate and approve or reject certificate applications to one or more LRAs not owned or operated by the IA under INDIA CPS § 2.1.3. When such delegation occurs and where the context requires, the term "IA" in this INDIA CPS shall include such LRAs with respect to the delegating IA's obligations, representations, warranties, and disclaimers.

J-L

KEY GENERATION

The trustworthy process of creating a private key / public key pair. The public key is supplied to an IA during the certificate application process.

KEY PAIR

A private key and its corresponding public key. The public key can verify a digital signature created by using the corresponding private key. In addition, depending upon the type of algorithm implemented, key pair components can also encrypt and decrypt information for confidentiality purposes, in which case a private key uniquely can reveal information encrypted by using the corresponding public key.

LOCAL REGISTRATION AUTHORITY (LRA)

An entity approved by an IA to assist persons in applying for certificates, revoking (or where authorized, suspending) their certificates, or both and also approving such applications. An LRA is not the agent of a certificate applicant. An LRA may not delegate the authority to approve certificate applications other than to authorized LRAAs of the LRA. (*Cf.*, **LOCAL REGISTRATION AUTHORITY ADMINISTRATOR**)

LOCAL REGISTRATION AUTHORITY ADMINISTRATOR (LRAA)

An employee of an LRA that is responsible for carrying out the functions of an LRA. (*Cf.*, **LOCAL REGISTRATION AUTHORITY**)

M-N

MESSAGE

A digital representation of information; a computer-based record. A subset of **RECORD**. (*Cf.*, **RECORD**)

MESSAGE INTEGRITY (*See* **DATA INTEGRITY**)

NAME

A set of identifying attributes purported to describe an entity of a certain type.

NAMING

Naming is the assignment of descriptive identifiers to objects of a particular type by an authority which follows specific issuing procedures and maintains specific records pertinent to an identified registration process. (*Cf.*, **NAMING AUTHORITY; SAFESCRYPT NAMING AUTHORITY**)

NAMING AUTHORITY

A body which executes naming policy and procedures and has control over the registration and assignment of primitive (basic) names to objects of a particular class. (*Cf.*, **NAMING; SAFESCRYPT NAMING AUTHORITY**)

NONREPUDIATION

Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of nonrepudiation. By way of illustration, a

digital signature verified pursuant to this INDIA CPS can provide proof in support of a determination of nonrepudiation by a trier of fact, but does not by itself constitute nonrepudiation.

NONVERIFIED SUBSCRIBER INFORMATION (NSI)

Information submitted by a certificate applicant to an IA, and included within a certificate, which has not been confirmed by the IA and for which the IA provides no assurances other than that the information was submitted by the certificate applicant. Information such as titles, professional degrees, accreditations, and Registration Field Information are considered NSI unless otherwise indicated.

NON-SAFESCRYPT IA

An IA that is not owned or operated by Safescrypt. (*See* INDIA CPS § 3.1; *Cf.*, **ISSUING AUTHORITY**)

NON-SAFESCRYPT ORGANIZATIONAL LRA

An LRA that is not owned or operated by Safescrypt and is restricted to performing LRA functions in connection with certificates issued to affiliated individuals that are affiliated with it. (*See* INDIA CPS § 2.5.4; *Cf.*, **LOCAL REGISTRATION AUTHORITY; AFFILIATED INDIVIDUALS**)

NORMAL CERTIFICATE (*See* **CERTIFICATE**)

NOTARY PUBLIC

A natural person authorized to perform certification services such as taking acknowledgments, administering oaths or affirmations, witnessing or attesting signatures, and noting protests of negotiable instruments, as prescribed by applicable national law.

NOTICE

The result of notification in accordance with this INDIA CPS. (*See* INDIA CPS § 12.10)

NOTIFY

To communicate specific information to another person as required by this INDIA CPS and applicable law.

O-P

ON-LINE

Communications that provide a real-time connection to the Safescrypt INDIA PCS.

OPERATIONAL CERTIFICATE

A certificate which is within its operational period at the present date and time or at a different specified date and time, depending on the context.

OPERATIONAL PERIOD

The period starting with the date and time a certificate is issued (or on a later date and time certain if stated in the certificate) and ending with the date and time on which the certificate expires or is earlier suspended or revoked.

ORGANIZATION

An entity with which a user is affiliated. An organization may also be a user.

