CERTIFICATION PRACTICE STATEMENT

Digital Signature Certification Services

Document Number	CPS
Version Number	1.0
Release Date	22.02.2016
Classification	Public

EXECUTIVE SUMMARY

Capricorn Identity Services Pvt. Ltd. – Certifying Authority (hereinafter referred to as "Capricorn CA") is a Certifying Authority licensed under the Indian IT Act 2000 read with Indian IT Act, 2008 (Amendment). As a Certifying Authority, Capricorn CA is authorized to issue Digital Signature Certificates to individuals, organizations, websites, devices and so on. Capricorn CA is promoted by the directors of M/S Capricorn Infotech Pvt. Ltd., a company with two decades of experience in secure access and authentication solutions and e-commerce.

This CPS is intended to act as a guide and control document for all the stakeholders participating in Digital Signature Certificate issuance, management and usage. The primary stakeholders and users of this document are: Capricorn CA, the Subscribers, the Relying Parties, the Office of the Controller of Certifying Authorities and the Applicants. The applicants after being issued the certificate are defined as the subscribers. Each of the applicants, is specifically advised to go through the provisions of the CPS to understand its rights and obligations. The CPS document defines the rights and obligations of other participating entities as well.

The document captures the process of identifying an individual applicant and the detailed procedure involved in issuance of a certificate. It also describes the procedures for revocation of certificates. In accordance with the provisions of the IT Act and various rules and regulations concerning Digital Signature Certificate and as per prevailing standards, Capricorn CA offers different classes of

certificates based on the trust levels. Accordingly, the procedures for the identification of applicants are different for the different classes of Certificates. Also these procedures conform to “Identity Verification Guidelines” issued by the Office of Controller of Certifying Authorities.

Issuance of ‘Digital Certificates’ being ‘Trust’ business, the document describes in detail the various security measures adopted by Capricorn CA for handling the sensitive information of the subscribers as well secure issuance and distribution of keys. The document also covers the various audit requirements and practices followed by the Capricorn CA for safe and reliable operations.

TABLE OF CONTENTS

PAGE LEFT BLANK INTENTIONALLY

1. Introduction

1.1 Background

Capricorn CA has been promoted by M/S Capricorn Identity Services Pvt. Ltd. which in turn is promoted by the directors of Capricorn Infotech Pvt. Ltd. M/S Capricorn Infotech has been in the business of providing solutions related to authentication, secure access and distribution of crypto tokens for 20 years.

This document is the Certification Practice Statement (CPS) of Capricorn Certifying Authority (Capricorn CA), a Certifying Authority defined under the Indian IT Act 2000 with its various amendments. This document follows the guidelines and rules and regulations formulated by the Controller of Certifying Authorities in exercise of his powers under the Indian IT Act 2000 and IT Act 2008 (amendments) read with various amendments issued from time to time.

This document has been prepared in general conformity to the RFC 2527 guidelines, wherever possible. There may be some variations in details and headings in order to meet the requirements of Capricorn CA as set forth by the Office of the CCA and Indian IT Act 2000 and IT Act 2008 (amendments) and the accompanying guidelines, rules and regulations, which are specific to the requirements of Electronic Signature Certificates.

It is assumed that the reader perusing this document is generally familiar with Public Key Infrastructure (PKI) and associated terminologies.

1.1.1 Introduction

This Certification Practice Statement (CPS) of M/S Capricorn Identity Services Pvt. Ltd. (hereinafter referred to as Capricorn Certifying Authority or Capricorn CA) outlines the practices that Capricorn CA follows to provide Digital Signature Certificates and related services to the general public, organizations and websites. This document governs the services provided by Capricorn CA and establishes the conformance to

The CPS is the principal practice statement governed by the Information Technology Act, 2000 (IT Act). All transactions carried out by electronic means like electronic data interchange and electronic means of communication, electronic commerce, electronic governance etc. are granted legal recognition under the Information Technology Act.

This CPS outlines the rights and obligations of the Certifying Authority, the subscribers or the applicants for Digital Signature Certificates, the Relying Parties which trust the Digital Certificates issued by the Certifying Authority.

The applicants for the Digital Signature Certificates are specifically instructed to go through the provisions contained in this document. They are also, specifically, cautioned about the requirements and guidelines for identification before applying for a Digital Signature Certificate. As the Digital Signature Certificates offered may have different 'Trust Levels', it is informed to the applicants to familiarize themselves with different rights and privileges as well as obligations applicable under each class of Digital Signature Certificates.

1.1.2 Overview

1.1.2.1 Capricorn CA has been licensed by the office of the Controller of Certifying Authorities, under the powers conferred on it by the Indian IT Act 2000 and its various amendments in force.

1.1.2.2 Capricorn CA has set up a facility for generation and management of Electronic Signature Certificates to enable on-line e-Commerce, e-Governance and other such applications which make use of authentication and electronic signatures.

1.1.2.3

1.1.2.4 To support its role as a Trusted Third Party providing Digital Signature Certificate services, 'Capricorn CA' has developed a framework captured in the document form as a Certificate Practice Statement (CPS). This document outlines the practices to control issuance and management of Digital Signature Certificates 1.1.2.5 The 'Caprico

1.2 Scope

The Certification Services of **Capricorn Identity Services Pvt. Ltd. – Certifying Authority** (hereinafter referred to as "Capricorn CA") are subject to various Indian Laws and jurisdiction of courts in India in accordance with, but not limited to, the Information Technology Act, 2000 (hereinafter referred to as "the Act"), the Rules and Regulations defined therein and the Information Technology Act (Amendment) 2008.

Use of Digital Signature Certificates should be as per the Information Technology Act and the Practices specified in the Certification Practice Statement (this document). Any violation shall be liable and shall be subject to punishment under the relevant law(s) of the Republic of India.

Capricorn CA reserves the right to proceed against or assist in the trial of any individual / organization who commits an offence in violation of the Act.

1.3 Definitions

This document makes use of the following defined terms:

- Activation data - Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass-phrase, or a manually-held key share).
- Authentication - The process of establishing that individuals, organizations, or things are who or what they claim to be. In the

context of a PKI, authentication can be the process of establishing that an individual or organization applying for or seeking access to something under a certain name is, in fact, the proper individual or organization. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organizations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organization, or device. Thus, it is said that a Digital Signature Certificate of a message authenticates sender of the message.

- Certificate policy - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
- Certification path - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
- Identification - The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization.

- Participant - An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate issuing authority, repository service provider or similar entity.
- Registration authority (RA) - . An entity appointed by Capricorn CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of subscriber credentials.

- Relying party - A recipient who acts in reliance on the digital signature certificate after verifying the authenticity of that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.
- Set of provisions - A collection of practices and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.
- Subject Certifying Authority (subject CA) - In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing Certifying Authority).
- Subscriber Agreement - An agreement between a CA and a Subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.
- Validation - The process of identification of certificate applicants. "Validation" is a subset of "identification" and refers to

identification in the context of establishing the identity of certificate applicants.

1.4 Contact Details

Capricorn CA welcomes suggestions and recommendations from Subscribers and the public for the improvement of Services offered by the Company.

Please contact us through our website on www.certificate.digital or at any of the below mentioned details:

709, Roots Tower, Plot -7, Laxmi Nagar District Centre, Delhi 110 092. Or through Telephone 011 – 224 22444 or Toll Free : 1800 – 53 – 22444 or through eMail : Support@Certificate.Digital

2. General Provisions

2.1 Obligations

2.1.1 Certifying Authority (CA) Obligations

2.1.1.1 Receive, maintain and renew the license from the Controller of Certifying Authorities (CCA) as per the Act and the Policies of Capricorn CA

2.1.1.2 Offer CA services and perform CA operations as stated in this CPS and as per the provisions of the IT Act.

2.1.1.3 Maintain the infrastructure, including all required operations of the infrastructure, securely and in conformance with the Act and provisions of this CPS.

