(n)Code Solutions CA

A DIVISION OF GUJARAT NARMADA VALLEY FERTILIZERS COMPANY LIMITED

CERTIFICATION PRACTICE STATEMENT

VERSION 2.0

THE *(n)Code Solutions CA* Certification Practice Statement

PRINTED IN INDIA

Acronyms

CA	Certifying Authority
CCA	Controller of Certifying Authorities
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
E-mail	Electronic Mail
FIPS	Federal Information Processing Standard
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
IETF	Internet Engineering Task Force
IT	Information Technology
ITU	International Telecommunications Union
LAN	Local Area Network
LRA	Local Registration Authority
OID	Object Identifier
PCS	The *(n)Code Solutions CA* Public Certification Services
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comment
RSA	Asymmetric Crypto Algorithm for Digital Signatures
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
WAN	Wide Area Network
WWW	World Wide Web
X.509	the ITU-T standard for Certificates and their corresponding authentication framework

WARNING

APPLICABILITY OF THE *(n)Code Solutions CA* PUBLIC CERTIFICATION SERVICES ARE SUBJECT TO ‘ IT ACT 2000’ AND ANY REVISIONS FRAMED THEREUNDER.

ANY STATEMENT WITH SUCH PARTICULARS AS THE CONTROLLER OF CERTIFYING AUTHORITIES (CCA) MAY SPECIFY BY REGULATION IN EXERCISE OF HIS POWERS UNDER THE INFORMATION TECHNOLOGY ACT, 2000 AND ANY REVISIONS THERETO WILL BE APPLICABLE TO THIS *(n)Code Solutions CA* CPS AS WELL.

ANY ACT OF KNOWINGLY PROVIDING FALSE OR INCORRECT INFORMATION WILL BE PENALISED UNDER SEC 73 OF THE INFORMATION TECHNOLOGY ACT, 2000. FURTHER, ANY USE OF THE DIGITAL CERTIFICATES OR CERTIFICATION SERVICES IN INDIA, WHICH CONSTITUTE A FRAUDULENT ACT OR MISUSE, SHALL BE LIABLE TO BE PROCEEDED WITH CONSEQUENCES CIVIL AND CRIMINAL, AND SUBJECTED TO PENALTIES AND PUNISHMENT UNDER THE RELEVANT ACTS. IT IS ASSUMED THAT SUBSCRIBERS ARE ADEQUATELY AWARE OF THE SPECIFIC DUTIES OF SUBSCRIBERS AS CONTAINED IN CHAPTER VIII OF THE INFORMATION TECHNOLOGY ACT, 2000 AND RULES AND CONTENTS OF THIS DOCUMENT.

ASSISTANCE WILL BE PROVIDED TO INDIAN LEGAL AUTHORITIES BY THE *(n)Code Solutions CA* AND ITS EMPLOYEES IN THE PROSECUTION OF ANY PERSON WHO ALLEGEDLY COMMITS A CRIME OR ANY ACT DIRECTLY AFFECTING THE *(n)Code Solutions CA* PUBLIC CERTIFICATION SERVICES.

BRIEF NOTES ON IMPORTANT CPS RIGHTS AND OBLIGATIONS

PLEASE SEE THE TEXT OF THIS CPS FOR DETAILS. THIS BRIEFING IS INCOMPLETE. MANY OTHER IMPORTANT ISSUES HAVE BEEN DISCUSSED IN DETAIL IN THE CPS.

The ***(n)Code Solutions CA*’s** Public Certification Service (PCS) offers Digital Signature Certificates recognised under the Information Technology Act, 2000.

1. Provisions and use of the ***(n)Code Solutions CA*’s** Public Certification Services [Section 2] -- including certificate application [Section 4.1], certificate issuance [Section 4.2], acceptance [Section 4.3], use and revocation [Section 4.4] have been specified in this ***(n)Code Solutions CA*** CPS.

2. Every user of this CPS acknowledges that the user has been advised to receive proper training in the use of public key techniques prior to applying, using, and relying upon a certificate and that the documentation, training, and education about digital signatures, certificates, PKI, and the PCS are available from the ***(n)Code Solutions CA***.

3. The ***(n)Code Solutions CA*** offers different classes of certificates [Section 4.1]. The User reserves the right to select the certificate that suits the user’s needs amongst the classes of certificates offered by the ***(n)Code Solutions CA***.

4. The user must generate a key pair [Section 6.1] and keep the private key secure from compromise in a trustworthy manner [Section 6.2]. User’s software system should provide this functionality.

5. The user must accept [Section 4.3] a certificate before communicating it to others, or otherwise inducing its use.

6. The responsibility whether to rely on a digital signature or certificate rests with its Relying Party. The ***(n)Code Solutions CA*** recommends that prior to relying on a Digital Signature or Certificate, the recipient may confirm the validity of the certificate at the ***(n)Code Solutions CA*** repository at www.ncodesolutions.com. After confirming the validity, the recipient may then use the certificate to verify [Section 2.1.4] that the digital signature was created during the operational period of the certificate by the private key corresponding to the public key listed in the certificate, and that the message associated with the digital signature has not been altered.

7. The user agrees to notify the ***(n)Code Solutions CA*** upon compromise of private key.

8. This CPS provides various liabilities and warranties made by the ***(n)Code Solutions CA*** [Section 2.2]. ***(n)Code Solutions CA*** has also given details of its Refund Policy in Section 2.5.5. Unless expressly specified in writing, warranties are disclaimed and liability is limited by ***(n)Code Solutions CA*** . [Sections 2.2].

9. Please call Tel: 91-79-26857315 for any queries regarding the deployment of, and reliance on, the ***(n)Code Solutions CA*** certificates.

For more information, visit the ***(n)Code Solutions CA's*** *web site or contact customer service.*

Comments And Suggestions

Comments and Suggestions for the future revisions and betterment of the CPS are solicited from users. Comments and suggestions could be forwarded to : **support@ncodesolutions.com**

Contact Address:

(n)Code Solutions
A Division of Gujarat Narmada Valley Fertilizers Company Ltd.,
301, GNFC Infotower,
Bodakdev,
Ahmedabad – 380054
Gujarat, India.
Website : www.ncodesolutions.com
Contact us at : support@ncodesolutions.com

TABLE OF CONTENTS

Definitions

The following definitions are to be used while reading the CPS of *(n)Code Solutions CA* (A Division of Gujarat Narmada Valley Fertilizers Company Limited),(hereinafter referred to as "The *(n)Code Solutions CA*") CPS. The definitions are provided in alphabetical order.

1) "Access" with its grammatical variations and similar expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network .
2) The word "Act" means the set of the following:
   a. The Information Technology Act, 2000
   b. The Information Technology (Certifying Authorities) Rules, 2000
   c. The Information Technology (Certifying Authority) Regulations, 2001
   d. Guidelines and Circulars issued by the Office of Controller of Certifying Authorities from time to time
3) "Affixing Digital Signature" with its grammatical variations and similar expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Digital Signature
4) "Applicant" is an end entity requesting a digital signature certificate and remains one before downloading his digital signature certificate
5) "Asymmetric Crypto System" means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.
6) "Auditor" means the auditor empanelled by the Controller of Certifying Authorities for conducting audit of Certifying Authority infrastructure - technical, physical and procedural.
7) "Authentication Code "and "Reference Code "together form a shared secret which is used to make secure communication between the applicant and the *(n)Code Solutions CA*.
8) "CA" refers to the Certifying Authority licensed by the Controller of Certifying Authorities.
9) "CA Administrator " is responsible for performing all CA related functions
10) "Compromise" means 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
11) "Computer" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network
12) "Computer Resource" means computer, computer system, computer network, data, computer data base or software
13) "Controller" means Controller of Certifying Authorities appointed under subsection (1) of Section 17 of the Act.
14) "CPS" means the *(n)Code Solutions CA* Certification Practice Statement

15) "Data" means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer

16) "Digital Signature" means authentication of any electronic record by a Subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act 2000.

17) “Digital Signature Certificate” means a Digital Signature Certificate issued under subsection 4 of section 35 of the Information Technology Act, 2000 and in accordance with chapter 4 (Operational requirement) of this CPS.

18) “End Entity” refers to any entity either the applicant/Subscriber/Relying Party who is the end user of the *(n)Code Solutions CA* Digital Signature Certificate

19) “Entity” refers to the users of the Digital Signature Certificate

20) “Information Asset” means all information resources utilized in the course of any organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks)

21) "Key Pair", in an asymmetric crypto system, means a private key and its mathematically related unique public key, which are so related that the public key can verify a Digital Signature created by the private key

22) “License” means a license granted to a Certifying Authority under section 24 of the Information Technology Act, 2000.

23) “Licensed Certifying Authority” refers to the *(n)Code Solutions CA* and other Certifying Authorities who have been granted licence under section 24 of the Information Technology Act, 2000.

24) “LRA” (Local Registration Authority) is an agent of the RA who performs verification of Digital Signature Certificate Request and related documents and approves or rejects the application based on the results of the verification process.

25) “Person” shall include an individual or a company or association or body of individuals, whether incorporated or not, or Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments

26) "Private Key" means one of the key of a key pair used to create a Digital Signature

27) "Public key" means one of the key of a key pair used to verify a Digital Signature and is listed in the Digital Signature Certificate.

28) “RA” (Registration Authority) is responsible for initiating the certificate issuance process after receiving approved application request from the LRA.

29) “RCAI” means the Root Certifying Authority of India established by the CCA under Section 18 (b) of The Information Technology Act 2000 to digitally sign the Public keys of the Certifying Authorities in the country.

30) “Relying Party” is an entity who relies on the information provided in a valid Digital Signature Certificate.

31) “SSL Server certificate Applicant” means a person , which can be either an Individual or an Enterprise ,applying for the *(n)Code Solutions CA* class IIIc certificate.

32) "Subscriber" means an end entity in whose name the Digital Signature Certificate has been issued and becomes one, once he successfully downloads the digital signature certificate. The term Subscriber includes an Individual Subscriber or an Enterprise Subscriber.

33) “Subscriber Identity Verification Method” means the method used to verify and authenticate the identity of a Subscriber by CA for the purpose of issuing Digital Signature Certificate.

34) “Trusted Person” means any person who has:

   a. direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act in respect of a Certifying Authority

   b. or duties directly involving the issuance, renewal, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority)

   c. or administration of a Certifying Authority's facilities

   d. or Creation and Management of CA signing keys.

35) “Sub CA” means a Certifying Authority falling under the *(n)Code Solutions CA* and the Public Key of such Sub CA is signed by the Private Key of the *(n)Code Solutions CA*.

36) “User” means Applicants, Subscribers and Relying Party with reference to the the *(n)Code Solutions CA*.

37) "Verify" in relation to a Digital Signature, electronic record or public key, with its grammatical variations and similar expressions means to determine whether -

   a. The initial electronic record was affixed with the Digital Signature by the use of private key corresponding to the public key of the Subscriber

   b. The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the Digital Signature.

Note : Words and expressions used herein and not defined shall have the meaning respectively assigned to them in that context. In case of conflict between the definitions given here and Definitions in the Act, definitions given in the Act shall prevail.

IN THE CPS , EXCEPT TO THE EXTENT THAT THE SUBJECT MATTER OR CONTEXT MAY OTHER WISE REQUIRE,

(I) EXPRESSIONS INCLUDING THE SINGULAR MAY INDICATE THE PLURAL AND VICE VERSA,

(II) EXPRESSIONS INDICATING ANY PARTICULAR GENDER MAY INDICATE ALL OTHER GENDERS AND

(III) EXPRESSIONS INDICATING BODIES CORPORATE MAY ALSO INDICATE NATURAL PERSONS AND VICE VERSA.

1. INTRODUCTION

This section presents the brief explanation of the Certification Practice Statement contents and its purpose.

1.1 Overview

1.1.1 The *(n)Code Solutions CA* in its capacity as a Certifying Authority (CA) acts as a trusted third party to confirm that a public key belongs to a named entity. Such confirmation is expressly represented by a *(n)Code Solutions CA* X.509 Version 3 Certificate (henceforth termed Certificate). An issued Certificate is a statement by the CA that the Certificate is associated with the person uniquely named within that Certificate.

1.1.2 To support its CA role, the *(n)Code Solutions CA* has established the *(n)Code Solutions CA* Public Certification Services Framework (the "*(n)Code Solutions CA* PCS") to issue, revoke, and renew Certificates in accordance with the practices set out in this CPS. The *(n)Code Solutions CA* PCS is designed to support secure electronic commerce and other general security services.

1.1.3 The *(n)Code Solutions CA* CPS is a detailed statement of the practices and operational procedures of the *(n)Code Solutions CA*.

1.1.4 The *(n)Code Solutions CA* has implemented various certificate classes and may implement changes to Certificate classes from time to time.

1.1.5 The electronic copy of the CPS can be found at the *(n)Code Solutions CA* web site at www.ncodesolutions.com or at such other places as may be determined by the *(n)Code Solutions CA*.

1.1.6 The *(n)Code Solutions CA* CPS is (i) intended to be applicable to and is a legally binding document between the *(n)Code Solutions CA*, its Registration Authorities (RAs), the Subscribers, the applicants, Subordinate CAs, the Relying Parties and each of their agents, employees and contractors; and (ii) intended to serve as notice to all parties within the context of the *(n)Code Solutions CA* PCS. Parties within the *(n)Code Solutions CA* PCS are required to understand and consult CPS in force from time to time during the lifetime of the Certificate

1.1.7 The CPS describes the entire certification process which begins with CA establishment and start-up procedures and then covers general CA operations, subscriber enrolment, certificate issuance, use of certificates; certificate revocation, and expiration.

1.1.8 This CPS should be cited in other documents as the “*(n)Code Solutions CA* CPS” or the “*(n)Code Solutions CA* Certification Practice Statement.” It is internally cited as the “CPS”. The CPS is updated periodically. Versions of the CPS are denoted by a version number following “CPS” (e.g., “version 2.0” or “CPS 2.0”).