ORIGINATOR

A person by whom (or on whose behalf) a data message is purported to have been generated, stored, or communicated. It does not include a person acting as an intermediary.

PARTIES

The entities whose rights and obligations are intended to be controlled by this INDIA CPS. These entities may include certificate applicants, IAs, subscribers, and relying parties. (*See* **USER; ISSUING AUTHORITY; RELYING PARTY**)

PASSWORD (PASS PHRASE; PIN NUMBER)

Confidential authentication information, usually composed of a string of characters used to provide access to a computer resource.

PC CARD (*See also* **SMART CARD**)

A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

PERSON

A human being or an organization (or a device under the control of a human being or organization) capable of signing or verifying a message, either legally or as a matter of fact. (A synonym of **ENTITY**.)

PERSONAL PRESENCE

The act of appearing (physically rather than virtually or figuratively) before an LRA or its designee and proving one's identity as a prerequisite to certificate issuance under certain circumstances.

PKI HIERARCHY

A set of IAs whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior IA.

PRIMARY CERTIFICATION AUTHORITY (PCA)

A person that establishes practices for all certification authorities and users within its domain.

PRIVATE KEY

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key. (*See also* **PUBLIC KEY CRYPTOGRAPHY; PUBLIC KEY**)

PROVISIONAL CERTIFICATE

A Class 2 certificate during the first 21 days of its operational period that is issued upon the successful completion of all required IA-internal validation procedures with respect to a Class 2 certificate application (in accordance with INDIA CPS § 5.1). The provisional state denotes that further validation of the certificate application regarding the subscriber's identity will be completed through a postal address "mail-back" procedure (*See* INDIA CPS § 5.1.4 - Postal Address Confirmation; *Cf.*, **CERTIFICATE**)

PUBLIC CERTIFICATION SERVICES (*See* SAFESCRYPT PUBLIC CERTIFICATION SERVICES)

PUBLIC KEY

A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files which can then be decrypted with the corresponding private key. (*See also* **PUBLIC KEY CRYPTOGRAPHY; PRIVATE KEY**)

PUBLIC KEY CERTIFICATE (*See* **CERTIFICATE**)

PUBLIC KEY CRYPTOGRAPHY (*Cf.*, **CRYPTOGRAPHY**)

A type of cryptography that uses a key pair of mathematically related

cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

PUBLIC KEY INFRASTRUCTURE (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. The PKI consists of systems which collaborate to provide and implement the INDIA PCS and possibly other related services.

PUBLIC/PRIVATE KEY PAIR (*See* **PUBLIC KEY; PRIVATE KEY; KEY PAIR**)

PUBLISH / PUBLICATION

To record or file information in the Safescrypt repository and optionally in one or more other repositories in order to disclose and make publicly available such information in a manner that is consistent with this INDIA CPS and applicable law.

Q-R

QUALIFIER (*See* **SAFESCRYPT QUALIFIER**)

RECIPIENT (of a **DIGITAL SIGNATURE**)

A person who receives a digital signature and who is in a position to rely on it, whether or not such reliance occurs. (*Cf.*, **RELYING PARTY**)

RECORD

Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term "record" is a superset of the two terms "document" and "message". (*Cf.*, **DOCUMENT; MESSAGE**)

RE-ENROLLMENT (*Cf.*, **RENEWAL**)

REGISTERED STRING

A class of object subject to registration and recording procedures which demonstrates the value is unambiguous within the records of the registration authority. The type of value recorded is a string of characters.

REGISTRATION AUTHORITY

An entity trusted to register other entities and assign them a relative

distinguished value such as a distinguished name or, a hash of a certificate. A registration scheme for each registration domain ensures that each registered value is unambiguous within that domain. (*Cf.*, **CERTIFICATION AUTHORITY**)

REGISTRATION FIELD INFORMATION

Country, zip code, age, and gender data included within designated certificates at the option of the subscriber.

RELATIVE DISTINGUISHED NAME (RDN)

A set of attributes comprising an entity's distinguished name that distinguishes the entity from others of the same type.

RELY / RELIANCE (on a **CERTIFICATE** and **DIGITAL SIGNATURE**)

To accept a digital signature and act in a manner that could be detrimental to oneself were the digital signature to be ineffective. (*Cf.*, **RELYING PARTY; RECIPIENT**)

RELYING PARTY

A recipient who acts in reliance on a certificate and digital signature. (*Cf.*, **RECIPIENT; RELY OR RELIANCE (**on a **CERTIFICATE** and **DIGITAL SIGNATURE**))

RELYING PARTY AGREEMENT

The agreement between a Relying Party and the IA.