2.1.1.4 Appoint a Registration Authority (RA) to execute duties and functions as per the provisions of this CPS. However, the Certifying Authority shall be responsible at all times for offering CA services and performing CA operations.

2.1.1.5 Capricorn CA shall not be liable for any loss, damage or penalty resulting from delays or failures in performance resulting from acts of God or other causes beyond its control. For purposes of clarity, such events shall include, but without limitation to, strikes, or other labour disputes, riots, terrorist actions, civil disturbances, actions or inactions of suppliers, acts of God, war, fire, explosion, earthquake, flood or other catastrophes.

Note : In any of the events mentioned hereof, Capricorn CA shall for the duration of such event be relieved of any and all obligations, responsibilities and duties covered in this CPS.

2.1.2 Registration Authority (RA) Obligations

The RA Administrator obligations are as listed hereunder :

2.1.2.2 Co-ordinate operations to ensure an effective and efficient verification and administration of Applications received from Subscribers.

2.1.2.3 Receive physical applications for issuance, renewal, revocation or suspension of Digital Signature Certificates (DSC).

Note : Subscribers shall be authenticated and their applications shall be verified as per rules laid down and modified from time-to-time.

2.1.2.4 Interact with the Subscriber to ensure an effective and efficient Customer service.

2.1.2.5 Report to the Certifying Authority of the activities performed.

2.1.3 Subscriber Obligations

2.1.3.1

2.1.3.2 Submit true, correct and complete documentation for Certificate subscription and renewal.

2.1.3.3 Follow the Terms and Conditions for the use of the DSC as prescribed in this CPS.

2.1.3.4 Generate the key pair as specified in this CPS.

2.1.3.5 Observe and comply with the security requirements of the private keys as specified in this CPS.

2.1.3.6 Ensure that only the Subscriber has access to the private keys.

2.1.3.7 Report any error or defect in the DSC immediately to the RA. Any subsequent changes to the DSC shall also be reported to the RA. The mode of communication for reporting shall be as prescribed in this CPS.

2.1.3.8 The Subscriber shall renew, if required, the DSC before the expiry date as prescribed in this CPS.

2.1.3.9 If the Subscriber's keys are compromised, the Subscriber shall inform Capricorn CA immediately to revoke the compromised keys.

2.1.3.10 Capricorn CA shall not be responsible and liable for use / distribution / circulation of the DSC by the Subscriber / Relying Party. Subscribers and Relying Parties are duty bound to use the DSC only for legal and lawful purposes. Capricorn CA disclaims any

liability / damage / loss arising out of / due to any circumstances / situations beyond the control of Capricorn CA.

2.1.4 Relying Party Obligations

2.1.4.1 The Relying Party is solely responsible to verify the purpose for which the DSC has been accepted.

2.1.4.2 The Relying Party shall use the DSC for the purpose for which it was intended.

2.1.4.3 The Relying Party is solely responsible to verify the authenticity of the DSC against the current Certificate Revocation List (CRL) as per the provisions of this CPS.

2.1.5 Repository Obligations

2.1.5.1 Capricorn CA shall publish the CPS, in its entirety, in its Repository whenever there is a change.

2.1.5.2 Capricorn CA shall publish and update the repository on issuance and revocation of each DSC.

2.1.5.3 Capricorn CA shall maintain in its Repository all CRL. The CRL shall be automatically updated and published upon revocation of any certificate.

2.2 Liability

2.2.1 Warranties and limitations on warranties

2.2.1.1 Warranties

Capricorn CA warrants that :

2.2.1.1.1 It has taken adequate precautions for the issuance, maintenance, renewal and revocation of the DSCs with the implementation of robust technologies with adequate failover features, adoption of standard operating procedures and placement of trained personnel to ensure an effective and efficient business environment.

2.2.1.1.2 The CA shall perform its duties and obligations for issuance, renewal and revocation as prescribed in the IT Act.

2.2.1.1.3 The CRL will be updated on revocation of the DSC by Capricorn CA.

The Subscriber warrants that :

2.2.1.1.4 All information provided by the Subscriber in the Application is true and correct at the time of the issue of the DSC

2.2.1.1.5 All information contained in the DSC is true and correct

2.2.1.1.6 The private keys shall be secured and kept confidential as per the provisions prescribed in this CPS

2.2.1.1.7 The Subscriber will immediately inform Capricorn CA for revocation of the DSC in case of any compromise / loss of the Private Key.

2.2.1.2 **Limitations on Warranties**

2.2.1.2.1 Capricorn CA makes no other warranties other than those expressly stated in this CPS.

2.2.1.2.2 Capricorn CA does not warrant any loss, damage or consequences arising out of compromised private keys, which are not expressly brought to the attention of Capricorn CA by the Subscribers.

2.2.2 Kinds of damages covered

2.2.2.1 Unless specifically stated in this CPS, Capricorn CA including its directors, employees, agents, representatives etc. shall not be responsible and liable for Capricorn CA services for any direct, indirect, consequential, remote loss/damage of any kind including but not limited to loss of data, loss of goodwill, loss of profits, loss of business, loss of opportunities, loss of reputation etc., caused by whatever acts/omissions/failures/defaults/negligence etc., of Capricorn CA including its directors, employees, agents, representatives etc.

2.2.3 Loss limitations (caps) per certificate or per transaction

2.2.3.1 Capricorn CA disclaims any liability that may arise from the use of the DSC other than that prescribed by the Act and / or provisions of this CPS.

2.2.3.2 Subject to the provisions of this clause, in the event that (i) any limitation or provision contained in this Agreement is held as

invalid for any reason; and / or (ii) Capricorn CA breaches any of its obligations pursuant to Section 2.1 above, and / or (iii) Capricorn CA becomes liable for loss or damage that would otherwise have been excluded hereunder or excludable in law, Capricorn CA shall only be liable for any such loss or damages if such loss or damage arose or is incurred during the subscription period. The aggregate liability of the Capricorn CA to all the parties collectively under any circumstances (including without limitation a subscriber, an applicant or a relying party) shall not exceed the applicable liability cap for such certificate set forth in each class in table below.

	Class of Certificate	**Liability Caps (Rs.)**
1.	Class 1 - Individual	1,000.00
2.	Class 1 - Organisational	1,000.00
3.	Class 2 - Individual	2,000.00
4.	Class 2 - Organisational	5,000.00
5.	Class 3	10,000.00

2.2.4 Other exclusions

Capricorn CA is not liable for any loss or damage:

2.2.4.1 due to indirect, consequential or punitive damages arising from or in connection with its services.

2.2.4.2 of any kind for any unauthorized use of DSC issued and use of DSC beyond the prescribed usage.

2.2.4.3 caused by fraudulent or negligent use of DSC or CRL

2.2.4.4 due to any incorrect or false information provided by the Subscriber.

2.2.4.5 resulting from delays or failures in performance due to war, riots, natural disasters, acts of terrorism, act of God or other uncontrollable forces

2.2.4.6 Incurred between the times a Certificate is revoked and the next scheduled issuance of the CRL

Capricorn CA assumes no liability for indirect, special, incidental or consequential damages, or for any loss of data / information or other indirect, consequential or punitive damages arising from or in connection with its services. Except as expressly provided in this CPS, Capricorn CA disclaims all other warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided.

2.3 Financial Responsibility

Capricorn CA does not provide any warranty of any financial transactions between the Subscriber and relying parties carried out through the DSC issued by Capricorn CA. The Subscriber and

the relying parties shall be responsible for any damage, loss or any consequence arising out of such transactions.

2.3.1 Indemnification of Certifying Authority by relying parties

2.3.1.1 Indemnification by Subscribers

2.3.1.1.1 To the extent authorized by the Act, the Subscriber shall indemnify and hold Capricorn CA, the RA, its agents, or employees harmless against any and all claims, demands, damages, liabilities and costs incurred by the Subscriber which directly or indirectly result from, or arise in connection with :

- any incorrect or false information provided by the Subscriber for any reason whatsoever.
- any kind for any unauthorized use of DSC issued and use of DSC beyond the prescribed usage.
- causes due to fraudulent or negligent use of DSC.
- failure to protect the Subscriber's private keys.
- delay in informing Capricorn CA of compromise of the Subscriber's DSC and / or private keys.
- Misrepresentations for any reasons, made to Relying Parties through the use of the DSC.