1.1.9 This CPS assumes that the reader possesses a basic level of knowledge or training of digital signatures, PKI methodology, and the *(n)Code Solutions CA* PCS in general. The *(n)Code Solutions CA* recommends that the reader must have basic level knowledge or some training in the use of public key techniques before the reader applies for a certificate. Further the *(n)Code Solutions CA* provides such educational and training information and services; the details for the same are accessible from the *(n)Code Solutions CA* website at www.ncodesolutions.com . Additional assistance is available from the *(n)Code Solutions CA* customer service representatives) support@ncodesolutions.com

1.1.10 The Act lays the foundation for Public Key Infrastructure and Electronic Transactions in India. The Act further awards evidentiary status to Digital Signatures in the Indian Courts of Law in lieu of physical signatures. A Statutory body viz: - the Controller of Certifying Authorities (CCA) has been set up under the Act to license the Certifying Authority (CA) who will issue Digital Signature certificates.

1.2 Identification

The *(n)Code Solutions CA* is assigned an Object Identifier (OID) (in ASN 1.3 format) by the Controller of Certifying Authorities.

1.3 Community & Applicability

1.3.1 **Certifying Authority (CA)**

1.3.1.1 The *(n)Code Solutions CA* is the CA licensed by CCA under the Indian Information Technology Act, 2000 that will create, sign and issue Certificates. Each Certificate shall bind the public key of each entity to its Digital Signature Certificate.

1.3.1.2 The *(n)Code Solutions CA* is a subordinate Certifying Authority to RCAI (Root Certifying Authority of India). The hierarchial implementation of PKI, with RCAI as the root, provides a natural cross certification model for all licensed Certifying Authorities. *(n)Code Solutions CA* may enter into cross certification arrangements with other licensed Certifying Authorities which shall be governed by the requirements under Rule 12 of the Information Technology Act 2000.

1.3.2 **Registration Authority (RA) / Local Registration Authority (LRA)**

1.3.2.1 Registration Authority (RA) is physically located at *(n)Code Solutions CA.* Whereas, Local Registration Authorities (LRAs) are geographically separate units, located at various locations around India. Basic interaction and identity / documents verification is performed by LRAs, whereas, technical activities such as addition / deletion of user is performed by RA. RA and LRA are jointly involved through the various phases in Digital Certificate life cycle starting with Certificate Application (Section 4.1) and ending with Certificate Revocation (Section 4.4).

1.3.2.2 Chapter 4 – Operational Requirements, of this CPS contains detailed registration procedure for various classes of certificates. Agreement with RAs & LRAs further clarify Roles and Responsibilities of RAs and LRAs. An LRA may employ agent(s) / to perform the registration functions in which case the LRA shall be directly accountable for the activities of the agent(s) and the functions that the agent performs on behalf of the LRA. The actions, inactions, and/or omissions of each agent shall be deemed to be the actions, inactions, and/or omissions of the LRA.However, (n)Code Solutions CA shall be responsible for all actions of RA, LRA or any agent appointed by the LRA to perform registration functions.

1.3.3 End Entity

1.3.3.1 Subscriber

Digital Certificate registration procedure clearly differentiates between the term “Applicant” and “Subscriber”. A person is termed as an Applicant till the time he downloads a Digital Certificate, whereas, his/her status changes to a Subscriber post download of Certificate. Downloading a Digital Signature Certificate from the *(n)Code Solutions CA* website constitutes acceptance of the Certificate. The term Subscriber includes an Individual Subscriber or an Enterprise Subscriber.

1.3.3.2 Relying Party

It is an entity that relies on the information provided in a valid Digital Signature Certificate issued by the *(n)Code Solutions CA* and/or on any other information provided in the *(n)Code Solutions CA* Repository to verify the identity and public Key of a Subscriber. The *(n)Code Solutions CA* offers these services through provision of a Repository in the form of updated Certificate Revocation Lists

1.3.4 Applicability

1.3.4.1 *(n)Code Solutions CA* Certificates are intended to support the following core security needs — Authentication - provides assurance of the identity of the Subscriber; Message integrity - checks that the content of a message is intact, and has not been altered in any way between the time of sending and its receipt; and

Digital Signature - facilitates non repudiation by providing assurance to the Relying Party against denial from a Subscriber that such Subscriber has authorised any particular transaction, if the transaction has been digitally signed by the Subscriber.

1.3.4.2 The *(n)Code Solutions CA* Certificates issued under this CPS are not designed, intended or authorized for use or resale as control equipments in hazardous circumstances or for users requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, etc where failure could lead directly to death, personal injury or severe environmental damage.

1.3.4.3 In addition, the *(n)Code Solutions CA* Certificate may be used to support confidentiality for the specific purpose of encrypting revocation requests only. The *(n)Code Solutions CA* shall not be responsible or liable in relation to use of Digital Certificate for any other confidentiality features and disclaims all direct and indirect damages, losses or liabilities that arise out of or pursuant to any such use.

1.3.4.4 The *(n)Code Solutions CA* PCS has been designed to support secure electronic commerce and other general security services to satisfy user’s technical, business, and personal needs for digital signatures and other network security services like SSL (Secure Socket layer). Independent assessment and determining the appropriateness of each class of Certificate for any particular purpose is the responsibility of the Subscribers and Relying Party.

1.3.4.5 The *(n)Code Solutions CA* shall not be responsible for any liabilities howsoever arising from the use of any Certificate unless the *(n)Code Solutions CA* has expressly undertaken to assume such liabilities in this CPS.

1.4 Contact Details

1.4.1 Specification Administration Organisation

This *(n)Code Solutions CA* CPS is published and administered by the *(n)Code Solutions CA* India

1.4.2 Contact Person

Chirag Mehta
(Help Desk)
(n)Code Solutions CA
A Division of Gujarat Narmada Valley Fertilizers Company Limited,
301, GNFC Infotower,
Bodakdev,
Ahmedabad - 380054
E-mail: support@ncodesolutions.com
Phone : 91 – 79 – 2685 7315

1.4.3 Person Determining CPS Suitability for the Policy

The suitability of the CPS is determined by the management of the (n)Code Solutions CA.

2. GENERAL PROVISIONS

This section provides an insight to the various obligations, liabilities, responsibilities and financial and legal considerations associated with the use of the ***(n)Code Solutions CA*** certificates.

The terms of this CPS are deemed to be effective:

– Upon publication of this CPS in-case of RA/ LRA and CA/Sub-CA

– Upon submission of an application for a ***(n)Code Solutions CA*'s** Digital Signature Certificate in-case of an Applicant.

2.1 Obligations

2.1.1 CA Obligations

2.1.1.1 Notwithstanding, any other provisions to the contrary contained in this CPS, the *(n)Code Solutions CA*'s obligations are to ensure —

That the *(n)Code Solutions CA* shall perform CA services and operations, and maintain the infrastructure related to certificates issued under this CPS, in substantial conformity with the requirements of the Information Technology Act, 2000 and this CPS.

That the public key algorithm employed and deployed by the *(n)Code Solutions CA* and *(n)Code Solutions CA*'s private signing key will be reasonably secured and safeguarded within the *(n)Code Solutions CA* PCS in accordance with government regulation and industry practices.

2.1.1.2 The provision set out above in Section 2.1.1.1 shall be *(n)Code Solutions CA*'s sole and absolute obligations in relation to its capacity as a CA and nothing contained herein this CPS shall be deemed to or be construed so as to imply that the *(n)Code Solutions CA* will be obliged to perform any other functions, or be obliged to ensure that any other matters are carried out by the *(n)Code Solutions CA*, its servants, employees or agents.

2.1.1.3 For purposes of clarity, this CPS sets out the procedures by which the *(n)Code Solutions CA* observes the *(n)Code Solutions CA* PCS and the technology under which the *(n)Code Solutions CA* deploys. Such services but all such procedures shall not be deemed to be obligations of *(n)Code Solutions CA* to perform, adhere or comply with but are merely procedures by which the *(n)Code Solutions CA* operates on in its PCS. The only obligations which the *(n)Code Solutions CA* is obliged to perform, adhere or comply with are set out above in Section 2.1.1.1.

2.1.1.4 The *(n)Code Solutions 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, civil disturbances, actions or inactions of suppliers, acts of God, war, fire, explosion, earthquake, flood or other catastrophes.

2.1.1.5 In any of the events mentioned in Section 2.1.1.4 hereof, the *(n)Code Solutions 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 LRA Obligations

2.1.2.1 The LRA is required to and shall comply with all registration procedures and safeguards as may be determined by the *(n)Code Solutions CA* and as set out in this CPS or the applicable LRA Agreement or as may be subsequently amended by the *(n)Code Solutions CA*. Without otherwise limiting their authority, LRAs may rely upon the following for confirming certificate applicant information: (i) notarisations that reasonably appear to be performed in good order and (ii) well-recognised forms of identification, as specified in section 4.2 for the identification requirements for various classes of certificates.

2.1.2.2 LRA is required to adhere to and comply with the provisions contained in this CPS specifically including but not limited to the provisions set out in Section 3.1 (Initial Registration) below. The LRA shall keep all such information given in clause 2.8.1.2 confidential.

2.1.3 Subscriber Obligations

All Subscribers are required to comply strictly with the procedures in relation to the application of Certificate and safekeeping and possession of their private keys. Subscribers shall undertake,

2.1.3.1 That all statements or information provided by the Subscriber in the Certificate application forms must be complete, accurate, true and correct in all respects and could be verified by LRA / the *(n)Code Solutions CA* or the RA;

2.1.3.2 That the procurement of a certificate from the *(n)Code Solutions CA* follows Certificate Application Process (4.1.2), Certificate Issuance Process (4.2.2) and Certificate Download and Acceptance Process (4.3.2);

2.1.3.3 That no other person other than the Subscriber has had access to the Subscriber's private signing key;

2.1.3.4 That all physical security measures as may be described in this CPS or as may be applicable under the Act and any other law in force or recommended by the *(n)Code Solutions CA* are observed and complied with to ensure the adequate and secure protection of the Subscriber's private keys;

2.1.3.5 That the Subscriber is familiar with the provisions of this CPS in relation to his Certificate and shall be familiar with and adhere to the restrictions applicable to the use of the Subscriber's Certificate;

2.1.3.6 That the Subscriber shall notify the *(n)Code Solutions CA* of any change in the information in the certificate at the earliest;

2.1.3.7 That the Subscriber shall promptly notify the *(n)Code Solutions CA*, occurrence of any event that would lead to the compromise, including but not limited to loss of, misplacement or exposure, of the Subscriber's private keys

2.1.4 Relying Party Obligations

All Relying Parties are required to ensure and acknowledge that the following provisions are adhered to when relying on any of the provisions in the Digital Certificate:

2.1.4.1 That the Relying Party is familiar with the provisions of this CPS in relation to the Subscriber's Certificate and shall be familiar with and shall comply with the purposes for which the Certificate is used.

2.1.4.2 The Relying Party is required to use the Subscriber's Certificate for its intended use only.

2.1.4.3 That the Relying Party, when relying on the Subscriber's Certificate, is required to check the status of that Certificate against appropriate and current CRL in accordance to the CRL practice and procedure in Section 4.4

2.1.4.4 That the Relying Party acknowledges the liability caps and warranties as mentioned in this CPS.

2.1.4.5 That the Relying Party has checked that the certificate is not expired

2.1.5 Repository Obligations

The *(n)Code Solutions CA* shall publish the *(n)Code Solutions CA* CPS and its CA Certificate in its repository which shall be updated whenever there is any change in any of them. The CRLs shall be published and updated in the *(n)Code Solutions CA* Repository, once every business working day. This Repository is made available at the *(n)Code Solutions CA* website at www.ncodesolutions.com.

2.2 Liability

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

THE *(n)Code Solutions CA* MAKES NO OTHER WARRANTIES EXPRESS OR IMPLIED AND HAS NO FURTHER OBLIGATIONS UNDER THIS CPS UNLESS PROVIDED EXPRESSLY IN THIS CPS.

2.2.1.2 Kinds of damages covered

The nature and extent of damages that *(n)Code Solutions CA* shall be liable for are provided in clause no. 2.2.1.3 and 2.2.1.4 . The *(n)Code Solutions CA* shall not be liable for any loss or damage whatsoever or howsoever caused arising directly or indirectly in connection with the use or reliance on any Certificate by any parties. Notwithstanding any other provisions to the contrary, the *(n)Code*

Solutions CA has expressly excluded liability for all indirect, special, incidental and consequential loss or damage, howsoever caused including without limitation, negligence, default or any acts of the *(n)Code Solutions CA*, its employees, agents, contractors, representatives, including but not limited to loss or damage to other equipment or property or for loss of profit, business, revenue, goodwill or anticipated savings pursuant to the use or reliance of any Certificate or any other transactions, services offered or contemplated by this CPS even if the *(n)Code Solutions CA* has been advised of the possibility of such damages. No action arising pursuant to the use or reliance of any Certificate, regardless of form, may be brought by any parties more than three (3) years after such cause of action has arisen.

2.2.1.3 Loss Limitations

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 (ii) the *(n)Code Solutions CA* breaches any of its obligations pursuant to Section 2.1 above, and the *(n)Code Solutions CA* becomes liable for loss or damage that would otherwise have been excluded hereunder or excludable in law, the *(n)Code Solutions 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 *(n)Code Solutions 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 2.1, BELOW.

CERTIFICATE CLASSES	LIABILITY CAPS (RS)
Class I	NIL
Class IIa	NIL
Class IIb	Rs. 5,000/-
Class IIIa	Rs. 10,000/-
Class IIIb	Rs. 10,000/-
Class IIIc	Rs. 10,000/-
Class IIId	Rs. 10,000 /-

TABLE 2.1 - LIABILITY CAPS

2.2.1.4 **Other Exclusions**

a. Digital Signature Certificates issued by the *(n)Code Solutions CA* should not be used or sold for critical systems where failure could lead directly to death, personal injury or severe environmental damage. The *(n)Code Solutions CA* expressly disclaims liability of any kind arising due to such usage.

b. The *(n)Code Solutions CA* disclaims liability from loss of profits and loss of Data and 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, civil disturbances, actions or inactions of suppliers, acts of God, war, fire, explosion, earthquake, flood or other catastrophes.

c. The *(n)Code Solutions CA* disclaims liability from any other damage except for those due to reliance of verified information in a certificate.

d. The *(n)Code Solutions CA* disclaims any liability incurred if the error in such verified information is not attributed to the *(n)Code Solutions CA* including error handling arising out of fraud/wilful misconduct of the applicant.