RENEWAL

The process of obtaining a new certificate of the same class and type for the same subject once an existing certificate has expired.

REPOSITORY

A database of certificates and other relevant information accessible on-line.

REPUDIATION (*See also* **NONREPUDIATION**)

The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REVOKE A CERTIFICATE

The process of permanently ending the operational period of a certificate from a specified time forward.

ROOT

The IA that issues the first certificate in a certification chain. The root's

public key must be known in advance by a certificate user in order to validate a certification chain. The root 's public key is made trustworthy by some mechanism other than a certificate, such as by secure physical distribution.

RSA

A public key cryptographic system invented by Rivest, Shamir & Adelman.

S

SAFESCRYPT NAMING AUTHORITY

A Safescrypt registration authority that establishes and enforces controls over and has decision-making authority regarding the issuance of relative distinguished names for all IAs (but not for end-user subscribers). (*Cf.*, **NAMING AUTHORITY**).

SAFESCRYPT INDIA PUBLIC CERTIFICATION SERVICES (INDIA PCS)

The certification system provided by Safescrypt and any Safescrypt-authorized IAs described in this INDIA CPS.

SAFESCRYPT QUALIFIER

A data syntax facilitating the representation of a set of values which restrict the meaning of the Safescrypt INDIA CPS. The qualifier value augments the standard certificate policy extension present in all certificates according to the rules defined by X.509 for that extension type.

SAFESCRYPT SECURITY POLICY (SSP)

The document describing Safescrypt's internal security policies.

SECRET SHARE

A portion of a cryptographic secret split among a number of physical tokens.

SECRET SHARE HOLDER

An authorized holder of a physical token containing a secret share.

SECRET SHARE ISSUER

The person designated by an IA to create and distribute secret shares.

SECRET SHARING (*See also* **SECRET SHARE)**

The practice of distributing secret shares of a private key to a number of secret share holders; threshold-based splitting of keys.

SECURE CHANNEL

A cryptographically enhanced communications path that protects messages against perceived security threats.

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations.

SECURITY POLICY

A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system in support of the INDIA PCS.

SECURITY SERVICES

Services provided by a set of security frameworks and performed by means of certain security mechanisms. Such services include, but are not limited to, access control, data confidentiality, and data integrity.

SELF-SIGNED PUBLIC KEY

A data structure that is constructed the same as a certificate but that is signed by its subject. Unlike a certificate, a self-signed public key cannot be used in a trustworthy manner to authenticate a public key to other parties.

SERIAL NUMBER (*See* **CERTIFICATE SERIAL NUMBER**)

SERVER

A computer system that responds to requests from client systems.

SIGN

To create a digital signature for a message, or to affix a signature to a document, depending upon the context.

SIGNATURE

A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances. (*Cf.,* **DIGITAL SIGNATURE**)

SIGNER

A person who creates a digital signature for a message, or a signature for a document.

SMART CARD

A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/MIME

A specification for E-mail security exploiting a cryptographic message syntax in an Internet MIME environment.

SUBJECT (OF A CERTIFICATE)

The holder of a private key corresponding to a public key. The term "subject" can refer to both the equipment or device that holds a private key and to the individual person, if any, who controls that equipment or device. A subject is assigned an unambiguous name which is bound to the public key contained in the subject's certificate.

SUBJECT NAME

The unambiguous value in the subject name field of a certificate which is bound to the public key.

SUBORDINATE IA

Within the Safescrypt PKI architecture's hierarchy of IAs, each IA is either a PCA, a CA or a "subordinate CA". The PCA's subordinate IA is a CA; a CA's subordinate IA is a subordinate CA. If present, a subordinate CA's subordinate IA is yet another subordinate CA. (*Cf.*, **SUPERIOR IA**)

SUBSCRIBER

A person who is the subject of, has been issued a certificate, and is capable of using, and authorized to use, the private key that corresponds to the public key listed in the certificate. (*See also* **SUBJECT**; *cf.*, **CERTIFICATE APPLICANT; USER**)

SUBSCRIBER AGREEMENT

The agreement executed between a subscriber and an IA for the provision of designated public certification services in accordance with this INDIA CPS.