2.3.1.2 Indemnification by Relying Parties

2.3.1.2.1 To the extent authorized by the Act, the Relying Party shall indemnify and hold Capricorn CA, the RA, its agents, or employees harmless against any and all claims, demands, damages, liabilities and costs incurred by the Relying Party which directly or indirectly result from, or arise in connection with :

- relying on the DSC for purposes other than that permitted for the corresponding class of DSC
- not validating the DSC before using the DSC
- relying on DSC that has been expired, revoked or is not valid.

2.3.2 Fiduciary relationships between the various entities

2.3.2.1 Capricorn CA, the RA, its agents, or employees shall be involved in the issuance, renewal, suspension and revocation of the DSC. This act does not constitute Capricorn CA as a principal, agent, fiduciary, trustee or representative to the Subscriber or any Relying Party.

2.3.3 Administrative processes

2.3.3.1 Administrative obligations like Annual Report and other statutory obligations shall be published as per the laws of the country.

2.4 Interpretation and Enforcement

2.4.1 Governing laws

2.4.1.1 The laws of the Government of India, the IT Act 2000 and any amendment to the Act hereafter, its Rules and Regulations and the Guidelines of the Controller of Certifying Authorities (CCA)

shall govern the construction, validity, enforceability and performance of this CPS.

2.4.2 Severability, Survival, Merger and Notice

2.4.2.1 Severability

2.4.2.1.1 If any part(s) of this CPS is held to be illegal or otherwise unenforceable, the remainder of the contract shall still apply.

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.

2.4.2.2 Survival

2.4.2.2.1 The obligations and restrictions contained within CPS (Audit, Confidential Information, Obligations of Capricorn CA and the RA shall survive the termination of this CPS.

2.4.2.3 Merger

2.4.2.3.1 Should Capricorn CA merge with another entity, the obligations and restrictions (Audit, Confidential Information, Obligations of the CA and the RA, and limitations upon such obligations) shall be borne by the new entity thus created by the merger.

2.4.2.4 Notice

2.4.2.4.1 Capricorn CA shall give any notice, demand, or request, to an Individual / Subscriber / Organisation, by electronic mail or by a

duly signed letter. Communication, by letter, shall be delivered by a date and time recorded method of delivery (courier / registered mail etc.). Notices to Capricorn CA are effective when received. Notices by Capricorn CA are effective when received by the Individual / Subscriber / Organisation.

2.4.2.4.2 An Individual / Subscriber / Organisation can send communications to Capricorn CA by electronic mail or by a duly signed letter at the address given below :

Capricorn Identity Services Pvt. Ltd.
709, Roots Tower, Plot -7, Laxmi Nagar District Centre,
Delhi 110 092.
Telephone 011 – 224 22444 or Toll Free : 1800–53 –22444
eMail : Support@Certificate.Digital

2.4.3 Dispute Resolution Procedures

2.4.3.1 Any dispute arising between Capricorn CA and the Subscriber or Relying Parties shall be resolved by Capricorn CA within 30 days.

2.4.3.2 If the dispute remains unresolved after 30 days, the dispute between Capricorn CA, the Subscriber or the Relying Parties shall be referred to the CCA as per the Act. The CCA is the competent authority, under the IT Act, clause 18(I), to resolve any dispute between the Certifying Authority and Subscribers.

2.4.3.3 The Cyber Appellate Tribunal, under the IT Act, 2000 is the competent court to appeal against any order passed by the CCA. All arbitration proceedings shall be in the English language and

judgment upon the award so rendered may be entered in the courts of New Delhi only.

2.5 Fees

Capricorn CA shall charge fees for the services listed hereunder

- issuance and renewal of DSC

The fee structure for different services shall be listed on the Company's website www.Certificate.Digital. The fees are subject to change and any such changes shall become effective immediately after posting at the Capricorn CA website. Please visit the Company's website www.Certificate.Digital to view the fee structure for various class of DSC and other services.

Note : Capricorn CA, at its sole discretion, may waive charges for some or all of the services listed above.

2.5.1 Fees for other services such as policy information

2.5.1.1 The CPS is available for download from the Company's website www.certficate.digitalfree of cost. However, a printed copy of the CPS shall be charged at Rs. 2,500.00

2.5.2 Certificate access fee

2.5.2.1 Capricorn CA shall not charge any fee for Certificate access.

2.5.3 Revocation or status information access fee

2.5.3.1 Capricorn CA shall not charge any fee for Revocation or Status Information access.

2.5.4 Fees for other services such as policy information

2.5.4.1 Capricorn CA shall put up on their website, www.certificate.digital, the structure of fees for other services.

2.5.5 Refund policy

2.5.5.1 Capricorn CA does not provide any refund for any services provided by it.

2.5.5.2 Since Capricorn CA reserves the right to refuse any application for issuance or renewal of DSC, Capricorn CA shall refund the fees paid by the applicant for the services denied and for which the fees have been paid.

2.6 Publication and Repositories

2.6.1 Certifying Authority's practice information

2.6.1.1 Capricorn CA shall publish the most recent CPS on the Company's website at www.Certificate.Digital.

2.6.1.2 Capricorn CA shall publish the fee structure of different class of DSC on the Company's website at www.Certificate.Digital.

2.6.1.3 Capricorn CA shall publish the DSC of Capricorn CA corresponding to its private key

2.6.1.4 Upon generation of a DSC by the Subscriber using the private key, Capricorn CA shall publish a copy of the DSC in one or more other repositories. The DSC and the status of the DSC can be verified through a link provided on the Company's website at www.Certificate.Digital.

2.6.1.5 Capricorn CA shall update its repository immediately on approval of a revocation request and publish the updated CRL immediately. Capricorn CA shall publish the CRL after every 7 days. The CRL can be accessed through a link provided on the Company's website at www.Certificate.Digital.

The Online Certificate Status Protocol (OCSP) shall be made available for obtaining the revocation status of a DSC.

2.6.2 Frequency of publication

2.6.2.1 The CPS shall be published if and when a change occurs in any of the practices of Capricorn CA

2.6.2.2 The fee structure shall be published if and when the fee structure for any of the services provided by Capricorn CA has been changed.

2.6.2.3 Capricorn CA shall publish an updated CRL on revocation of a DSC or after every 7 days.

2.6.3 Access control on published information

2.6.3.1 Capricorn CA shall publish information on its website www.certificate.digital, which can be accessed by the public at large, the subscribers, the relying parties and officials of Capricorn CA.

2.6.3.2 Capricorn CA shall publish information on its website www.certificate.digital, which can be accessed only by the personnel of the Company. This information shall be maintained in a read-only format. Owners of information can request changes to the published information only through the Change Management process.

2.6.4 Certifying Authority's repository

2.6.4.1 Capricorn CA shall maintain several repositories, some of which, shall be accessible to authorized personnel only.

2.6.4.2 Capricorn CA shall maintain DSC and CRL information in its repositories which shall be accessible to Subscribers and Relying Parties.

2.7 Compliance Audit

2.7.1 Frequency of compliance audits

2.7.1.1 Capricorn CA shall carry out an annual compliance audit as per the Act, Rules and Regulations.

2.7.1.2 Capricorn CA shall carry out internal audit(s) as per the requirements of the CCA.

2.7.2 Identity/qualifications of the auditor

2.7.2.1 Capricorn CA shall carry out the annual audit by an Auditor empanelled by the CCA.

2.7.2.2 Capricorn CA shall carry out internal audit(s) by an Auditor.

2.7.3 Auditor's relationship to the entity being audited

2.7.3.1 Capricorn CA shall appoint auditors who are independent entities and do not have any relationships or transactions, other than as auditors, with the Company or with the Vendor(s) whose products or services are provided to the Company and are within the scope of the audit.