2.2.2 **LRA Liability**

2.2.2.1 The LRA will undertake liability to ensure that for obtaining a Digital Certificate, adequate verification of the Applicant will be ensured. Further liabilities of the LRA are addressed in the appropriate and applicable LRA Agreement entered into between the applicable LRA and the *(n)Code Solutions CA*.

2.2.2.2 The LRA undertakes to ensure the forwarding of Certificate application request and revocation request of Subscriber to the *(n)Code Solutions CA*.

2.2.3 **Subscriber Liability**

The *(n)Code Solutions CA* Subscriber Agreement requires Subscribers to warrant that:

2.2.3.1 Each Digital Signature created using the private key corresponding to the public key listed in the Certificate is the Digital Signature of the Subscriber,

2.2.3.2 No other person has ever had access to the Subscriber's private key,

2.2.3.3 All representations and information given by the Subscriber in the Certificate Application are true and valid at the time of certificate usage.

2.2.3.4 All information supplied by the Subscriber and contained in the Certificate is true,

2.2.3.5 The subscriber is also liable to provide timely information to the *(n)Code Solutions CA* about Certificate revocation in case of loss / compromise of private key.

2.2.3.6 The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS, specifically for the purpose as stipulated/stated in the certificate application form only, and

2.2.3.7 The Subscriber is an end-user and not a CA, and is not using the private key corresponding to public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

2.2.4 Relying Party Liability

Relying Parties acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations as mentioned in section 2.1.4.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Party and Subscriber

2.3.1.1 In the event of or as a result of any act or default by the Relying Party, its agents and employees making use of or relying on the Digital Signature Certificate, any or all of the above parties agree to indemnify the *(n)Code Solutions CA* from and against all loss, damage, liability , legal fees and costs incurred by the *(n)Code Solutions CA*.

2.3.1.2. Subscribers are liable for any misrepresentations or any other statements made with fraudulent intent, negligence or error in their applications for Certificate to relying parties, who reasonably rely on the representations contained therein.

2.3.1.3 *(n)Code Solutions CA*, ITS RA, LRAs AND THEIR AGENTS AND CONTRACTORS SHALL BE HELD HARMLESS BY SUBSCRIBERS AND RELYING PARTIES FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE AND ANY SUITS AND EXPENSES OF ANY KIND INCLUDING REASONABLE LEGAL FEES, THAT THE *(n)Code Solutions CA*, ITS RA, 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 AUTHORISED 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 *(n)Code Solutions CA*, ITS RA, THEIR AGENTS AND CONTRACTORS OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE (iii) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE, LOSS, DISCLOSURE, MODIFICATION OR UNAUTHORISED USE OF THE SUBSCRIBER'S PRIVATE KEY. THIS STATEMENT IS IN ACCORDANCE WITH SECTION 73 OF THE INDIAN INFORMATION

TECHNOLOGY ACT , WHICH PRESCRIBES PENALTIES FOR THE FRAUDULENT USE OF DIGITAL SIGNATURES.

2.3.1.4 Subscriber along with Relying Party shall jointly and severally indemnify the *(n)Code Solutions CA*, its RA, LRA and their agents and contractors pursuant to this CPS. The Subscriber is solely responsible for notifying the *(n)Code Solutions CA* of any misrepresentations and omissions made by an agent.

2.3.2 Fiduciary Relationships

The (n)Code Solutions CA and RA are not the agents, fiduciaries, trustees or other representatives of Subscriber or Relying Party. The relationship between the (n)Code Solutions CA and Subscriber and that between the (n)Code Solutions CA and Relying Party are not that of agent and principal. Neither Subscriber nor Relying Party have any authority to bind the (n)Code Solutions CA, by contract or otherwise, to any obligation. The (n)Code Solutions CA does not make any representations to the contrary, either expressly, implicitly, by appearance or otherwise.

2.3.3 Administrative Processes

Administrative procedures (such as accounts and annual report) maybe published yearly in accordance with the laws of the Republic of India.

2.4 Interpretation and Enforcement

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

2.4.1 Governing Law

The laws of India and more particularly the Information Technology Act, 2000, The Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001, and the guidelines issued and clarifications made from time to time by the Controller of Certifying Authorities, Ministry of Information Technology shall govern the construction, validity, enforceability and performance of the *(n)Code Solutions CA* CPS.

2.4.2 Severability of Provisions, Survival, Merger & Notice

2.4.2.1 Severability of Provisions

In the event that any or any part of the terms, conditions or provisions contained in this CPS are determined invalid, unlawful or unenforceable to such extent any term, condition or provision shall be severed from the remaining terms, conditions and provisions which shall continue to be valid and enforceable to the fullest extent permitted by the Governing Law.

This CPS shall supersede any and all previous negotiations, agreements, memoranda and commitments in relation to the subject matter unless otherwise explicitly mentioned in those agreements. The *(n)Code Solutions CA* shall be entitled to amend, modify and change any of the terms, conditions or provisions herein contained at any time and without prior notice to any parties, excepting the Controller of Certifying Authorities of India. The *(n)Code Solutions CA* shall be entitled to place and/or publish amendments in the *(n)Code Solutions CA* repository either (i) in the form of an amended version of the CPS; (ii) in the *(n)Code Solutions CA* website at www.ncodesolutions.com ; (iii) in such other manner as may be determined by the *(n)Code Solutions CA*. All amendments, modification and changes shall, unless otherwise expressly stated in such amendments, modification and changes are effective immediately upon placement and/or publication. The subscriber's decision not to request revocation of his Certificate within fifteen (15) days following such placement and/or publication shall constitute agreement to the amendments, modification and changes.

The *(n)Code Solutions CA*'s failure or forbearance to enforce any right or claim against any party arising hereunder shall not be deemed to be a waiver by the *(n)Code Solutions CA* to such right or claim. Any of the *(n)Code Solutions CA*'s waiver of a breach of any provision of this CPS shall not operate or be construed as a waiver of any subsequent breach or breaches of the same or any other provision.

2.4.2.2 Survival

The obligations and restrictions contained within CPS (Audit, Confidential Information, Obligations of the *(n)Code Solutions CA* and the RA, and Limitations Upon Such Obligations) shall survive the termination of this CPS.

2.4.2.3 Merger

Should the *(n)Code Solutions CA* merge with another entity, the obligations and restrictions (Audit, Confidential Information, Obligations of the *(n)Code Solutions 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

Any notice required or permitted to be given to a Subscriber shall be in writing and shall in the case of a recipient being (i) a company be sent to its registered office from time to time; (ii) an individual be sent to its address as set out in its application. Any such notice shall be delivered personally or sent in a letter by the recorded delivery service and shall be deemed to have been served if by personal delivery when delivered and if by recorded delivery 48 hours after posting. If the *(n)Code Solutions CA* so elects, the *(n)Code Solutions CA* shall be entitled to send any such notice to the Subscriber via electronic mail ("e-mail") to the e-mail address designated by the Subscriber at the time of application for the Certificate.

Any notice required or permitted to be given to the *(n)Code Solutions CA* shall be in writing and shall be sent to its designated office from time to time. Current designated office for the above mentioned purpose is,

(n)Code Solutions CA
A Division of Gujarat Narmada Valley Fertilizers Company Limited,
301, GNFC Infotower,
Bodakdev,
Ahmedabad 380054
Gujarat, India

Any such notice shall be delivered personally or sent in a letter by the recorded delivery service and shall be deemed to have been served, if by personal delivery when delivered, and if by recorded delivery, 48 hours on receipt by the *(n)Code Solutions CA*. Any such notices may be sent to the *(n)Code Solutions CA* via electronic mail ("e-mail") and such notices shall only be deemed to be valid if the Subscriber confirms such e-mail notices to the *(n)Code Solutions CA* in writing within 24 hours of the receipt of the e-mail notice by the *(n)Code Solutions CA*.

2.4.2.5 Each of the Certificate and all the terms and provisions of this CPS are personal to each of the Subscriber and the Subscriber shall not assign their Certificate to any other parties.

2.4.2.6 The headings contained in this CPS are inserted for convenience of reference only and are not intended to be part of or to affect the meaning or interpretation of any of the terms, conditions or provisions of this CPS.

2.4.3 Dispute Resolution Procedures

2.4.3.1 For any disputes CPS, the aggrieved party shall first intimate the *(n)Code Solutions CA* Helpdesk either through phone, e-mail or fax or post for the purpose of dispute resolution.
If the dispute is not resolved within ten (10) business working days after initial notice as above, then aggrieved party shall submit the dispute in writing to Distinguished Panel of Experts maintained by the *(n)Code Solutions CA*.

2.4.3.2 If the dispute cannot be amicably resolved by the parties, as per section 2.4.3.1, then the matter will be referred to the Controller of Certifying Authorities. The parties may refer the dispute to arbitration and the provisions of Arbitration and Reconciliation Act 1996 will prevail. Each party shall be entitled to appoint an arbitrator each. Each of the arbitrators can in turn appoint a third arbitrator for dispute resolution. The CCA is competent under the IT Act, clause 18(l), to resolve any dispute between Certifying Authorities and Subscribers. However, Cyber Appellate Tribunal, under the Information Technology 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 Ahmedabad.

2.5 Fees

2.5.1 Certificate Issuance & Renewal Fees

The *(n)Code Solutions CA* charges Subscribers and all such other parties for their use of the *(n)Code Solutions CA*'s PCS and all Subscriber and all such other parties shall be obliged to pay to the *(n)Code Solutions CA* such charges in accordance with its Schedule of Fees and at such times as may be prescribed by the *(n)Code Solutions CA*. Current schedule of Fees is published on the *(n)Code Solutions CA* website www.ncodesolutions.com.

2.5.2 Certificate Access Fees

No fee is charged for certificate access. This is subject to change and any such change shall be published at the *(n)Code Solutions CA* website immediately.

2.5.3 Revocation or Status Information Access Fees

No fee is charged for certificate revocation or status information access. This is subject to change and any such change shall be published at the *(n)Code Solutions CA* website immediately.

2.5.4 Fees for Other Services such as Policy Information

No fee is charged for other services like online access of this CPS. A fee of Rs. 1,000/- (Rupees One Thousand only) shall be charged for a printed version of this CPS.

This is subject to change and any such change shall be published at the *(n)Code Solutions CA* website immediately.

2.5.5 Refund Policy

The *(n)Code Solutions CA* does not provide any refund of the fees paid for the *(n)Code Solutions CA* Digital Signature Certificates or services provided by the *(n)Code Solutions CA*.

The *(n)Code Solutions CA* 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. Upon a refusal to issue a Certificate, the *(n)Code Solutions CA* shall refund to any Certificate applicant any paid Certificate enrolment fee, unless the Certificate applicant submitted fraudulent or falsified information to the LRA. In such a case the fee shall not be refunded.

2.6 Publication and Repositories

The *(n)Code Solutions CA* shall maintain the repository to store information relevant to the operations of the *(n)Code Solutions CA* Public Key Infrastructure Services. All the information and modifications are published in the repository to provide access to the updated information. This information is subject to changes and any such change shall be published in the *(n)Code Solutions CA* repository as detailed in other relevant sections of this CPS.

2.6.1 Publication of CA Information

2.6.1.1 The following information is published in the *(n)Code Solutions CA* repository at www.ncodesolutions.com :

a. The *(n)Code Solutions CA* CPS

b. The Certificates issued by the *(n)Code Solutions CA* and the status information of the Certificates which can be verified in the *(n)Code Solutions CA* repository through a link provided at www.ncodesolutions.com.

c. The Certificate of the *(n)Code Solutions CA* corresponding to its private key

d. The CRL for the Certificates revoked by the *(n)Code Solutions CA*. The CRL shall be updated frequently as mentioned in this CPS and updated in the Repository

2.6.1.2 The following information is published on the *(n)Code Solutions CA* website at www.ncodesolutionss.com :

a. Fee structures of the various services

b. Search facility for Digital Certificates

c. Search facility for various services

2.6.2 Frequency of Publication

The *(n)Code Solutions CA* shall publish the *(n)Code Solutions CA* CPS and its CA Certificate in its repository which shall be updated whenever there is any change in them. The CRLs shall be published and updated in the *(n)Code Solutions CA* Repository, once every business working day. This Repository is made available at the (n)Code Solutions CA website at www.ncodesolutions.com. This shall be done in accordance with the policy set forth in the Section 8 of this CPS.

2.6.3 **Access Control**

2.6.3.1 The *(n)Code Solutions CA* publishes information as provided in Clause 2.6.1 on the *(n)Code Solutions CA* website which would be accessible to the *(n)Code Solutions CA* ,all RA/LRA, Applicants, Subscribers, Relying Parties.

2.6.3.2 *(n)Code Solutions CA* also implements access control and/or security measures such that only authorised *(n)Code Solutions CA* personnel can write or modify the online version of the *(n)Code Solutions CA* publications.

2.6.3.3 **Repositories**

The (n)Code Solutions CA repositories are maintained by the *(n)Code Solutions CA* and are accessible to the authorised personnel. The *(n)Code Solutions CA* repositories are a collection of databases for storing and retrieving certificates and other information related to certificates and contain certificates, CRLs, current and prior versions of the *(n)Code Solutions CA* CPS and other information as prescribed by the *(n)Code Solutions CA* from time to time. The *(n)Code Solutions CA* repositories are updated periodically as specified in this *(n)Code Solutions CA* CPS and as required by the Act. The National Repository of Digital Signature Certificates, hosted by the Controller of Certifying Authorities along with the *(n)Code Solutions CA* repositories are the only approved source for CRLs and certificates issued by (n)Code Solutions CA.

2.7 Compliance Audit

2.7.1 **Frequency of Entity Compliance Audit**

An auditor empanelled by the CCA shall audit the *(n)Code Solutions CA*'s PKI operations annually as per Rule 31 of the Information Technology (Certifying Authorities) Rules, 2000.