SUBSCRIBER INFORMATION

Information supplied to a certification authority as part of a certificate application. (*Cf.*, **CERTIFICATE APPLICATION**)

SUPERIOR IA

Within the Safescrypt PKI architecture's hierarchy of IAs, each IA is either a PCA, a CA or a "subordinate CA". The superior IA of a subordinate CA is either another subordinate CA or a CA; a CA's superior is a PCA; a PCA's superior is itself. **(***Cf.*, **SUBORDINATE IA)**

SUSPEND A CERTIFICATE

A temporary "hold" placed on the effectiveness of the operational period of a certificate without permanently revoking the certificate. A certificate suspension is invoked by, *e.g.*, a CRL entry with a reason code. (*Cf.*, **REVOKE A CERTIFICATE**)

T

TEST CERTIFICATE

A certificate issued by an IA for the limited purpose of internal technical testing. Test certificates may be used by authorized persons only. (*See* INDIA CPS
§ 2.2.4).

THREAT

A circumstance or event with the potential to cause harm to a system, including the destruction, unauthorized disclosure, or modification of data and/or denial of service.

TIME STAMP

A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

TOKEN

A hardware security token containing a user's private key(s), public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

TRANSACTION

A computer-based transfer of business information which consists of specific processes to facilitate communication over global networks.

TRUST

Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and an IA. An authenticating entity must be certain that it can trust the IA to create only valid and reliable certificates, and users of those certificates rely upon the authenticating entity's determination of trust.

TRUSTED PERSON

A person who serves in a trusted position and is qualified to serve in it in accordance with this INDIA CPS. (*Cf.*, **TRUST; TRUSTED POSITION; TRUSTED THIRD PARTY; TRUSTWORTHY SYSTEM**)

TRUSTED POSITION

A role within an IA that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.

TRUSTED ROOT

A trusted root is a public key which has been confirmed as bound to an IA by a user or system administrator. Software and systems implementing authentication based on public cryptography and certificates assume that this key value has been correctly obtained. It is confirmed by always accessing it from a trusted system repository to which only identified and trusted administrators have modification authorizations.

TRUSTED THIRD PARTY

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. A trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship. (*Cf.*, **TRUST**)

TRUSTWORTHY SYSTEM

Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

TYPE (OF CERTIFICATE)

The defining properties of a certificate which limit its intended purpose to a class of applications uniquely associated with that type.

U-V

UNAMBIGUOUS NAME (*See* **DISTINGUISHED NAME**)

UNIFORM RESOURCE LOCATOR (URL)

A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

USER

An authorized entity that uses a certificate as applicant, subscriber, recipient or relying party, but not including the IA issuing the certificate. (*Cf.*, **CERTIFICATE APPLICANT; ENTITY; PERSON; SUBSCRIBER**)

VALID CERTIFICATE

A certificate issued by an IA and accepted by the subscriber listed in it.

VALIDATE A CERTIFICATE (*i.e.,* of an **END-USER SUBSCRIBER CERTIFICATE)**

The process performed by a recipient or relying party to confirm that an end-user subscriber certificate is valid and was operational at the date and time a pertinent digital signature was created.

VALIDATE A CERTIFICATE CHAIN

For each certificate in a chain, the process performed by the recipient or relying party to authenticate the public key (in each certificate), confirm that each certificate is valid, was issued within the operational period of the corresponding IA certificate, and that all parties (IAs, end-user subscribers, recipients, and relying parties) have operated in accordance with this INDIA CPS as to all certificates in the chain.

VALIDATION (OF CERTIFICATE APPLICATION)

The process performed by the IA (or its LRA) following submission of a certificate application as a prerequisite to approval of the application and the issuance of a certificate. (*Cf.,* **AUTHENTICATION**)

VERIFY (a **DIGITAL SIGNATURE)**

In relation to a given digital signature, message, and public key, to determine accurately that (i) the digital signature was created during the operational period of a valid certificate by the private key corresponding to the

public key contained in the certificate and (ii) the associated message has not been altered since the digital signature was created. (*Cf.*, **AUTHENTICATION**; **CONFIRM**)

W-Z

WORLD WIDE WEB (WWW)

A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

WRITING

Information in a record that is accessible and usable for subsequent reference.

X.509

The ITU-T (International Telecommunications Union-T) standard for certificates. X.509 v3 refers to certificates containing or capable of containing extensions.

***

13.2 Index

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

14.