2.7.4 List of topics covered under the compliance audit

2.7.4.1 Capricorn CA shall get its operations audited annually by an auditor and such audit shall include *inter alia,*-

- security policy and planning;
- physical security;
- technology evaluation;
- Certifying Authority's services administration;
- relevant Certification Practice Statement;
- compliance to relevant Certification Practice Statement;
- contracts / agreements;

- regulations prescribed by the Controller of Certifying Authorities ;
- Information Technology (Certifying Authority) Rules, 2000.

2.7.4.2 Capricorn CA shall conduct,-

- half yearly audit of the Security Policy, physical security and planning of its operation by an Internal Auditor;
- Annual audit by an External Auditor.

2.7.5 Actions taken for deficiency found during compliance audit

2.7.5.1 On receipt of the audit findings, Capricorn CA shall take preventive and corrective actions to correct the deficiency within reasonable and agreed upon timeframes.

2.7.6 Compliance audit results

2.7.6.1 Capricorn CA's compliance audit results shall not be made public unless required by law. Within Capricorn CA, the audit report will be made available on a need-to-know and need-to-do basis.

2.7.6.2 The results of the audit along with the remedial actions taken / future action plan for the observed non-conformities shall be communicated by Capricorn CA to the CCA within 4 weeks of the completion of the audit.

2.8 Policy of Confidentiality

2.8.1 Types of confidential information

2.8.1.1 The Subscriber's private keys should be kept confidential and secure by the Subscriber.

2.8.1.2 Capricorn CA shall maintain confidentiality of information provided by the Subscriber in the application form for issuance, revocation or suspension of DSC, unless required by law, to be disclosed.

2.8.1.3 Subscriber access, data, transactional information and data in transit, in custody / control of Capricorn CA, generated during the use of DSC shall be confidential, unless required by law, to be disclosed.

2.8.1.4 Capricorn CA's operational practices, roles and responsibilities of its personnel, type of Information Technology hardware and software used to support Capricorn CA's services shall be deemed confidential.

2.8.1.5 Capricorn CA's security operations, contingency plans and business continuity plans shall be deemed confidential.

2.8.1.6 Sensitive information like Information Systems Audit Reports, Remedial Action Plans, various types of Audit Trails shall be kept confidential, unless required by law, to be disclosed.

2.8.1.7 Capricorn CA's agreements with various service providers, contracts and correspondence with the RAs, agents and personnel shall be kept confidential, unless required by law, to be disclosed.

2.8.2 Types of information that are not confidential

2.8.2.1 Capricorn CA shall not consider the following information confidential :

- Subscriber's information in the DSC
- CRL
- The contents of this CPS
- Information of Capricorn CA on the website www.Certificate.Digital

2.8.3 Information of Revocation or Suspension of Certificates

2.8.3.1 DSCs shall be revoked or suspended only on the explicit request of the Subscriber. Reasons for the request shall be kept confidential and shall not be disclosed unless required, by law, to be disclosed.

2.8.3.2 Revoked or suspended DSC shall be updated in the CRL for the benefit of the Relying Parties.

2.8.4 Policy on release of information to law enforcement officials

2.8.4.1 Capricorn CA shall release confidential information in its custody after obtaining a notice, as per the laws of the Republic of India, from a competent authority, recognized by the laws of the

Republic of India, to receive the confidential information. Disclosures, in such cases, shall not be considered a breach of the confidentiality obligations.

2.8.5 Information that can be revealed as part of civil discovery

2.8.5.1 Capricorn CA, if required, shall release confidential information in its custody for any judicial, arbitration, litigation or administrative proceedings. Any such release shall not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality as listed in this CPS.

2.8.6 Disclose upon Subscriber's Request

2.8.6.1 Capricorn CA shall not release any confidential information of a Subscriber unless an authenticated request from the Subscriber is received providing a specific reason for such request.

2.8.6.2 The Subscriber shall indemnify Capricorn CA for any and all liabilities arising out of the disclosure of the Subscriber's confidential information at the Subscriber's request.

2.8.7 Other circumstances to disclose information

2.8.7.1 Capricorn CA shall not disclose any confidential information except in circumstances provided in clauses 2.8.1 – 2.8.6 above.

2.9 Intellectual Property Rights

2.9.1 Capricorn CA

2.9.1.1 Capricorn CA's Intellectual Property (IP) includes but is not limited to the Certificate, software, firmware, hardware, CPS, Copyrights, Trademarks, Capricorn CA documentation, proprietary processes and methods developed and deployed, whether disclosed or undisclosed.

2.9.1.2 Capricorn CA reserves sole and absolute rights over its IP.

2.9.1.3 Capricorn CA shall be entitled to continue using it’s IP in whatever form, manner or model it so selects.

2.9.2 Ownership Rights of Certificate

2.9.2.1 Capricorn – Certifying Authority

2.9.2.1.1 Capricorn CA's Intellectual Property (IP) includes but is not limited to the Certificate, software, firmware, hardware, CPS, Copyrights, Trademarks, Capricorn CA documentation, proprietary processes and methods developed and deployed, whether disclosed or undisclosed.

2.9.2.1.2 Capricorn CA reserves sole and absolute rights over its IP.

2.9.2.1.3 Capricorn CA shall be entitled to continue using it’s IP in whatever form, manner or model it so selects.

2.9.2.1.4 Capricorn CA retains all Intellectual Property Rights in and to the Certificates and revocation information that it issues.

2.9.2.1.5 All parties acknowledge that any and all of the intellectual property rights used or embodied in or in connection with any and all Certificate issued and all software supplied by the Capricorn CA pursuant to this CPS, including all documentation and manuals relating hereto, are and shall remain the property of Capricorn CA, and that all the parties shall not during the life of the Certificate or at any time after the revocation or expiry the Certificate, in any way question or dispute the ownership or any other such rights of Capricorn CA.

2.9.2.1.6 Capricorn CA expressly prohibits any user, certificate applicant, subscriber, relying party, or any other party to monitor, interfere, with or reverse engineer the technical implementation of Capricorn CA DSC service except as explicitly permitted by this CPS. Any act in contravention of above will be subject to punitive action under the Indian Laws.

2.9.2.2 **Subscriber**

2.9.2.2.1 Capricorn CA, the RA and personnel shall comply with the Act regarding all information of an Applicant. The Subscriber shall have all rights on the information provided by the Subscriber.

2.9.3 Ownership Rights of this CPS

2.9.3.1 Capricorn CA shall be the absolute Owner and custodian of this CPS.

2.9.3.2 Capricorn CA grants permission to reproduce this CPS provided

- The copyrights notice being retained in all the copies of the CPS.
- The CPS is reproduced fully and accurately.

2.9.4 Ownership Rights of Names

2.9.4.1 An Applicant / Subscriber retains all rights (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

2.9.5 Ownership Rights of Keys

2.9.5.1 Capricorn – Certifying Authority

2.9.5.1.1 Capricorn CA shall retain sole and exclusive ownership of all right, title and/or interest in the key pairs generated by Capricorn CA to issue DSCs.

2.9.5.2 Subscriber

2.9.4.2.1 The Subscriber shall retain sole and exclusive ownership of all right, title and/or interest in the key pairs generated by the Subscriber.

2.9.6 Copyrights and Trademarks

2.9.6.1 Capricorn CA considers its trademark all developed software, all assembled hardware, this CPS and all documentation relating the

DSC services and operations as the Intellectual Property (IP) of Capricorn CA.

3. Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

3.1.1.1 Capricorn CA shall issue DSCs in compliance with the X.500 naming convention and the Inter-Operability Guidelines (IOG) issued by the CCA.