2.7.2 **Identity/Qualifications of Auditor**

The auditor, empanelled by the Controller of Certifying Authorities, shall do the audit.

2.7.3 **Auditor's Relationship to Audited Party**

The auditor shall be independent of (n)Code Solutions CA.

2.7.4 **Topics Covered by Audit**

2.7.4.1 Annual audit shall include inter alia,

i. Security policy and planning;
ii. Physical security;

iii. Technology evaluation;

iv. *(n)Code Solutions CA*'s services administration;

v. Relevant CPS;

vi. Compliance to relevant CPS;

vii. Contracts/agreements;

viii. Regulations prescribed by the Controller;

ix. Policy requirements of Information Technology (Certifying Authorities) Rules, 2000.

2.7.4.2 Half yearly audit shall include inter alia,

i. The Security Policy

ii. Physical security

iii. Planning of operation;

2.7.4.3 A quarterly audit shall include inter alia,

i. *(n)Code Solutions CA* repository.

2.7.5 Actions Taken as a Result of Deficiency

If irregularities are found, the *(n)Code Solutions CA* will prepare a report as to the action it will take in response to the audit report. Based on the severity of the irregularities, the *(n)Code Solutions CA* will carry out corrections of problems in a most expeditious manner and in accordance with generally accepted international practice and the Governing Law.

If the *(n)Code Solutions CA* determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the *(n)Code Solutions CA* , a corrective action plan will be developed and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, the *(n)Code Solutions CA* management will evaluate the significance of such issues and determine the appropriate course of action.

2.7.6 Compliance Audit Results

2.7.6.1 The *(n)Code Solutions CA* compliance audit results will not be made public unless required by law. Where appropriate, the method and detail of notification of audit results to the *(n)Code Solutions CA* partners will be defined within respective agreements between the *(n)Code Solutions CA* and the other party.

2.7.6.2 The results of the audit along with the actions taken on the non conformities will be communicated to the Controller of Certifying Authorities within a period of four weeks of the completion of the audit.

2.8 Confidentiality

2.8.1 Types of Information to be Kept Confidential

2.8.1.1 The types of information the *(n)Code Solutions CA* will keep confidential include agreements, transactional records, correspondence and business arrangement with its RA/LRA, and Subscriber. This information is considered sensitive and shall not be disclosed without prior consent of the other respective party, unless required by law.

2.8.1.2 Information pertaining to digital certificate applications, whether approved or rejected shall be kept confidential. Digital Certificate information collected from the Subscriber as part of registration and verification records but not included in the information contained in the Digital Certificate shall also be kept confidential.

2.8.1.3 The Subscriber's private keys are to be kept secret by the Subscriber. Disclosure of these keys by the Subscriber is at Subscriber's own risk.

2.8.1.4 Audit results and information are considered sensitive and will not be disclosed to anyone other than *(n)Code Solutions CA* authorized and trusted personnel and the CCA. This information will not be used for any purpose other than audit purposes or where required by law.

2.8.1.5 Information pertaining to the *(n)Code Solutions CA* operations, contingency plans, and disaster recovery plans and security measures controlling hardware and software used for administering the *(n)Code Solutions CA* PCS infrastructure shall only be disclosed to the *(n)Code Solutions CA* authorized personnel on a need-to-know basis.

2.8.1.6 Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the *(n)Code Solutions CA*'s custody shall be implemented. Confidential information provided by the Subscriber shall not be disclosed to a third party without the Subscribers' consent, unless the information is required to be disclosed under the law or a court order.

2.8.1.7 Data on the usage of the Digital Signature Certificates by the Subscribers and other transactional data relating to the Subscribers' activities generated by the *(n)Code Solutions CA* in the course of its operation, if any, shall be protected to ensure the subscribers' privacy.

2.8.1.8 A secure communication channel between the *(n)Code Solutions CA* and its applicant shall be established to ensure the authenticity, integrity and confidentiality of the exchange of information during Certificate Issuance process.

2.8.2 Types of Information not Considered Confidential

The types of information that are not considered confidential include information contained in Subscriber's Certificate, CRL, the *(n)Code Solutions CA* CPS, list of certificate holders and corporate information that appear in the *(n)Code Solutions CA* web site.

2.8.3 Disclosure of Certificate Revocation Information

2.8.3.1 The *(n)Code Solutions CA* shall publish the Certificate revocation details of all the Certificates revoked by the *(n)Code Solutions CA*. The Certificates revoked / after verification of revocation request by the RA will be added to a CRL that shall be published and updated at the *(n)Code Solutions CA* web site. Revocation of certificates shall be only for due cause.

The reasons for the revocation shall be disclosed only to the subscriber or to the agencies having the power to compel the disclosure.

2.8.4 Release to Law Enforcement Officials

In the event that the *(n)Code Solutions CA* is required under any provision of any rules, regulations or statutory provisions or by any order of court to release any information that is deemed to be or construed to be of a confidential nature under this CPS, the *(n)Code Solutions CA* shall be at liberty to release all such information required by the respective competent authority without any liabilities and any such release shall not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality.

2.8.5 Release as Part of Civil Discovery

In the event that the *(n)Code Solutions CA* is required, pursuant to any suit or legal proceedings initiated by itself or otherwise, under any provision of any rules, regulations or statutory provisions or by any order of court to release any information that is deemed to be or construed to be of a confidential nature under this CPS, the *(n)Code Solutions CA* shall be at liberty to release all such information required to be disclosed under any provision of any said rules, regulations or statutory provisions or by any order of court without any liabilities and any such release shall not be construed as or be deemed to be a breach of any obligations or requirements of confidentiality. The *(n)Code Solutions CA* shall in such case inform the concerned entity for such disclosure made.

2.8.6 Disclosure upon Subscriber's Request

In the event that the owner of any confidential information requests that the *(n)Code Solutions CA* reveal or disclose any confidential information owned by the said owner for any reasons whatsoever, the *(n)Code Solutions CA* shall do so only if it forms the opinion that the release of any such information will not result in the incurrence of any liability on any other party and the *(n)Code Solutions CA* shall not be liable for any damages or losses arising out of any such revelation or disclosure of such confidential information and the owner of the confidential information shall indemnify the *(n)Code Solutions CA* for any and all liabilities, damages, losses or any and all such liabilities arising out of or pursuant to any such revelation or disclosure of such confidential information.

2.8.7 Other Information Release Circumstances

a. The *(n)Code Solutions CA* shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release from the person to whom the *(n)Code Solutions CA* owes a duty to keep such information confidential and

b. the person requesting confidential information (if not the same person); may have a court order. The *(n)Code Solutions CA* may require that the requesting person pay a reasonable fee before disclosing such information.

c. Confidential Information will also be disclosed by the *(n)Code Solutions CA* when ordered to do so by the CCA.

d. Any and all such other information may be released by the *(n)Code Solutions CA* upon such times and under such circumstances as the *(n)Code Solutions CA* management may at the time determine after due approval from CCA.

2.9 Intellectual Property Rights

2.9.1 Subscribers

2.9.1.1 The (n)Code Solutions CA shall comply with Applicant/Subscriber's information protection as per the Act. The information supplied by the Applicant/Subscriber is the property of the respective Applicant/Subscriber. All Applicants/Subscribers shall grant to the (n)Code Solutions CA and the RAs a non-exclusive, world-wide, paid-up, royalty-free license to use, copy, modify, publish and distribute such information subject to Applicant/Subscriber's information protection as per the Act.

2.9.1.2 The *(n)Code Solutions CA* shall grant to the Subscribers and the Relying Parties a non-exclusive, non-transferable license to use, copy and distribute the *(n)Code Solutions CA* Digital Signature Certificates provided that:

a. The Digital Signature Certificates are used as specified in this *(n)Code Solutions CA* CPS, Subscriber Agreement

b. The Digital Signature Certificates are represented fully and accurately.

c. The Digital Signature Certificates are not published in the publicly available databases, Repositories and the directories without the express written permission of the *(n)Code Solutions CA*.

2.9.1.3 The *(n)Code Solutions CA* grants permission to reproduce the *(n)Code Solutions CA* CPS provided,

a. The copyrights notice being retained in all the copies of the *(n)Code Solutions CA* CPS.

b. The *(n)Code Solutions CA* CPS is reproduced fully and accurately.

2.9.2 The *(n)Code Solutions CA* shall retain sole and exclusive ownership of all right, title and/or interest in and to the Certificate and all software supplied by the *(n)Code Solutions CA*. The *(n)Code Solutions CA* shall be entitled to continue using the Certificate and all software supplied in whatever form, manner or model it so elects.

2.9.3 All parties are to acknowledge that any and all of the copyrights, trademarks and other intellectual property rights used or embodied in or in connection with any and all Certificate issued and all software supplied by the *(n)Code Solutions CA* pursuant to this CPS, including all documentation and manuals relating thereto, is and shall remain the property of the *(n)Code Solutions CA* and the parties shall not during or at any time after the revocation or expiry of any of their Certificate, in any way question or dispute the ownership or any other such rights of the *(n)Code Solutions CA*.

2.9.4 The parties also acknowledges that such trademarks, copyrights and other rights in the Certificate belongs to the *(n)Code Solutions CA* and/or that the *(n)Code Solutions CA* has the authority to use all such trademarks, copyrights and all such other rights and shall not be used by the parties unless with the express written consent of the *(n)Code Solutions CA* and under the prescribed format in the *(n)Code Solutions CA* brand management document. Upon the termination, revocation, or expiry of any Certificate, the parties shall forthwith discontinue such use, without receipt of compensation for such discontinuation and the parties shall deliver unto the *(n)Code Solutions CA* any and all copies of the Certificate and software supplied by the *(n)Code Solutions CA* that it has in its possession or shall at the request of the *(n)Code Solutions CA* destroy any and all copies of the Certificate and software supplied by the *(n)Code Solutions CA* that it has in its possession and shall render the *(n)Code Solutions CA* a certification that the parties has duly done so.

3. IDENTIFICATION AND AUTHENTICATION

This section describes the registration, renewal and revocation procedures associated with *(n)Code Solutions CA* Digital Certificate processes. This procedure and the norms under this document are in accordance with the Indian Information Technology Act, 2000 read with Information Technology (Certifying Authority) Rules, 2000 and the Information Technology (Certifying Authorities) Regulations, 2001

3.1 Initial Registration

3.1.1 Types of Names

3.1.1.1 Each Subscriber will be represented by a clearly distinguishable and unique X.509 V3 Distinguished Name (DN) in the Certificate subject name field and in accordance with PKIX Part 1.

3.1.1.2 Each Entity may use an alternative name via the Subject Alternate Name field, which will be in accordance with PKIX Part 1.

3.1.1.3 The DN may be in the form of a printable string or in such other form but will not be blank.

3.1.2 Need for Names to be Meaningful

3.1.2.1 The ‘Subject name’ field in the Digital Certificate must be associated with the name of the Subscriber.

3.1.2.2 In the case of individuals, Relative Common Name (DN) should be a combination of first name, surname, and optionally any other identifiable information.

3.1.2.3 This DN may also include an organizational position or role.

3.1.2.4 In the case of other entities the DN shall reflect the authenticated legal name of the Subscriber.

3.1.2.5 If a Certificate refers to a role or position, the Certificate may also contain the identity of the person who holds that role or position.

3.1.3 Rules for Interpreting Various Name Forms

The distinguished names will include the following details:

- CN = Common name that is unique for every subscriber
- Serial Number = Reference number
- OU = Organisational units distinguished within an Organisation
- OU = Company
- OU = Certificate Class
- O = Organisation = Entity Name
- C = Country = IN (As per CCA guidelines)

3.1.4 Uniqueness of Names

DN must be unique for all Subscribers of the *(n)Code Solutions CA*. The *(n)Code Solutions CA* adopts the Unique Identifier such that Subscribers with identical names can be supported in the *(n)Code Solutions CA*.

3.1.5 Name Claim Dispute Resolution Procedure

In the event of any disputes concerning name claim issues, the *(n)Code Solutions CA* reserves the right to make all decisions and shall be the final arbiter of all such claims in relation to Subscriber names in all assigned Certificates. A party requesting a Certificate must demonstrate its right to use a particular name. The *(n)Code Solutions CA* will have the right to reject any name at its sole and absolute discretion.

3.1.6 Recognition, Authentication and Role of Trademarks

The use of trademarks will be reserved to registered trademark holders and proper documentary proof of such ownership must be produced to the *(n)Code Solutions CA*.

3.1.7 Method to prove possession of Subscriber's Private Key

The *(n)Code Solutions CA* provides Set-up Information to the applicant at the initial stage of registration. This Setup Information is subsequently used by the applicant to confirm with the *(n)Code Solutions CA* that the applicant is the rightful owner of the private key(s). The Setup Information is distributed to the applicant securely.

3.1.8 Authentication of Organization Identity

3.1.8.1 An application for an organization subscriber must be made by an individual authorized to act on behalf of the prospective Subscriber. The *(n)Code Solutions CA* or the applicable LRA will perform the necessary verification of the Subscriber as per the class of certificate applied for.

3.1.8.2 Identification and authentication of the prospective Subscriber must be through one of the following means —

The *(n)Code Solutions CA* or the LRA must examine copies of documentation, duly certified by such persons recognised by the *(n)Code Solutions CA*, providing evidence of the existence of the individual/server/any other entity or organisation.

3.1.8.3 The *(n)Code Solutions CA* or the LRA will also verify the identity and authority, including any and all letters of authorisation, of the individual acting on behalf of the prospective Subscriber and their authority to generate keys and receive certificate on behalf of that organisation.

3.1.8.4 The *(n)Code Solutions CA* or the LRA will keep a record of the Subscriber's information as detailed in the Subscriber's application form.