3.1.1.2 Capricorn CA shall use Distinguished Name (DN) to provide identities to the Subscriber.

3.1.1.3 The DSC shall contain the fields as per the IOG issued by Office of the CCA.

3.1.2 Meaningful Names

3.1.2.1 It will be mandatory to have meaningful name of an Individual or Organisation. This will enable easy verification and authentication of the Subscriber against the documents provided.

3.1.2.2 The DN forms the basis for the uniqueness of each assigned name, but the same Applicant/Subscriber can have multiple Digital

Signature Certificates with the same DNs for different Digital Signature Certificate purposes as specified in the CPS.

The distinguished names should be able to uniquely identify the Subscriber in the public Repository in which it is published.

3.1.3 Rules for Interpreting Various Name Forms

3.1.3.1 The rules for interpretation of Names is as given in 3.1.1.

3.1.4 Resolution of Name Claim Disputes

3.1.4.1 The disputing party / parties may approach Capricorn CA for any dispute in the assigned DN. Capricorn CA shall permit the party / parties to present their case for any objections to the DN assigned by Capricorn CA.

3.1.4.2 Capricorn CA shall submit its decision to the disputing party / parties. The decision of Capricorn CA shall be considered final and binding on the party / parties.

3.1.5 Recognition, Authentication, and Role of Trademarks

3.1.5.1 Trademarks, if provided by the Subscriber with legal proof of ownership, shall be reserved by Capricorn CA to the rightful Owner.

3.1.6 Possession of Private Key

3.1.6.1 Capricorn CA shall provide to the Applicant a setup method during the Registration process. On authentication of the Applicant, unique codes shall be generated by Capricorn CA's software and provided to the Applicant securely.

3.1.7 Authentication Requirements for Organizational Identity

3.1.7.1 Only an Individual shall be provided with a DSC. An Individual / Subscriber, on behalf of an Organisation, shall provide along with the Application Form the required documentation for each Class of Certificates. The documentation required shall be displayed when the Subscriber completes the Application Form on-line.

3.1.7.2 The required documentation may change from time-to-time as per the Rules laid down by the CCA. These changes shall be reflected in the on-line Application Form.

3.1.7.3 The identification of the Applicant for issuance for Digital Signature Certificate will be as per the provisions of Identity Verification Guidelines issued by the office of CCA.

3.1.7.4 The RA shall verify the Application Form and the attached documentation and on satisfactory observation authorize generation of the DSC for the Subscriber.

3.1.8 Authentication Requirements for an Individual

3.1.8.1 The Subscriber shall provide along with the Application Form, the documentation as required by each Class of Certificates.

3.1.8.2 The required documentation may change from time-to-time as per the Rules laid down by the CCA.

3.1.8.3 The identification of the Applicant for issuance for Digital Signature Certificate will be as per the provisions of Identity Verification Guidelines issued by the office of CCA.

3.1.8.4 The RA shall verify the Application Form and the attached documentation and on satisfactory observation the RA shall authorize generation of the DSC by the Subscriber.

3.2 Routine Re-key

3.2.1 Capricorn CA shall change its key pairs on expiry.

3.2.2 Capricorn CA shall not allow re-key of expired certificates. A Subscriber needs to apply for a new DSC and generate a new private – public key pair as per the requirements detailed in this CPS. All charges / fees for the new DSC shall be as listed on the website www.Certificate.Digital

3.3 Re-key After Revocation

3.3.1 Capricorn CA shall not allow re-key of revoked certificates. A Subscriber needs to apply for a new DSC and generate a new private – public key pair as per the requirements detailed in this CPS. All charges / fees for the new DSC shall be as listed on the website www.Certificate.Digital

3.4 Revocation Request

3.4.1 DSCs shall be revoked only on the explicit request of the Subscriber. The request shall be accompanied by adequate documentation to authenticate the requestor as the Subscriber.

3.4.2 Revoked or suspended DSC shall be updated in the CRL for the benefit of the Relying Parties.

4. Operational Requirements

4.1 Certificate Application

4.1.1 There are two ways in which an Applicant can make an application for a DSC viz. Manual by the Applicant and Online Application by the Applicant.

4.1.2 In either case, the Application Form is printed, signed in blue ink by the Applicant and submitted with all relevant documents. The RA verifies the Application Form and all relevant documents with the originals and authorizes the form.

4.1.3 In case of Class 3 DSC a video recording of the Applicant for confirmation is also taken.

4.2 Certificate Issuance

4.2.1 After the RA verifies and authorizes the Application Form, the attached documentation and the video recording, the application software sends an e-mail at the registered e-mail address to the Subscriber with a link to generate the DSC. An sms containing the "Auth Key" is sent on the registered mobile number of the Applicant.

4.2.2 The Subscriber shall click on the link which will direct to a web-page. The Subscriber shall enter the AUTH key and also “Agree” to the Terms and Conditions specified on the web-page.

4.2.4 On agreeing to the terms and conditions, the DSC shall be downloaded in the crypto-token in case of Class II and Class III DSCs.

4.3 Certificate Acceptance / Rejection

4.3.1 The Digital Signature Certificate of the Subscriber shall be considered to be accepted by the Subscriber when the corresponding Subscriber downloads the Certificate.

4.3.2 Capricorn CA reserves the right to reject an Application where details provided by the Application fails the validation check or is incomplete.

4.4 Certificate Suspension and Revocation

4.4.1 Capricorn CA shall follow a process, as detailed hereunder, for the revocation of a DSC. Suspension service of a DSC will not be offered by Capricorn CA.

4.4.2 On revocation of a Certificate, Capricorn repository will be automatically updated and the CRL shall be immediately published.

4.4.3 Capricorn CA shall revoke a DSC in the following circumstances:

4.4.3.1 Capricorn CA will revoke a Certificate Based on the request of the Subscriber / Duly Authorised Representative of the Subscriber:

4.4.3.1.1 The Subscriber (or the representative) shall submit the Digital Signature Revocation Form to the RA.

4.4.3.1.2 The RA shall verify the details in the Form from the details provided during the application of the DSC. After confirmation, the RA shall authorise the revocation of the Form.

4.4.3.1.3 The Subscriber is notified by e-mail and SMS about the revocation on the e-mail Id and the Phone Number provided during the application for a DSC.

4.4.3.2 In addition, Capricorn CA shall also revoke a DSC in the following circumstances (including but not limited to)

- Capricorn CA's private key or systems are compromised;
- The Subscriber's private key corresponding to the public key in the DSC has been compromised;
- A material fact represented in the DSC has changed or is false or has been concealed;
- Upon the death or insolvency of the Subscriber;
- Upon the dissolution of the Firm / Company where the Subscriber is a Firm / Company;
- Any other circumstances as may be determined by the Capricorn CA in accordance with the rules or regulations or the governing law;

4.4.3.2.1 In such cases, Capricorn CA shall inform the RA to revoke the DSC.

4.4.3.2.2 The Subscriber is notified by e-mail and SMS about the revocation on the e-mail Id and the Phone Number provided during the application for a DSC.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

Capricorn CA shall maintain records of all events relating to the security of its systems. The records shall be maintained in audit log file and shall include such events as:

- System start-up and shutdown
- Certifying Authority's application start-up and shutdown
- Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;
- Changes to keys of the Certifying Authority or any of his other details
- Changes to Digital Signature Certificate creation policies, e.g. validity period;
- Login and logoff attempts;
- Unauthorised attempts at network access to the Certifying Authority's system;

- Unauthorised attempts to access system files
- Generation of own keys
- Creation and revocation of Digital Signature Certificates
- Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys;
- Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

4.5.2 **Frequency with which Audit Logs are Processed or Audited**

Audit logs shall be reviewed on the basis of the classification of the logs as defined hereunder:

- Highly critical logs shall be reviewed daily;
- Moderately critical logs shall be reviewed weekly; and
- Low critical logs shall be reviewed monthly.

4.5.3 **Period for which audit logs are kept**

Audit logs shall be maintained on site for a period of 7 years.