3.1.9 **Authentication of Individual/ Company or Organization /Government Organization or Agency Identity**

3.1.9.1 The process of identification of a Subscriber will differ based on the class of Certificate that the Subscriber is applying for and may include any or all of the following:- verification of e-mail, postal address, face to face authentication and verification of stipulated documents. An application for a Certificate must be made (i) personally by an individual or, (ii) by the duly authorised representative of the Subscriber. Additional identification in the form of Authority letter from the employer company will be required, where the certificate is intended to be used for Web form signing, User authentication ,Code signing, VPN client purposes or for securing servers and VPN devices. For identifying organisations, details like registration details, Income Tax records/ Annual reports / bank details will be required. For Class IIIc Certificates, Domain name shall be identified based on documentary proof from the relevant Registrar of Domains. Similarly for Class IIId certificates for VPN devices, the proof of ownership of the VPN device shall be obtained from the certificate applicant.

3.1.9.2 E-mail validation, identification and authentication of the individual / Organizational or Government Organization applicant will be done by checking and verifying that the e-mail address of the applicant does in fact exist and the applicant is able to access the information sent through e-mail.

3.1.9.3 Address verification will be done by sending a letter by courier or registered post to the address mentioned in the applicant’s certificate application form and/or by sending an agent personally to verify the address.

3.1.9.4 The physical (personal) identification and authentication of the individual / Organizational or Government Organization applicant including agent of any other entity must be through the following means —

THE LRA will verify the identity of the individual / Organizational or Government Organization applicant with the identification document (attested / certified photocopies). Identification document must be a government- issued identification.

3.2 Routine Rekey

3.2.1 Subscribers will need to re-apply after the expiration of existing certificate. Subscribers shall generate a new private- public key pair on a trustworthy medium and complete the initial registration process once again.

3.2.2 The corresponding RA may put reasonable efforts to inform the subscriber in advance about the expiration of the Subscriber's Certificate.

3.2.3 Key pair comprising of public and private key pair of the *(n)Code Solutions CA* shall be changed at the expiry of five years from the date of generation in accordance with Regulation 4(1)(i)(2) of the Information Technology (Certifying Authority) Regulations, 2001. Subsequent to the key change over by the *(n)Code Solutions CA*, new digital certificates shall be issued to the existing subscribers at that time for the balance period of their subscription.

3.3 Renewal after Revocation

In the event of any suspected key compromise, the Certificate issued must be revoked. It is the responsibility of that Subscriber or person authorised by the Subscriber to notify the *(n)Code Solutions CA* or the relevant RA who issued the Certificate immediately upon such suspicion. The process of renewals carried out by the *(n)Code Solutions CA* or the relevant RA after such revocation will be in the same manner as the process of initial registration. Any change in any information contained in a Certificate will have to be re-certified by the *(n)Code Solutions CA* or the relevant RA before any Certificate is issued. All charges as per the Fee Schedule prevalent at the time of renewal will be applicable in such cases.

3.4 Revocation Request

3.4.1 The *(n)Code Solutions CA* or its RA will verify any request for revocation for a Certificate. Revocation requests received by the LRA shall be forwarded to (n)Code Solutions CA for further processing. The procedures for processing any revocation request and the means by which its validity is established are stipulated in Section 4.4

3.4.2 The *(n)Code Solutions CA* or its RA will log all revocation requests as the case may be.

4. OPERATIONAL REQUIREMENTS

This section describes the certificate application, issuance, validation, and acceptance process.

4.1 Certificate Application

4.1.1 Classes of Certificate

The *(n)Code Solutions CA* is offering following classes of certificates

Class	Category	Suggested Use
I	Individual	(a) Secure E-Mail
IIa	Individual	(a) Web Form Signing (b) User Authentication (c) Other low Risk Transactions (d) Secure E-Mail
IIb	Enterprises/ Government Organizations or Agencies	(a) Web Form Signing (b) User Authentication (c) Other low Risk Transactions (d) Secure E-Mail
IIIa	Individual	(a) VPN User (b) Code Signing (c) Web Form Signing (d) User Authentication (e) Secure E-Mail
IIIb	Enterprises/ Government Organizations or Agencies	(a) VPN User (b) Code Signing (c) Web Form Signing (d) User Authentication (e) Secure E-Mail
IIIc	Individual / Enterprises/ Government Organizations or Agencies	(a) SSL Server Authentication
IIId	Individual / Enterprises/ Government Organizations or Agencies	(a) VPN Device Authentication

Table 4.1 – Suggested usages of various classes of certificates

“The *(n)Code Solutions CA* currently supports the above listed seven (7) distinct classes within its Certification Practice Statement.” ALL THE CLASSES OF CERTIFICATE OFFERED FOR SPECIFICATION BY THE *(n)Code Solutions CA* ARE VALID UNDER THE INFORMATION TECHNOLOGY ACT, 2000. Each class provides for a designated level of trust. The following sub-sections describe and qualify the features of each class in continuation of the features mentioned in the preceding table.

THE DESCRIPTIONS FOR EACH CERTIFICATE CLASS 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 THE *(n)Code Solutions CA* 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.

4.1.1.1 **Class I Certificates**

Class I certificates are issued to individuals only and can be used for secure email. Class I certificates provide a lower level of assurance when compared with other certificates issued by *(n)Code Solutions CA.*

4.1.1.2 **Class II Certificates**

a. **Class IIa Certificates:**

Only individuals are eligible for application and issuance of Class IIa certificates. They are typically used for web form signing, user authentication and other low risk transactions. They can also be used to secure e-mail.

Class IIa certificates do not require physical presence of the applicant individual and hence provide a lower assurance of the identity of the subscriber when compared with Class IIIa certificates. They represent a simple validation of unique DN, operational email address, validation of postal address and verification of attested copies of the stipulated documents. A photograph is also required for all Class IIa certificate applicants.

b. **Class IIb Certificates:**

Only applicants representing an Organization / Government Organization or Agency are eligible for application and issuance of a Class IIb certificate. Like Class IIa, these certificates are also used for web form signing, user authentication, low risk transactions and secure e-mail.

Class IIb certificates do not require verification of the physical presence of the applicant representing the Organization/ Government Organization or Agency. They provide limited assurance of the identity of the subscriber when compared with Class IIIb certificates. They represent a simple validation of unique DN, operational email address, validation of postal address and verification of attested copies of the stipulated documents confirming the existence of the Organization / Government Organization or Agency. A photograph is also required for all Class IIb certificate applicants.

THESE CERTIFICATES PROVIDE A HIGHER LEVEL OF ASSURANCE WHEN COMPARED WITH CLASS I CERTIFICATES. THEY ARE NOT INTENDED FOR HIGH VALUE COMMERCIAL TRANSACTIONS WHERE PROOF OF IDENTITY IS REQUIRED AND SHOULD NOT BE RELIED UPON FOR SUCH USES.

4.1.1.3 Class IIIa Certificates

Only individuals are eligible for application and issuance of Class IIIa certificates. Every issued Class IIIa certificate confirms that the Subscriber's postal address is valid and the e-mail address given by the subscriber does exist and subscriber is able to access and operate given e-mail identification. Class IIIa certificates further require attested copies of the stipulated documents and the photograph of the applicant. Class IIIa certificates also require the applicant Individual to appear personally before the stipulated LRA. The general usage of Class IIIa certificates is primarily for single sign on applications, code signing or authentication for VPN client, web form signing and user authentication. They can also be used for secure e –mail.

4.1.1.4 Class IIIb Certificates

Class IIIb certificates are issued to firms, companies, corporate bodies, Government Organizations/ Agencies.

Class IIIb certificates can provide assurances of the existence and name of various organisations (such as Public and Private limited Companies, Partnership Firms, Proprietorship Firms and Government Organizations / Agencies). Validation of Class IIIb certificate applications for corporate organisations includes verification of the registration details of the company / enterprise and verification of the Income Tax records / Annual reports / Balance Sheets/ Bank details. Validation of Class IIIb certificates in case of Government Organization or Agency constitutes verification of the attested identity proof submitted by the applicant of the Government Organization/ Agency.

Validation of Class IIIb certificate applications also include verification of the applicant's identity authorization to act on behalf of the Enterprise / Government Organization or Agency to obtain and use a Class IIIb Digital Certificate.. Class IIIb certificates also require the authorized applicant from the organization to appear personally before the stipulated LRA for verification of physical presence. Class IIIb certificates are used by Subscribers primarily for code signing, VPN user, web form signing and user authentication applications. They can also be used for secure e-mail.

4.1.1.5 Class IIIc Certificates

Class IIIc certificates are issued to Individuals, Enterprises, corporate bodies, Government Organizations / Agencies for the web server category

Class IIIc certificates can provide assurances for the domain name of a Registered domain. Class IIIc certificates are used by the *(n)Code Solutions CA* subscribers primarily for SSL server authentication.

4.1.1.6 Class IIId Certificates

Class IIId certificates are issued to Individuals, Enterprises, corporate bodies, Government Organizations/ Agencies for VPN devices.

Class IIId certificates ensure security of communication between two VPN devices. These certificate also enables secure login by users having Digital Certificate.

CLASS III CERTIFICATES PROVIDE THE HIGHEST LEVEL OF ASSURANCE IN THE INDIVIDUAL/ ENTERPRISE/ GOVERNMENT ORGANIZATION OR AGENCY SUBSCRIBER CATEGORY, AS THEY ALSO REQUIRE PHYSICAL PRESENCE OF AN INDIVIDUAL/ AUTHORIZED INDIVIDUAL FROM THE ORGANIZATION. THE DECISION TO OBTAIN, USE, OR RELY UPON CLASS III CERTIFICATES SHOULD TAKE INTO ACCOUNT THEIR RELATIVE BENEFITS AND LIMITATIONS, AND THE CERTIFICATES SHOULD BE USED ACCORDINGLY.

4.1.2 Certificate Application Process

4.1.2.1 Applicant will access the *(n)Code Solutions CA* website at **www.ncodesolutions.com** to select customer type and class of certificate and shall also accept the Subscriber Agreement by confirming acceptance on the relevant web page on the *(n)Code Solutions CA* website.

4.1.2.2 Applicant will be taken to online registration form complying with the Information Technology (Certifying Authorities) Rules, 2000, Schedule IV and as per the changes communicated by the CCA through Notifications in the Official Gazette / establishment of new Guidelines

4.1.2.3 Applicant will fill the online form and choose a pass phrase for later authentication.

4.1.2.4 After due verification of mandatory fields, Applicant will be given an opportunity to confirm the given details. Applicant will also print the displayed form to hand sign and send it across to the *(n)Code Solutions CA*. Alternatively, applicant can download the blank application form from the *(n)Code Solutions CA* website and courier / hand deliver the duly filled up and signed form.

4.1.2.5 Applicant will be shown the list of documents required with reference to the category and the class of certificate chosen. If the class of certificate chosen requires physical presence, then the time period for physical presence will also be displayed.

4.1.2.6 Applicant will also be provided with payment details.

4.1.2.7 For bulk registrations, the *(n)Code Solutions CA* will follow below mentioned process:

a. Bulk registration requests will be accepted for class IIb and IIIb only.

b. Company / Government Organization or Agency seeking bulk registration, will submit soft copy of the bulk registration form to the *(n)Code Solutions CA* along with the authentication data for each subscriber.

4.1.3. **Certificate Application Form**

Information Technology (Certifying Authority) Rules, 2000 has prescribed the Application forms for different categories of Subscribers. The *(n)Code Solutions CA* application form is in compliance with the Information Technology (Certifying Authority) Rules, 2000 and the changes communicated by the CCA through Notifications in the Official Gazette / establishment of new Guidelines. The *(n)Code Solutions CA* Certificate Application Form is available at various *(n)Code Solutions CA* offices as well as on the *(n)Code Solutions CA* website at www.ncodesolutions.com.

4.2 Certificate Issuance

4.2.1 Certificate issuance process involves verification and validation checks to establish identity and other information acquired through the application form for the applicant. The *(n)Code Solutions CA* has varied requirements for documents as well as other checks for different classes of certificates.

4.2.2 **Certificate Issuance Process**

4.2.2.1 Applicant will receive an email on the email address provided in the application form with a link for email id verification.

4.2.2.2 Applicant will also post / courier / hand deliver the documents with reference to the class of certificate requested to the relevant *(n)Code Solutions* LRA. Following table describes the documents and physical presence stipulations:

Class of Certificate	Verification documents required
Class I (Individuals)	a. Copy of any one: • Passport or • Driving license or • Voters ID or • PAN Card or • PF Statement/PF Book or • Ration Card
Class IIa	a. Attested* Copy of any one:

(Individuals)	• Passport or • Driving license or • Voters ID or • PAN Card or • PF Statement/PF Book or • Ration Card b. Attested* Copy as address proof of any one: • Latest telephone bill (landline or mobile) or • Latest electricity bill or • LIC receipt (if LIC policy is taken by applicant) c. Latest photograph of the applicant
Class IIb (Organizations)	Documents required with each Digital Certificate Application : a. Authorization Letter in favour of the certificate applicant from the applicant organization (as per the format attached with the application form) b. Latest photograph of the applicant Documents required only once for an Organization / Enterprise: c. Certified true copy (from Company Secretary / a Director / Partner of the organization) of any one: • Certificate of Incorporation or • Memorandum and Articles of Association or • Registered Partnership Deed or • Valid business license document d. Certified true copy of any one: • Annual Report or • Income Tax Return or • Statement of Income or • Bank details of the organization
Class IIb (Govt. Orgn. / Agency)	a. Attested * Copy of any one: • ID Card having Employee Identification No. or • Passport or • Driving License or • Voter's ID or • PAN Card or • PF Statement / PF Book or • Ration Card b. Authorization Letter in favour of the certificate applicant from the Govt. organization (as per the format attached with the application form) c. Latest photograph of the applicant
Class IIIa (Individuals)	a. Attested* Copy of any one: • Passport or

	• Driving license or • Voters ID or • PAN Card or • PF Statement/PF Book or • Ration Card b. Latest Photograph of the applicant c. Attested* Copy as address proof of any one: • Latest telephone bill (landline or mobile) or • Latest electricity bill or • LIC receipt (if LIC policy is taken by applicant d. *Verification of physical presence*
Class IIIb (Organizations)	Documents required with each Digital Certificate Application : a. Authorization Letter in favour of the certificate applicant from the applicant organization (as per the format attached with the application form) b. Latest photograph of the applicant c. *Verification of physical presence* Documents required only once for an Organization / Enterprise: d. Certified true copy (from Company Secretary / a Director / Partner of the organization) of any one: • Certificate of Incorporation or • Memorandum and Articles of Association or • Registered Partnership Deed or • Valid business license document e. Certified true copy of any one: • Annual Report or • Income Tax Return or • Statement of Income or • Bank details of the organization
Class IIIb (Govt. Orgn./ Agency)	a. Attested * Copy of any one: • ID Card having Employee Identification No. or • Passport or • Driving License or • Voter's ID or • PAN Card or • PF Statement / PF Book or • Ration Card b. Authorization Letter in favour of the certificate applicant from the Govt.

	organization (as per the format attached with the application form) c. Latest photograph of the applicant. d. *Verification of physical presence*
Class III c (Individuals)	a. Attested* copy of address proof of any one: • Latest telephone bill (landline or mobile) or • Latest electricity bill or • LIC receipt (if LIC policy is taken by applicant) b. Latest Photograph of the applicant. c. Domain Name Registration proof from the Registrar of Domains. d. Attested* copy of latest Income Tax return of the applicant. *e. Verification of physical presence*
Class IIIc (Organizations)	Documents required with each Digital Certificate Application : a. Authorization Letter in favour of the certificate applicant from the applicant organization (as per the format attached herewith) b. Latest photograph of the applicant c. Domain Name Registration proof from the Registrar of Domains. d. *Verification of physical presence.* Documents required only once for an Organization / Enterprise: e. Certified true copy (from Company Secretary / a Director / Partner of the organization) of any one: • Certificate of Incorporation or • Memorandum and Articles of Association or • Registered Partnership Deed or • Valid business license document f. Certified true copy of any one: • Annual Report or • Income Tax Return or • Statement of Income or • Bank details of the organization
Class IIIc (Govt. Orgn./ Agency)	a. Attested * Copy of any one: • ID Card having Employee Identification No. or • Passport or • Driving License or • Voter's ID or • PAN Card or

	• PF Statement / PF Book or • Ration Card b. Authorization Letter in favour of the certificate applicant from the Govt. organization (as per the format attached with the application form) c. Latest photograph of the applicant. d. *Verification of physical presence* e. Domain Name Registration proof from the Registrar of Domains.
Class IIId (Individuals/ Enterprise / Govt. Deptt. or agency)	Same documents are that of Class IIIc certificates for Individuals / Enterprises and Govt. Organizations or Agencies. The only difference is that instead of ' Domain Registration Proof' a 'Device Ownership Proof ' is asked for.

Table 4.2 – Stipulated documents for various classes of certificates

Wherever the term 'attested' is mentioned in the table above, attestation may be by a Bank Manager of a Nationalized or Private bank (excluding Cooperative banks) or a Public Notary or a Class I Gazetted Officer.

** In case of bulk certificates for Companies / Government Organizations or Agencies, only one set of company details pertaining to registration will be collected annually instead of with every application.

4.2.2.3 After email verification / receipt of documents as above / physical appearance, if required and payment of stipulated fees, a set of authentication codes will be delivered to the address provided in the application form. In case of class I certificates authentication codes will be communicated via email. In case of all other classes, authentication codes will be printed and delivered by regular mail while the URL and the Reference code will be sent by e-mail. Later on, the subscriber will use these codes for issuance of certificate. Along with the authentication codes a URL for certificate download and acceptance will also be communicated.

4.2.2.4 Subscriber will be informed his unique Customer ID in the e-mail containing the Reference Code.

4.2.2.5 A period of maximum one month would be given to the applicant for the completion of the above verification process, failing which the (n)Code Solutions CA may decide to reject the application.

4.2.2.6 Applicants will be presented the contents of the certificate for verification at the time of completing the Registration process , before the same is issued. Only after due verification and acceptance of the information given in the certificate by the applicant would the certificate be issued. Also *(n)Code*

Solutions CA shall take care to ensure that the name of the certificate applicant does not appear in its list of compromised users before issuing a Digital Certificate.

4.2.2.7 For bulk registrations, the *(n)Code Solutions CA* will follow below mentioned guidelines:

a. Responsibility for the verification of above-mentioned documents will be with the LRA appointed by the company applying for bulk registration.

b. The *(n)Code Solutions CA* will communicate URL, user ID and password to the LRA of the applicant company for accessing the activation codes (ref code and auth codes) for applicants from the CA software. For each bulk registration process, a new username and password shall be created to access the activation codes.

4.2.3 **Table below describes certain properties of each certificate class.**

	Summary Of Confirmation Of Identity
Class I	Confirmation of a unique DN, Verification of Operational email address, Unattested identity proof on record.
Class IIa	Confirmation of a unique DN, Verification of Operational email address and postal address, Attested identity proof , photograph and address proof on record.
Class IIb	For Organizations: Confirmation of a unique DN, Verification of Operational email address and postal address of the applicant. Identity verification from registration details / partnership deed etc, and Income Tax Records/ Annual Report/ Balance Sheet/ Bank Details. Identity and authority confirmation by photograph and relevant authorization from the organization, For Government Organizations/ Agencies: Confirmation of a unique DN, Verification of Operational email address and postal address of the applicant. Attested identity proof, photograph and Authorization Letter for the applicant on record.
Class IIIa	Confirmation of a unique DN, Verification of Operational email address and postal address, Attested identity proof , address proof and latest photograph on record along with physical appearance by the applicant.

Class IIIb	For Organizations: Confirmation of a unique DN, Verification of Operational email address and postal address of the applicant. Identity verification from Registration details / Partnership deed etc. and Income Tax Records/ Annual Report/ Balance Sheet/ Bank Details . Identity and authority confirmation by relevant authorization from the organization, latest photograph of the applicant on record and physical appearance of the applicant representing the organization. For Government Organization / Agency : Authority verification from the Authorization letter of the Authorized signatory of the Government Organization/Agency, latest photograph of the applicant representing the organization on record. Identity verification from the attested identity proof submitted by the applicant and physical appearance of the applicant representing the organization.
Class IIIc	For Individuals : Verification of the domain ownership /registration documents, identity verification from the Income Tax Records and postal address proof .Latest photograph of the applicant. on record along with physical appearance. For Organizations: Verification of the domain ownership / registration documents, identity verification through registration documents/ partnership deed/ other valid business license documents as applicable. Identity verification from the Annual Report/ Balance Sheet/ Income Tax Return/ Bank Details. Identity and authority confirmation by relevant authorization from the organization, latest photograph of the applicant and physical appearance of the applicant representing the organization. For Government Organization / Agency: Verification of the domain ownership / registration documents. Identity and authority verification from the Authority letter of the Authorized signatory of the Government Organization/Agency and the attested identity proof submitted, latest photograph of the applicant and physical appearance of the applicant representing the organization.
Class IIId	For Individuals: Verification of the VPN device ownership proof (in the name of the applicant), identity verification from the Income Tax Records and postal address proof .Latest photograph of the applicant on record along with physical appearance.

	For Organizations: Verification of the VPN device ownership proof (in the name of the applicant), identity verification through registration documents/ partnership deed/ other valid business license documents as applicable. Identity verification from the Annual Report/ Balance Sheet/ Income Tax Return/ Bank Details. Identity and authority confirmation by relevant authorization from the organization, latest photograph of the applicant and physical appearance of the applicant representing the organization. For Government Organization /Agency: Verification of the VPN device ownership proof (in the name of the applicant). Identity and authority verification from the Authority letter of the Authorized signatory of the Government Organization/Agency and the attested identity proof submitted. Latest photograph of the applicant and physical appearance of the applicant representing the organization.

Table 4.2.3 – Identification and Authentication for various Certificate classes

Each class of certificate is characterized by a different level of the properties such as confirmation of identity (such as through personal presence). While the certificates (and the *(n)Code Solutions CA*'s supporting products and services) possess many other properties, those listed in above table provide a framework for distinguishing some of their aspects that affect their relative trust.

4.2.4 The *(n)Code Solutions CA* suggests the use of an Internet browser preferably the Microsoft Internet Explorer, version 5 and later for the generation of the signing key pair. This recommended browser generates the Subscriber's signing key pair at Subscriber's end and sends public verification key to the *(n)Code Solutions CA* for certification. This is communicated via the secured Internet connection by using Secure Socket Layer (SSL protocol) with 128 bit encryption [(n)Code Solutions CA's web certificate will be used for this].

The *(n)Code Solutions CA* validates the authenticity of the certification request. Upon validation it, creates the Subscriber's Certificate. The *(n)Code Solutions CA* reserves the right to accept or reject the application as a result of verification process.

4.2.5 Validation Requirements for Certificate Applications

Upon receipt of a certificate application the CA/LRA shall confirm that:

(a) The certificate applicant has accepted the terms and conditions of the Subscriber Agreement. The Subscriber shall do so by confirming acceptance on the relevant web page on the *(n)Code Solutions CA* website.

(b) The registration form is filled completely, payment for certification services and reply to e-mail confirmation has been received.

(c) The certificate applicant and the person identified in the request are the same.(in accordance with and only to the extent provided in the certificate class descriptions),

(d) The certificate applicant's name does not appear in the (n)Code Solutions CA's list of compromised users.

(e) The certificate applicant generates his key pair and is in possession of the private key corresponding to the public key to be listed in the certificate.

(f) The applicant confirms that the verified information to be listed in the certificate is accurate , refers to the URL communicated to him, enters the activation codes (ref. code and auth. code) provided to him and downloads the certificate. Certificate download constitutes acceptance of the certificate and the certificate is considered issued for publication in the repository.

(g) The *(n)Code Solutions CA* /LRA have no responsibility to monitor and investigate the accuracy of the information in a certificate after its issuance.

The validation requirements for each certificate class are different and are unique for that specific class. To continuously improve and strengthen the validation process, the *(n)Code Solutions CA* reserves the right to add and/or modify the validation procedures.

4.2.6 **Summary of the Validation requirements:**

Validation Requirements	**Class I**	**Class IIa**	**Class IIb**	**Class IIIa**	**Class IIIb**	**Class IIIc**	**Class IIId**
Physical Presence before the *(n)Code Solutions CA* authorised representative	No	No	No	Yes	Yes	Yes	Yes
Postal Address Confirmation	No	Yes	Yes	Yes	Yes	Yes	Yes
E-Mail Address Confirmation	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 4.2.6 (Validation Requirements for Certificate Applications)

4.2.6.1 Physical Presence Verification

For strengthening the authentication process and providing high level of assurance and trust, applicants applying for Class IIIa, IIIb,IIIc and IIId certificates must appear personally before an LRA to facilitate the confirmation of their identity.

4.2.6.2 Postal Address Confirmation

The *(n)Code Solutions CA* shall send through registered post or courier a letter to the applicant confirming the postal address submitted in the certificate application. This confirmation procedure further substantiates evidence that the subscriber's address matches the address listed in the certificate application and therefore provides further assurance on the identity of the subscriber. The confirmation letter contains Authorisation Codes & URL that must be used to complete the certificate application process.

4.2.6.3 Email Address confirmation

The *(n)Code Solutions CA* shall send an email at the email address given in the application form. The e-mail shall contain a URL, by accessing which the applicant can verify his email address. This shall validate that the email address provided in the application form is operational and the applicant is able to access the same.

4.2.7 Approval of Certificate Applications

Upon successful performance of all required validations specified in the Class of certificate application (in accordance with CPS Section 4.2), the *(n)Code Solutions* CA shall approve the application. Approval is demonstrated by issuing a Digital Certificate according to CPS Section 4.3.

4.2.8 Rejection of Certificate Application

The *(n)Code Solutions CA* reserves the right to reject the certificate application in cases where details of the applicant fail a validation check. The applicant will be notified regarding the same through e-mail by being provided the reason code (except where prohibited by law) for such failure. An opportunity to be heard shall be provided to the applicant in cases of validation failure caused as a result of third-party services. A person whose certificate application has been rejected may thereafter reapply.

4.2.9 *(n)Code Solutions CA*'s Representations to Subscriber

4.2.9.1 The *(n)Code Solutions CA* warrants to the subscriber named in the certificate that unless otherwise expressly provided in this CPS or mutually agreed upon by both the *(n)Code Solutions CA* and the subscriber in an agreement –

a. It has complied with the provisions of the IT Act 2000 and the Rules and Regulations made there under.

b. The information contained in the Digital Signature Certificate is accurate.

c. No misrepresentations of fact in the certificate known to the *(n)Code Solutions CA* or originating from the *(n)Code Solutions CA* have been made at the time of certificate issuance.

d. Reasonable care has been taken in creation of certificate using uniform and fail-safe procedures, and

e. All requirements of this CPS and any amendments made thereto are complied with by the *(n)Code Solutions CA*. The certificate and the *(n)Code Solutions CA* PCS complies with requirements of the Information Technology Act, 2000.

f. The *(n)Code Solutions CA* has published the Digital Signature Certificate or otherwise made it available to such person relying on it and the Subscriber has accepted it.

g. The Subscriber holds the private key corresponding to the public key, listed in the Digital Signature Certificate.

h. The Subscriber's public key and private key constitute a functioning key pair.

i. The *(n)Code Solutions CA* has no knowledge of any material fact, which if it had been included in the Digital Signature Certificate would adversely affect the reliability of the above-mentioned representations.

4.2.9.2 The *(n)Code Solutions CA* warrants to the subscriber that reasonable efforts shall be made to promptly revoke certificates in accordance with CPS, on intimation from the subscriber or information of compromise of private key and to notify subscribers of any facts known to it that materially affect the validity and reliability of the certificate it issued to such subscriber.

4.2.9.3 No party other than subscriber can enforce the obligations and representations in CPS Section 2.1.1 and 2.1.2 on the *(n)Code Solutions CA*. The same are solely for the benefit of the subscriber.

4.2.10 ***(n)Code Solutions CA*'s Representations to Relying Parties**

The *(n)Code Solutions CA* warrants to all who reasonably rely on a digital signature verifiable by the public key listed in the certificate that it is consistent with this CPS:

The accuracy of verified information in or incorporated by reference within the certificate is assured, and

The *(n)Code Solutions CA* has complied with the CPS and Information Technology Act, 2000 when issuing the Certificate.