4.5.4 **Protection of audit logs**

4.5.4.1 Only authorized personnel, with trusted roles, shall be allowed access to the audit logs.

4.5.4.2 All audit logs shall be protected with read-only permissions to prevent any modification to the logs.

4.5.5 **Audit log back up procedures**

4.5.5.1 Electronic audit logs shall be backed-up daily using automated tools.

4.5.5.2 Physical documents shall be copied and retained as per the backup procedure.

4.5.6 **Whether the audit log accumulation system is internal or external to the entity**

4.5.6.1 Audit log accumulation of Capricorn CA operations shall be internal to Capricorn CA.

4.5.7 **Is subject who caused an audit event to occur is notified of the audit action**

4.5.7.1 Subject who has caused the event shall be notified if any irregularity, unauthorized activity or any risk is observed in the action performed.

In such cases, an enquiry shall be initiated and any action taken shall be recorded and shall be as per the provisions of the Act and the Rules and Regulations thereof.

4.5.8 **Vulnerability assessments**

4.5.8.1 Vulnerability Assessments of all critical systems shall be carried out regularly and as per the provisions of the Act and the Rules and Regulations thereof.

4.6 Records Archival

4.6.1 **Types of Events Recorded**

4.6.1.1 Capricorn CA shall archive all events as specified in 4.5.1.

4.6.2 **Retention Period of Archives**

All archived logs shall be retained off-site for a period of 7 years.

4.6.3 **Protection of Archive**

4.6.3.1 Only authorized personnel, with trusted roles, and authorization from the level of Operations Manager or senior shall be allowed access to the archived logs.

4.6.3.2 All audit logs shall be protected with read-only permissions to prevent any modification to the logs.

4.6.3.3 The audit logs will only be accessible in a read only mode.

4.6.4 **Archive / Back-up Procedures**

4.6.4.1 Electronic audit logs shall be archived using automated tools.

4.6.5 **Requirements for time-stamping of records**

4.6.5.1 Capricorn CA has defined the procedure for time-stamping archived records.

4.6.6 **Whether archival system is internal or external to the entity**

4.6.6.1 The archival system of Capricorn CA operations shall be external to Capricorn CA.

4.6.6.2 The external entity shall execute a Service Level Agreement (SLA) and a Non Disclosure Agreement (NDA) with Capricorn CA.

These Agreements shall bind the external entity to the Information Security Policy of Capricorn CA, to the specific requirements of this CPS, to the Act and the Rules and Regulations thereof.

4.6.6.3 Capricorn CA shall verify all on-site and off-site backup periodically for integrity, readability and restorability.

4.7 Key Changeover

4.7.1 Capricorn CA shall change the keys as per the Act and the Rules and Regulations thereof. The keys shall be changed as per the process described in this CPS.

The validity of the CA key pairs shall be 10 years.

4.7.2 Capricorn CA shall inform all active Subscribers and Relying Parties, in advance, of the pending key change. However, changes in the key pair shall not affect the key pairs of the existing Subscribers, unless in the case of a compromise of the existing key pairs of the Subscriber.

4.8 Compromise and Disaster Recovery

4.8.1 Compromise

4.8.1.1 In case of a compromise of the Capricorn CA keys, all DSCs issued shall be revoked and the CRL shall be immediately updated. All Subscribers shall be informed by E-Mail and through the portal of Capricorn CA viz. www.capricorn.com.

On receiving the DSC for the new key pairs from the CCA, the Subscribers shall be provided with new DSCs. Such Subscribers

shall be informed of the activation by E-Mail and through the portal of Capricorn CA viz. www.certificate.digital. Such Subscribers shall be asked to download the new key pairs on their tokens.

4.8.1.2 If a Subscriber's DSC is compromised, the Subscriber shall make an explicit request for the revocation of the DSC. The request shall be accompanied by adequate documentation to authenticate the requestor as the Subscriber.

Capricorn CA shall revoke the Subscriber DSC and notify the Subscriber of the action taken.

4.8.2 Disaster Recovery

4.8.2.1 Capricorn CA has documented and implemented a Disaster Recovery Plan. Details of this plan are confidential and shall not be published in this CPS.

4.9 Certifying Authority Termination/Suspension

4.9.1 Termination of Services

4.9.1.1 In case of cessation of CA activities, Capricorn CA shall inform the CCA, with a Notice of at least 3 months in advance by digitally signed e-mail and registered post.

4.9.1.2 In case of cessation of CA activities, Capricorn CA shall advertise in Newspapers and would follow the procedures as per the rules under IT Act 2000.

5. Physical, Procedural, and Personnel Security Controls

5.1 Physical, Procedural, and Personnel Controls

5.1.1 Site Location and Construction

5.1.1.1 The site location of Capricorn CA Office and the Data Centre has been selected and modified to adhere to the Rules of the IT Act, 2000 with 2008(amendment).

5.1.2 Physical Access

5.1.2.1 Capricorn CA operational premises shall always be protected from unauthorized access

5.1.2.2 Capricorn CA shall log all entries made into the critical areas. These entries shall be manned by 24 X 7 X 365 by guards who shall allow entry to authorized personnel only.

Personnel entering the Data Centre shall be frisked to ensure non-secure items like mobile phones, food etc. are not taken into the critical areas.

5.1.2.3 Capricorn CA has implemented multi-tiered (3 levels) entry to the Data Centre. Two-factor access control method has been implemented to log entry made into the areas designated as Data Centre.

5.1.2.4 Authorised persons shall accompany any visitor to the Data Centre.

5.1.3 Power and Air Conditioning

5.1.3.1 Capricorn CA has ensured availability of power on a 24x7x365 days basis. Capricorn CA has implemented dual true online UPS for clear power. Also, dual power generators in automatic failover mode with adequate fuel to power the infrastructure for 24 hours has been implemented.

5.1.3.2 Precision air-conditioners with Humidity and Temperature control has been implemented with fully redundant configuration.

5.1.4 Water Exposures

5.1.4.1 The Data Centre facility is located in a non-flooding area. The facility is housed at least twenty feet above ground level. The building, housing the Data Centre, has implemented "Fire Walls" which are additional walls at least two feet beyond the internal walls of the Data Center. Such dual walls restrict the seepage of water from the physical walls.

5.1.4.2 The false flooring of the Data Center has been populated with water leak detection system.

5.1.5 Fire Prevention and Protection

5.1.5.1 Capricorn CA has installed adequate fire detection, prevention and protection systems. A Certificate has been obtained from the local Fire Brigade Department certifying the adequacy of these implemented systems.

5.1.6 **Media Storage**

5.1.6.1 Capricorn CA has installed a strong fire-proof box within the Data Centre for media storage. Access to the media shall be allowed to authorised personnel only.

5.1.7 **Waste Disposal**

5.1.7.1 Unused and unwanted documents shall be destroyed within the Data Centre. Unauthorised documents shall not be allowed to be taken in or taken out from the Data Centre.

5.1.7.2 Other materials shall be scrutinized before being released for disposal.

5.1.8 **Off-site backup**

5.1.8.1 Capricorn CA has made provision to maintain one copy of the backup at an off-site location.

5.1.8.2 The backup copy shall be secured in a tamper-proof container and transported by an authorized person.

5.2 Procedural Controls

5.2.1 **Trusted Roles**

5.2.1.1 Capricorn CA has assigned and shall assign “trusted” roles to personnel who carry out critical duties to ensure an effective and efficient CA operations. Personnel with a “trusted” role shall carry out a defined set of functions within the CA operations.

5.2.1.2 Capricorn CA has assigned “trusted” roles for the following :

- Management of critical IT infrastructure
- Granting Physical and Logical Access

5.2.2 **Number of persons required**

5.2.2.1 Capricorn CA has employed “segregation of duties” principle while assigning “trusted” roles.

5.2.3 **Identification and Authentication for each Role**

5.2.3.1 Each person with a “trusted” role shall be authenticated before being allowed to carry out any function assigned to the role.