4.2.11 ***(n)Code Solutions CA*'s Representations upon Publication**

The *(n)Code Solutions CA* warrants to Relying Parties that the Certificate is published in the *(n)Code Solutions CA* Repository only after completion of certificate issuance procedures and the acceptance of the Certificate by the Subscriber.

4.2.12 **Limitations on the *(n)Code Solutions CA* Representations**

The above-referred warranties are subject to disclaimers of warranty and limitations of liability mentioned in this CPS .

THE *(n)Code Solutions CA* (OR THE APPLICABLE RA/LRA) DISCLAIMS ANY RESPONSIBILITY FOR PROTECTION OF PRIVATE KEYS OF THE CERTIFICATE APPLICANT. THE CERTIFICATE APPLICANT (AND, UPON APPROVAL, THE SUBSCRIBER) ACKNOWLEDGES THAT SUCH PERSON IS EXCLUSIVELY ALONGWITH ANY AGENT OR REPRESENTATIVE WHERE APPLICABLE RESPONSIBLE FOR PROTECTING HIS, HER, OR ITS PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORISED USE.

THE *(n)Code Solutions CA* EXPRESSLY PROHIBITS ANY USER, CERTIFICATE APPLICANT, SUBSCRIBER, RELYING PARTY, RA, LRA OR ANY OTHER PARTY TO MONITOR, INTERFERE WITH, OR REVERSE ENGINEER THE TECHNICAL IMPLEMENTATION OF THE *(n)Code Solutions CA* PCS EXCEPT AS EXPLICITLY PERMITTED BY THIS CPS OR UPON PRIOR WRITTEN APPROVAL FROM THE *(n)Code Solutions CA*. ANY ACT IN CONTRAVENTION OF ABOVE WILL BE SUBJECT TO PUNITIVE ACTION UNDER THE INDIAN LAWS

4.2.13 Right to Investigate Compromises

The *(n)Code Solutions CA* may, but is not obligated to, investigate all compromises to the furthest extent of the law. By submitting a certificate application (see Section 4.1), 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 *(n)Code Solutions CA* deems appropriate and consistent with the CPS, provided that such investigations comply with all applicable privacy and data protection laws of the Republic of India. Investigations of the *(n)Code Solutions CA* 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.

4.2.14 Certificate Validity & Operational Periods

Successful downloading of the certificate by the subscriber shall mark the beginning of the validity period of all certificates. The lifetime of the certificates will be as follows:

Class	Life
I	1 year / 2 years
IIa	1 year / 2 years
IIb	1 year / 2 years
IIIa	1 year / 2 years
IIIb	1 year / 2 years
IIIc	1 year / 2 years
IIId	1 year / 2 years

4.3 Certificate Download and Acceptance

4.3.1 Once a subscriber has completed certificate Application and Issuance procedures, certificate download and acceptance procedures are the final steps towards getting a Digital Signature Certificate.

4.3.2 **Certificate Download and Acceptance Process**

4.3.2.1 Applicants will access the URL communicated to them.

4.3.2.2 Applicants will provide pass phrase and will be redirected to certificate download URL on verification.

4.3.2.3 Class I, IIa, IIb, IIIa and IIIb applicants will provide the authentication codes provided to them by *(n)Code Solutions CA* in the URL for certificate download

4.3.2.4 Class IIIc Applicants will provide CSR (Certificate Signing Request) generated from the web server, along with the authentication codes provided by *(n)Code Solutions CA* in the URL for certificate download.

4.3.2.5 Class IIId Applicants will provide CSR (Certificate Signing Request) generated from the VPN device, along with the authentication codes provided by *(n)Code Solutions CA* in the URL for certificate download.

4.3.2.6 After validating the authentication codes, subscribers for class I, IIa, IIb, IIIa and IIIb certificates will download the requested certificate in the certificate store of their machine/smart cards/tokens through a secure channel. Class IIIc and Class IIId Applicants will download the certificate to their web server / VPN device respectively.

4.3.2.7 For bulk registrations, the *(n)Code Solutions CA* will follow below mentioned guidelines:

a. Applicants will access the communicated URL and will provide user ID, password and email address.

b. Subsequent to the validation of User ID and password, certificate will be downloaded to the certificate store of the user machine/smart card/token through a secure channel.

4.3.3 **Certificate Acceptance**

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

4.4 Certificate Suspension and Revocation

Suspension is the process of making a certificate invalid temporarily, pending certain investigations. In such situations, *(n)Code Solutions CA* revokes the certificate as suspension of certificates is not supported by *(n)Code Solutions CA*. Revocation is the process of making a certificate invalid permanently. The revoked certificates cannot be reused and are listed in the CRL. The revocation process for a Subscriber's certificate can be achieved in two ways:

1. Subscriber revocation request through hand delivery or courier (This manual revocation is useful, when private key is not under the possession of the subscriber).
2. Online Subscriber Certificate Revocation Request Process (This process can be used only when the private key is under possession of the subscriber, and when the Subscriber wants to revoke the certificate due to any key compromise or any other reason).

4.4.1 **Circumstances for Revocation**

4.4.1.1 A Certificate would be liable to/will be revoked in any of the following circumstances (including but not limited to) —

a. A material fact represented in the Digital Signature Certificate is false or has been concealed

b. The *(n)Code Solutions CA*'s private key or security system is compromised

c. The Subscriber's private key corresponding to the public key in that Certificate has been compromised.

d. Where the information in the Digital Certificate has changed.

e. The Subscriber has breached or failed to meet his obligations under this CPS, or any other agreement, regulation or law that may be in force.

f. Upon the death or insolvency of the subscriber

g. Upon the dissolution of the firm or winding up of the company, where the subscriber is a firm or a company

h. Where the subscriber or any other person authorised by him makes a request to that effect

i. Any other circumstances as may be determined by the *(n)Code Solutions CA* from time to time in accordance with any requirements, rules or regulations of the governing law.

4.4.2 **Who Can Request Revocation**

The revocation request can only be made by —

- The Subscriber in whose name the Certificate has been issued.
- The duly authorised representative of the Subscriber.

- Authorised personnel of the *(n)Code Solutions CA* or RA when the Subscriber has breached the agreement, regulation, or law that may be in force.

4.4.2.1 The *(n)Code Solutions CA* or its RA who execute the revocation requests must ensure that the verification of the requester's identity and authority are duly performed through matching of details provided in the Revocation Request Form with the details provided during Digital Certificate application. The verifier's name, designation, signature and date on which the verification and revocation are performed are recorded for accountability and audit purpose.

4.4.3 Procedure for Revocation Request

1. ***Hand Delivery / Courier***

a. Subscriber will download revocation request form from the *(n)Code Solutions CA* website at www.ncodesolutions.com or contact *(n)Code Solutions CA*'s office or any of its LRAs for getting paper copy of the same.

b. Subscriber will duly fill in the form and hand sign it.

c. Duly filled and signed form will either be couriered or hand delivered to the *(n)Code Solutions CA*'s office.

d. The *(n)Code Solutions CA* will verify the information contained in the revocation request with the issued certificate and application form.

e. In the event of a mismatch of information, subscriber will be intimated accordingly through an email and revocation request will not be processed.

f. The *(n)Code Solutions CA* will proceed with the revocation as per the below mentioned grace period.

g. *(n)Code Solutions* reserves the right to revoke a Digital Certificate if it is of the opinion that the Subscriber has been declared insolvent or dead or where the Subscriber is a firm or company, which has been dissolved, wound-up or otherwise ceased to exist; a material fact represented in the Digital Signature Certificate is false or has been concealed. In such a case (n)Code Solutions CA shall provide an opportunity to the Subscriber to be heard in the matter before proceeding with revocation of the Digital Certificate.

2. ***Online***

a. An email with the revocation form in an attachment will be sent to the *(n)Code Solutions CA* helpdesk at **ra@ncodesolutions.com** with the subject line as "Revocation Request". The Subscriber shall encrypt this transaction by using the public key of the *(n)Code Solutions CA*. The transaction shall be digitally signed by the subscriber even though the private key may have already been compromised.

b. The (n)Code Solutions CA shall verify the information and will proceed for revocation as per the revocation grace period.

c. In the event of mismatch of information, subscriber will be intimated accordingly through an email and revocation will not be proceeded with.

4.4.4 Revocation Request Grace Period

4.4.4.1 The *(n)Code Solutions CA* PCS provides a revocation request handling mechanism along with the revocation request grace period for various classes of certificates in accordance with the following procedures.

The certificate revocation request should reach the *(n)Code Solutions CA* in the format prescribed in 4.4.9 (as per the Information Technology Certifying Authority Regulations 2001).

The table below gives the time frame available as revocation request grace period

Class of certificate	Revocation	CRL publication with revoked certificate
I	On receipt of the revocation request and information in the prescribed format, the *(n)Code Solutions CA* will decide acceptance / rejection of the revocation request. After determining suitable acceptability, The *(n)Code Solutions CA* will revoke the certificate and shall update and publish the CRL in the repository once every business working day.	The revoked certificate would be updated in the CRL which would be published in the repository once every business working day.
IIa		
IIb		
IIIa		
IIIb		
IIIc		
IIId		

4.4.4.2 The *(n)Code Solutions CA* will inform the Subscriber of the revocation action within forty-eight hours of such revocation.

4.4.5 Circumstances for Suspension

Not applicable

4.4.6 Who can request for Suspension

Not applicable

4.4.7 Procedure to Request Certificate Suspension

Not applicable

4.4.8 Limits on Suspension Period

Not applicable

4.4.9 CRL Issuance Frequency

The *(n)Code Solutions CA* updates and publishes the Certificate Revocation List (CRL) once every business working day. It is the responsibility of the Relying Party to ensure that the Certificate in use is validated against the up-to-date CRL published by the *(n)Code Solutions CA*.

4.4.10 CRL Checking Requirements by Relying Party

The Relying Party is strongly advised to (i) check the class of certificate and the status of Certificate against the up-to-date CRL published by the *(n)Code Solutions CA* prior to its use; and (ii) verify the authenticity and integrity of the CRL to ensure that it is issued and digitally signed by *(n)Code Solutions CA*.

4.4.11 Online Revocation/status checking availability

4.4.11.1 The repository and the CRL are made available to Relying Parties and to the general public via the *(n)Code Solutions CA* web site.

4.4.11.2 The repository contains all information of the Subscribers Certificates relating to their validity, activation and revocation through CRL.

4.4.12 Online Revocation Checking Requirements

The Relying Party must check the Certificate details online before trusting a Digital Certificate. The *(n)Code Solutions CA* shall not be held responsible for any loss/damage caused by Certificates issued by the *(n)Code Solutions CA* that are used by the Relying Party without checking revocation status. The Digital Certificates for each class contain the Uniform Resource Locator for checking of revocation status of the Digital Certificate in the section titled ‘CRL distribution points’.

4.4.13 Other forms of Revocation Advertisements Available

No other forms of revocation advertisements are available except from the *(n)Code Solutions CA* web site / Repository

4.4.14 Checking Requirements for Other Forms of Revocation Advertisement

Relying Party can verify revocation status only from the *(n)Code Solutions CA* web site or the Uniform Resource Locator (URL) mentioned at the CRL distribution points of respective Digital Certificate to be relied upon.

4.4.15 **Special Requirements**

There are no variations on the stipulation of revocation in the event of private key compromise or any other reason.

4.5 System Security Audit Procedures

4.5.1 **Types of Event Recorded (Audit)**

The *(n)Code Solutions CA* maintains record of all events relating to the security of its system. The records are maintained in audit log file and includes such events as:

i. System start-up and shutdown;
ii. *(n)Code Solutions CA*'s application start-up and shutdown;
iii. Attempts to create, remove, set passwords or change the system privileges of the critical users of the system;
iv. Changes to keys of the *(n)Code Solutions CA* or any of its other details;
v. Changes to Digital Signature Certificate creation policies, e.g. validity period;
vi. Login and logoff attempts;
vii. Unauthorised attempts at network access to the *(n)Code Solutions CA* 's system;
viii. Unauthorised attempts to access system files;
ix. Generation of own keys;
x. Creation and revocation of Digital Signature Certificates;
xi. Attempts to initialise remove, enable, and disable subscribers;
xii. Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) Repositories.

Monitoring and Audit Logs

(i) The *(n)Code Solutions CA* has deployed the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions are maintained:

a) Registration;
b) Certification;
c) Publication;
d) Revocation.

(ii) Records and log files are reviewed regularly for the following activities:

a) Misuse;
b) Errors;
c) Security violations;

d) Execution of privileged functions;

e) Change in access control lists;

f) Change in system configuration.

(iii) All logs, whether maintained through electronic or manual means, carry the date and time of the event, and the identity of the subscriber/subordinate/entity which caused the event.

(iv) The *(n)Code Solutions CA* also collects and consolidates, either electronically or manually, security information which is not generated by the *(n)Code Solutions CA* system, such as:

a) Physical access logs;

b) System configuration changes and maintenance;

c) Personnel changes;

d) Discrepancy and compromise reports;

e) Records of the destruction of media containing key material, activation data, or personal subscriber information.

(v) To facilitate decision-making, all agreements and correspondence relating to services provided by the *(n)Code Solutions CA* are collected and consolidated, either electronically or manually, at a single location.

4.5.2 Frequency of Audit Log processing

The *(n)Code Solutions CA* ensures that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews also involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews is documented.

4.5.3 Retention Period for Audit Log

The *(n)Code Solutions CA* shall retain its audit logs onsite for at least twelve months and offsite for seven years.

4.5.4 Protection of Audit Log

Audit logs can only be viewed, by the designated administrators of the system. They cannot be modified or deleted. Unauthorised access to the audit logs is restricted by physical and logical access control systems.

4.5.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up or copied if in manual form.

4.5.6 Audit Collection System

Audit log collection/ accumulation system is internal to the *(n)Code Solutions CA*.

4.5.7 Notification to Event Causing Subject

The Audit logs will provide information of any unauthorized access to the*(n)Code Solutions* CA system or premises. In case of any such event the authorized personnel shall be informed immediately and actions shall be taken as required by the *(n)Code Solutions CA* Security Audit Procedures Manual.