5.2.3.2 A ”trusted” role shall be able to carry out the functions of the role only through a unique non-shared identification created for the role and a password created by the person assigned the “trusted” role.

5.3 Personnel Controls

5.3.1 **Background, Qualifications, Experience and Clearance Requirements**

5.3.1.1 Capricorn CA has employed and shall continue to employ personnel on the basis of their competence and experience in discharging their duties responsibly for the job they have been selected.

5.3.1.2 Capricorn CA has followed and shall continue to follow the following procedures while selecting personnel :

- Personnel shall be selected after a thorough examination of their qualifications and verification of their experience. Personnel shall be mapped for the role and responsibility in Capricorn CA to their qualification and experience.
- Carry out an experience check through verification of prior employment.
- Enforce a Non-Disclosure Agreement with each personnel employed by the Company.
- Obtain an Agreement to abide by the Information Security Policy of the Company.

5.3.2 **Background Check Procedures**

5.3.2.1 Capricorn CA has carried out and shall continue to carry out background checks as given hereunder :

- Carry out a verification of the qualifications.
- Carry out an experience check through verification of prior employment.
- Carry out a Police Verification.

5.3.2.4 Any discrepancy observed during the background checks shall result in immediate dismissal of the personnel.

5.3.3 **Training Requirements**

5.3.3.1 Capricorn CA has provided and shall continue to provide all personnel with an induction training which shall consist of :

- Relevant provisions of Information Technology Act, 2000, Rules and Regulations, Information Technology Act, 2008 (Amendment)
- Information Security Policy of the Company.
- Relevant training on the operations for which the personnel was selected.
- Physical Security procedures and drills.
- Business Continuity and Disaster Recovery
- On satisfactory performance, training shall be provided in other areas to ensure skills enhancement and prevent attrition of skilled personnel.

5.3.4 **Retraining Frequency and Requirements**

5.3.4.1 Capricorn CA shall monitor the performance of its personnel. Retraining shall be mandated in areas where weakness is observed in the discharge of their duties.

5.3.4.2 Retraining shall be offered to enhance operational performance.

5.3.4.3 Retraining shall be offered to improve the efficiency of the Business Continuity Plan and the Disaster Recovery Plan.

5.3.4.3 Retraining in the areas of physical protection has been provided and shall continue to be provided to improve the evacuation timings of the fire drills.

5.3.5 **Job Rotation**

5.3.5.1 Job rotation between trusted roles shall be carried out periodically.

5.3.5.2 Job rotation between non-trusted roles shall be carried out to ensure skills enhancement and prevent attrition of skilled personnel.

5.3.6 **Sanctions for Unauthorized Actions**

5.3.6.1 Capricorn CA shall take disciplinary action against personnel for any violation of the Information Security Policy of the Company.

5.3.6.2 For any unauthorized action in the role and responsibility assigned to the personnel shall result in immediate suspension. A Disciplinary Action Committee shall decide on the quantum of punishment which shall be based on the severity and criticality of the unauthorized action.

5.3.6.3 For any unauthorized action outside the role and responsibility assigned to the personnel shall result in immediate suspension. A Disciplinary Action Committee shall decide on the quantum of punishment which shall be based on the severity and criticality of the unauthorized action.

5.3.7 **Documentation Supplied to Personnel**

5.3.7.1 Capricorn CA has made available and shall make available relevant Information Security Policy of the Company on the basis of the role and responsibility of the personnel.

5.3.7.2 All Capricorn CA personnel have been provided and shall be provided a copy of this CPS.

5.3.7.3 Capricorn CA has provided and shall provide technical documentation on the basis of the role and responsibility assigned to the personnel.

5.3.7.4 Contracting Personnel

Contracting personnel shall always be accompanied by a personnel with a trusted role. All actions performed by the contracting personnel shall be supervised by Capricorn CA personnel who has a trusted role.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 Capricorn CA key pairs are generated in a controlled environment, under dual observation, by using certified hardware and software. The key pairs are generated on a secure medium.

6.1.1.2 Subscribers shall generate their own key pairs through an application provided by Capricorn CA. The key pairs shall be 2048 bits long and shall be generated on a secure medium prescribed by the CCA.

6.1.2 Public Key Delivery to Certificate Issuer

6.1.2.1 The Capricorn CA Public key shall be delivered to the National Root CA as a PKCS #10 request.

6.1.2.2 For Subscribers, the Capricorn CA supports the requirements, where the public key is delivered to Capricorn CA using a secure online protocol.

6.1.3 Capricorn CA's Public Key Delivery to Users

6.1.3.1 Capricorn CA's public key certificate is available at the Capricorn CA's website and can be downloaded from the Repository.

6.1.4 **Key Sizes**

6.1.4.1 The asymmetric key pair will be 2048 bits for Capricorn CA and Subscribers.

6.1.5 **Public Key Parameters**

6.1.5.1 Capricorn CA application is configured to set parameters for CA Public Key and Subscriber Public Key generation.

6.1.6 **Public Key Parameters**

6.1.6.1 Capricorn CA Public Key & Subscriber Public Key are generated by Capricorn CA's application which shall be configured to set parameters.

6.1.7 **Hardware / Software Key Generation**

6.1.7.1 Capricorn CA's key pair is generated in a trustworthy hardware cryptographic module as described in section 6.8.

6.1.7.2 Subscriber's key pairs is generated in a trustworthy software module / crypto device as per Certificate Policy requirements for the particular class of DSC.

6.1.8 **Key Usage Purposes (as per X.509 vv3 key usage field)**

6.1.8.1 Key usage purposes are incorporated in the Capricorn CA CPS as detailed in chapter 7 – Certificate and CRL Profiles.

6.1.9 **Time Source**

6.1.9.1 The real time clock of the computer systems is set accurately to ensure the accuracy of audit logs. The real time clock of all the critical servers and communications devices is set to Indian

Standard Time (IST) as determined by National Physical Laboratory (NPL).

There is a procedure to periodically check and correct drift in the real time clock.

6.2 Private Key Protection

6.2.1 Key Standards

6.2.1.1 The cryptographic module used by the Capricorn CA system to generate CA keys is designed to comply with FIPS 140-1/2 level 3. Also Refer to Section 6.8.

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

6.2.2.1 Capricorn CA private key which is accessed through the hardware security module (HSM) requires the presence of two (2) out of three (3) persons to complete the generation successfully No single Capricorn CA trusted personnel is allowed to generate the CA private key. For accessing the HSM, minimum 2 out of 3 persons are required.

6.2.3. Private Key Escrow

6.2.3.1 Capricorn CA does not escrow CA or Subscriber private keys with any third party. Escrow Agreement for the Private Key has not been implemented.

6.2.4 Backup of Private Key

6.2.4.1 Capricorn CA's Private key is backed up in an encrypted format and stored at multiple locations. The key is backed up as per the Security Policy of the Company.

6.2.5 Archival of Private Key

6.2.5.1 Capricorn CA's Private Key shall be archived using hardware cryptographic modules that meet the requirements of the Act and Rules and Regulations thereof.

6.2.6 Private Key Entry into Cryptographic Module

6.2.6.1 Capricorn CA's Private Key is generated by the application, stored in an encrypted format and is decrypted only during its usage. During backup to another cryptographic mode, the Private Key is transported in an encrypted format.

6.2.7 Private Key Activation

6.2.7.1 CA private keys are activated by a threshold number of Shareholders supplying their activation data. The Private Key is activated for an indefinite period and the module remains online in the Data Centre.

6.2.7.2 For a Subscriber, Private Key is activated by the client application.

6.2.8 Deactivation of Private Key

6.2.8.1 Capricorn CA Private Key shall remain active as long as the module remains online in the Data Centre.

6.2.8.2 The Subscriber's Private Key may be deactivated after each operation, upon logging off their system, or upon removal of cryptographic media.

6.2.9 **Destruction of the Private Key**

6.2.9.1 Capricorn CA's one or more copies of the CA private key are archived in accordance with this CPS. Remaining copies of the Private Key shall be securely destroyed. In addition, archived private keys shall be securely destroyed at the conclusion of their archive periods. Key destruction activities shall require the participation of multiple trusted individuals.

6.3 Other Aspects of Key Pair Management

6.3.1 **Archival of Public Key**

6.3.1.1 Capricorn CA and Subscriber Certificates are backed up and archived as part of routine backup procedures.

6.3.2 **Active Lifetime of Private and Public Keys**

6.3.2.1 Private and Public key maximum lifetime for each entity is as given hereunder:

- For CA 10 years
- For Subscriber upto 3 years

6.4 Activation Data

All key management activities like Certificate generation, suspension, activation or revocation and CRL generation shall use

the private key stored in FIPS 140-1 Level 3compliant storage, which is activated using tokens

6.4.1 Activation Data Generation and Installation

Activation data Generation and Initialization is carried out using HSM / Smartcard / Token in conjunction with appropriate Access control mechanisms (PIN) by authorized personnel only. Access control mechanisms (PIN) are utilized for initialization and generation of HSM / Smartcard / Token.

6.4.2 Activation Data Protection

Activation data protection is achieved by utilization of regulated and secure systems, housed in a secure location under climate controlled environment. Data used to unlock/utilize private keys will be protected from disclosure using Password and PIN and access provided to only authorized personnel.

6.4.3 Other Aspects of Activation Data

A token re-key or a maintenance outage will change the activation data or when the devices are disposed of or are dispatched for maintenance/repair.

6.5 Computer Security Controls

6.5.1 Capricorn CA's DSC services and related hardware and software are housed in a secure environment as per the specifications of the Act, Rules and Regulations thereof.

6.5.2 Only authorized personnel with trusted roles shall be allowed access through an authentication process. All actions by these personnel shall be logged.

6.5.3 Capricorn CA's DSC services and related hardware and software is monitored to ensure confidentiality, integrity and availability of the services at all times.

6.5.4 Remote access to the DSC services, from outside the Data Centre, is not allowed.

6.5.5 Remote access for the management of operations is allowed only to authorized personnel. All actions by these personnel are logged.

6.6.6 Capricorn CA's DSC generation system provides reasonable assurance that the system software and the data files used to issue, suspend, activate and revoke DSCs is secured from unauthorized access.

6.6.7 Capricorn CA's DSC services and related hardware and software is and shall be as per the specifications laid down by the Act and the Rules and Regulations thereof.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

6.6.1.1 Capricorn CA has implemented industry-best practices for the development of systems. Security controls is a part of the system development process.

6.6.1.2 The system development process adheres to the relevant clauses of the Act and the Rules and Regulations thereof.

6.6.2 **Security Management Controls**

6.6.2.1 Capricorn CA has deployed appropriate tools for security management. These tools shall be used to enhance the effectiveness and efficiency of operational security.

6.6.3 **Life-Cycle Security Ratings**

6.6.3.1 All life cycle security controls have been implemented as per the Act and the Rules and Regulations thereof

6.7 Network Security Controls

6.7.1 Capricorn CA has implemented a robust network infrastructure including Firewalls, Intrusion Detection System, Network Security &Performance Monitoring System to ensure a secure environment for the DSC services.

6.8 Cryptographic Module Engineering Controls

6.8.1 Capricorn CA has implemented and utilizes Hardware Security Module in compliance with IT Act 2000 and notification issued under Act. 3.

7. Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Number

7.1.1.1 The Capricorn CA Certificate is x.509 version 3 in accordance with ITU-T Rec. X.509 (2000) and Common standard ISO/IEC 9594-8 (1997).

7.1.2 Certificate Extensions Populated

7.1.2.1 The Capricorn CA certificate extension fields are defined as per the Inter-Operability Guidelines of the CCA, which is available at http://cca.gov.in.

7.1.3 Cryptographic Algorithm

7.1.3.1 Capricorn CA has adopted the SHA-2 algorithm in conformance with the Inter Operability Guidelines of the CCA, which is available at http://cca.gov.in.

7.1.4 Name Forms

7.1.4.1 Capricorn CA supports unique name.

7.1.5 Name Constraints

7.1.5.1 None specified

7.1.6 Certificate Policy Object Identifier (OID)

7.1.6.1 The Capricorn CA Certificate shall be based on the OID issued by the National Root CA of India

Class	Category	Suggested Use
1	2.16.356.100.2.1	a. Secure E-Mail b. Non-commercial transactions
2	2.16.356.100.2.2	a. Form Signing b. User Authentication c. Other low Risk Transactions d. Secure E-Mail e. Data Encryption
3	2.16.356.100.2.3	a. Form Signing b. User Authentication c. Secure E-Mail d. Data Encryption e. VPN User
Special Class	Special Purpose Certificates (same as Class 3 certificates)	a. Time Stamping services b. OCSP responder services c. Code Signing certificate, d. SSL e. System Certificate f. Encryption Certificate g. Document Signer

7.1.6.2 Class 1 Certificate

Class 1 Digital Signature Certificates are issued to individuals, business and government organizations. They can be used for Web browsing and personal e-mail, to enhance the security of these environments.

Class 1 certificates shall be issued after verification of documents relating to identity proof, address proof and operational e-mail address of the applicant.

7.1.6.3 Class 2 Certificates

Class 2 Digital Signature Certificates are issued to individuals, representatives of business and government organizations after verifying the accuracy of the information submitted by the Subscriber.

7.1.6.4 Class 3 Certificates

Class 3 Digital Signature Certificates are issued to individuals, representatives of business and government organizations.

Class 3 certificates provide a high degree of assurance as the DSC is issued only after verifying the physical presence of the Subscriber and accuracy of the information submitted by the Subscriber.

Class 3 Digital Signature Certificates are used for electronic commerce applications / transactions such as electronic banking, electronic data interchange (EDI), and membership-based online services.

7.1.6.5 Special Class Certificates

Special Class certificates can be issued to devices or systems owned by individuals or organizations for Time Stamping services for OCSP responder services, Code Signing certificate, System Certificate and Encryption Certificate services.

Special Class Certificates, like Class 3 certificates, provide a high degree of assurance as the DSC is issued only after verifying the physical presence of the Subscriber and accuracy of the information submitted by the Subscriber.

The Object Identification (OID) of special class certificate will be the same as that of Class II and Class III DSC as prescribed in the India PKI CP Guidelines

7.1.7 **Usage of the Policy Constraints Extension**

7.1.7.1 None specified

7.1.8 **Policy Qualifiers Syntax and Semantics**

7.1.8.1 None specified

7.1.9 **Processing Semantics**

7.1.9.1 None specified

7.2 CRL Profile

7.2.1 Capricorn CA's CRL Profiles is in conformance with the Inter Operability Guidelines of the CCA which is available at http://cca.gov.in.

8. Specification Administration

8.1 Specification Change Procedures

8.1.1 The contents of this CPS may change periodically. The process for change is as detailed hereunder :

8.1.1.1 Capricorn CA shall follow the defined Change Management Procedure. Each change shall be documented and the change shall be approved / disapproved by the Owner.

8.1.1.2 On approval, the change shall be forwarded to the CCA for approval.

8.1.1.3 On approval by the CCA, the change shall be immediately implemented. Version numbers etc. shall be updated to reflect the changes.

8.1.1.4 The updated CPS shall be published and notified as per 8.2. Publication and Notification Procedures.

8.2 Publication and Notification Procedures

8.2.1 The CPS, and its versions, shall be published on Capricorn CA's website www.certificate.digital,

8.2.2 The changes shall be archived and notified on Capricorn CA's website www.certificate.digital,

8.3 CPS Approval Proceduress

8.3.1 Capricorn CA shall follow the defined Change Management procedure. Each change shall be documented and the change shall be approved / disapproved by the Owner.

8.3.2 On approval, the change shall be forwarded to the CCA for approval.

8.3.3 On approval by the CCA, the change shall be immediately implemented.