4.5.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The *(n)Code Solutions CA* has ensured that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

4.5.9 The real time clock of the computer or communication device is set accurately to Indian Standard Time (IST). A procedure to correct any drift in the real time clock is implemented.

4.6 Records Archival

4.6.1 Types of Events Recorded (Archive)

The records of following events are archived by *(n)Code Solutions CA* :

i. System start-up and shutdown;

ii. The *(n)Code Solutions CA* 's application start-up and shutdown;

iii. Attempts to create, remove, set passwords or change the system privileges of the critical users of the system;

iv. Changes to keys of the *(n)Code Solutions CA* or any of his other details;

v. Changes to Digital Signature Certificate creation policies, e.g. validity period;

vi. Login and logoff attempts;

vii. Unauthorised attempts at network access to the *(n)Code Solutions CA* 's system;

viii. Unauthorised attempts to access system files;

ix. Generation of own keys;

x. Creation and revocation of Digital Signature Certificates;

xi. Attempts to initialise remove, enable, and disable subscribers, and update and recover their keys;

xii. Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) Repositories.

4.6.2 Retention Period for Archive

Type of record	Archive retention period
Digital Signature Certificates	Seven Years
Events recorded at 4.6.1.1 above	Seven Years
Subscriber Agreements	Seven Years
Verification, identification and authentication information in respect of applicants	Seven Years
Rejected applications	Seven Years

All archived information is stored within the country. This information shall be taken out of the country only with the permission of CCA and where a properly constitutional warrant or such other legally enforceable document is produced.

4.6.3 Protection of Archive

Archives can be viewed, only by the designated administrators of the *(n)Code Solutions CA* system. They cannot be modified or deleted. Unauthorised access to the archives is restricted by physical and logical access control systems.

4.6.4 Archive Backup Procedures

A copy of all information retained or backed up is stored at two locations within the country including the *(n)Code Solutions CA* site and is adequately secured. The storage locations have adequate protection from environmental threats such as temperature, humidity and magnetism. The storage location is reachable in few hours.

4.6.5 Time-Stamping of Records

The archived records will be time-stamped by the *(n)Code Solutions CA*.

4.6.6 Archives Collection System

Archive collection system is internal to the *(n)Code Solutions CA*.

4.6.7 Procedure to Obtain and Verify Archive Information

The Certifying Authority shall verify the integrity of the backups at least once every six months. Information stored off-site shall be periodically verified for data integrity

4.7 Key Changeover

4.7.1 The *(n)Code Solutions CA* keys shall be changed periodically as stipulated by Regulation 4(1)(i) of the Information Technology (Certifying Authority) Regulations, 2001 Act and the Key change shall be processed as per Key Generation specified in this CPS.

4.7.2 The *(n)Code Solutions CA* shall provide reasonable notice to the Subscribers and Relying Parties of any change to a new key pair used by the Certifying Authority to sign Digital Signature Certificates.

4.7.3 The Subscriber keys shall not change during the validity period of the Subscriber's certificate. In case of key compromise , the Subscriber's existing Digital Certificate shall be revoked.

4.7.4 The Subscribers of the *(n)Code Solutions CA* shall be issued a Certificate by the *(n)Code Solutions CA* for a specified period of time. Before or after the expiration of the Certificate, the Subscribers shall generate a new private-public key-pair and submit the public key along with the new application to the *(n)Code Solutions CA* for renewal/ issuance of a new certificate. This should be done preferably a month before the expiry of the existing certificate.

4.7.5 The period of maximum validity of the Certificates shall be as mentioned below unless otherwise mentioned in this CPS

- Certifying Authority's keys and associated Certificates – five years
- Subscriber Digital Signature Certificate and signing key – maximum of two years

4.8 Compromise and Disaster Recovery

Detailed Disaster Recovery Procedures support the *(n)Code Solutions CA* PCS. Regular updates, modifications and testing for the same shall be carried out at specified intervals.

4.8.1 In the Event of Computing Resources, Software and/or Data being Corrupted

The *(n)Code Solutions CA* has established business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data

4.8.2 Recovery Procedures used if CA Certificate is revoked

In case the *(n)Code Solutions CA* certificate is revoked by CCA, all the certificates issued by the *(n)Code Solutions CA* shall be revoked and a CRL shall be generated. The CRL will be posted on the *(n)Code Solutions CA* website. Subsequently, the *(n)Code Solutions CA* shall obtain a new certificate from the CCA. All customers whose certificates are valid will be notified via email, and will be provided new certificates signed with the new *(n)Code Solutions CA* private key on request for the period left for the validity of the certificate and not their original certificate. There will be no extra charge for this.

4.8.3 Recovery Procedures used if Private Key is compromised

The *(n)Code Solutions CA* shall maintain a backup of all the critical information and its public keys shall be archived permanently. The compromise of the *(n)Code Solutions CA* private key shall be informed to the CCA and all the Subscribers as soon as practicable and shall also be published to the *(n)Code Solutions CA* website.

In case of subscriber's private key being compromised, the *(n)Code Solutions CA* shall immediately revoke the associated Digital Signature Certificate and publish the details in the CRL as per the CRL publication schedule.

In case of CA private Key compromise, the CA certificate shall be revoked by the CCA and the procedures as given in section 4.8.2 shall be followed.

4.8.4 Secure Facility after a Natural or Other Type of Disaster

In the event of natural or other type of disaster, the *(n)Code Solutions CA* has established a disaster recovery plan outlining the steps to be taken to re-establish a secure facility.

4.8.5 Incident Management Plan

An Incident Management Plan has been developed and approved by the management of *(n)Code Solutions CA*. The plan includes the following areas:

i. Certifying Authority's certification key compromise;
ii. Hacking of systems and network;
iii. Breach of physical security;
iv. Infrastructure non availability;
v. Fraudulent registration and generation of Digital Signature Certificates; and

An incident response action plan has also been established to ensure the readiness of *(n)Code Solutions CA* to respond to incidents. The plan includes the following areas:

i. Compromise control;
ii. Notification to user community;
iii. Revocation of affected Digital Signature Certificates;
iv. Responsibilities of personnel handling incidents;
v. Investigation of service disruption;
vi. Service restoration procedure;
vii. Monitoring and audit trail analysis; and
viii. Media and public relations.

4.9 CA Termination

4.9.1 In the event of *(n)Code Solutions CA* deciding to discontinue its operations, the *(n)Code Solutions CA* will give the CCA , RA and Subscriber a minimum of three months written notice before terminating its operations and will follow procedures in compliance with the Act.

4.9.2 The *(n)Code Solutions CA* will make arrangements for its records and Certificates to be archived in a manner prescribed by the IT Act.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This section describes physical, environmental and personnel security controls applied by the *(n)Code Solutions CA* in order to secure its Public Certificate Services

A detailed Information Systems Security Policy compliant with Information Technology Act, 2000 and Information Technology (Certifying Authority) Rules, 2000 is implemented and practiced to address various Information Systems Security concerns. Following sections contain extracts from this Information Systems Security Policy document.

5.1 Physical Controls

5.1.1 Site Location and Construction

Guidelines given in Schedule II and III of the Information Technology (Certifying Authority) Rules, 2000, have been considered for selecting, constructing and securing the site for the *(n)Code Solutions CA* PCS.

5.1.2 Physical Access

The *(n)Code Solutions CA* shall always be protected from unauthorised access. The *(n)Code Solutions CA* has implemented various manual as well as automated access control mechanisms to restrict access to authorised personnel only. These measures are in absolute conformity with the Act.

5.1.3 Power and Air Conditioning

The *(n)Code Solutions CA* systems shall have backup capability adequate to automatically finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

The *(n)Code Solutions CA* systems are adequately protected against water exposures and preventive, continuity and recovery procedures for water exposures are adopted, which are compliant with the Act .

5.1.5 Fire Prevention and Protection

The *(n)Code Solutions CA* systems are adequately protected against fire and preventive, continuity and recovery procedures for fire related disasters which are compliant with the Act.

5.1.6 Media Storage

The *(n)Code Solutions CA* media are adequately secured and stored in conformance with the Act.

5.1.7 Waste Disposal

The *(n)Code Solutions CA* systems perform waste disposal of information generated within the premises so as to prevent any compromise of critical data. These procedures are compliant with the Act.

5.1.8 Offsite Backup

The *(n)Code Solutions CA* system employs full system backups, of its critical CA components like CA, LDAP etc to recover critical operations. These procedures are compliant with the Act.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is a role assigned to a person who performs functions that can introduce security problems if not carried out properly. The personnel selected to carry out these roles must be responsible and skilled or the integrity of *(n)Code Solutions CA* shall be under threat.

The *(n)Code Solutions CA* has established trusted roles to perform the critical CA function. The appointment of these trusted roles is to ensure segregation of duties such that no one person can use the CA system. Each of these trusted roles is limited to the actions required to be performed to fulfill their responsibilities.

5.2.2 Number of Persons Required Per Task

The *(n)Code Solutions CA* has ensured that no single individual may gain access to the *(n)Code Solutions CA*. As a minimum, two individuals, using a split knowledge technique such as twin passwords, are required to perform critical CA administrative operations. The certificate revocation management procedure ,being a signing activity shall also be under dual control.

5.2.3 Identification and Authentication for Each Role

5.2.3.1 An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.3.2 The *(n)Code Solutions CA* shall ensure that the personnel performing trusted roles —

a. have been given a user account or digital certificate directly attributable to them.

b. have been given a user account or digital certificate which is not shared.

c. are restricted to actions authorised for their role through the use of their user account and/or digital certificate and *(n)Code Solutions CA* software and procedural controls.

d. are using tokens /smart cards as access mechanisms to HSM / CA / RA.

5.3 Personnel Controls

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

5.3.1.1 All persons filling trusted roles shall be selected on the basis of their trustworthiness, integrity and shall possess appropriate skills.

5.3.1.2 The *(n)Code Solutions CA* realises the above requirements by employing the following-

a. The *(n)Code Solutions CA* has ensured that personnel performing duties for the *(n)Code Solutions CA* have been appointed by a contract in writing.

b. The qualifications and experience of the *(n)Code Solutions CA* trusted personnel are in accordance to the job responsibility assigned to them. The *(n)Code Solutions CA* provides comprehensive training with respect to the duties they have to perform.

c. The *(n)Code Solutions CA* will implement appropriate background checks for its key CA trusted personnel. The RAs are recommended to conduct such checks for their administrators.

d. The *(n)Code Solutions CA* establishes procedural controls such that the CA trusted personnel are bound by statute or contract not to disclose sensitive *(n)Code Solutions CA* PCS information.

5.3.2 **Background Check Procedures**

The *(n)Code Solutions CA* 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. The *(n)Code Solutions CA* shall conduct periodic investigations of all personnel who serve in trusted positions to verify their continued trustworthiness and competence in accordance with *(n)Code Solutions CA*'s personnel practices or equivalent.

5.3.3 **Training Requirements**

All personnel performing duties with respect to the operation of the *(n)Code Solutions CA* system shall receive comprehensive training.

The *(n)Code Solutions CA* ensures that comprehensive training is provided to respective *(n)Code Solutions CA* trusted roles in areas listed below:

a. Training on all relevant policies and procedures;

b. Disaster recovery training; and

c. *(n)Code Solutions CA* security principles and mechanism

d. *(n)Code Solutions CA* software version in use
e. *(n)Code Solutions CA* operating systems and network implementation
f. Operational duties
g. *(n)Code Solutions CA* Information Technology Security Policies, Standards, Procedures and Guidelines
h. Governing regulations and rules, where appropriate

5.3.4 Retraining Frequency and Requirements

The re-training frequency is subject to the frequency of changes in the *(n)Code Solutions CA* PCS systems.

All personnel involved in running CA, RAs and LRAs within the *(n)Code Solutions CA* shall have:

a. Follow-on training conducted in a manner consistent with maintaining acceptable operational readiness;
b. Refresher training.

5.3.5 Job Rotation Frequency

The *(n)Code Solutions CA* shall not follow job rotation process.

5.3.6 Sanctions for Unauthorized Actions

Contravention of the *(n)Code Solutions CA* Policies and Practises is subject to appropriate disciplinary actions.

The *(n)Code Solutions CA* shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the *(n)Code Solutions CA* or its repository not authorized in their policies or other procedures established by the *(n)Code Solutions CA*.

The *(n)Code Solutions CA* will suspend the trusted personnel access to the *(n)Code Solutions CA* , in the event that he / she is suspected, or has performed unauthorised actions such as unauthorised use of authority and unauthorised use of the *(n)Code Solutions CA* Systems or operations.

The suspension will be immediate upon detection and the period of suspension will be subject to investigation reports.

5.3.7 Contracting Personnel Requirements

Contractors employed to perform functions pertaining to the *(n)Code Solutions CA* system shall meet applicable requirements set forth by the *(n)Code Solutions CA*.

5.3.8 Documentation Supplied to Personnel

5.3.8.1 All the documentation relating to the *(n)Code Solutions CA* and corresponding operations are classified for criticality of data and appropriate controls are in place to restrict and control movement of such documentation.

5.3.8.2 Pertaining to the training listed in Section 5.3.3, the respective documentation will be made available to the *(n)Code Solutions CA* personnel, where relevant.

6. TECHNICAL SECURITY CONTROLS

This section describes the necessary technical controls and procedures that are to be applied and followed in order to secure the *(n)Code Solutions CA* Public Certification System

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The *(n)Code Solutions CA* key pairs are generated using the trustworthy *(n)Code Solutions CA* controlled key generation software and hardware. The cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3.

For Subscribers, key pair will be generated at subscriber's end using application approved / recommended by the *(n)Code Solutions CA*.

The *(n)Code Solutions CA* PCS allows the Subscriber to have control of the generation of his key pair.

The key generation process shall generate statistically random key values that are resistant to known attacks.

6.1.2 Private Key Delivery to Entity

The *(n)Code Solutions CA* private key is generated at system initialisation stage. There is no requirement to deliver this key as this key remains in the *(n)Code Solutions CA* System.

Subscriber private key is generated at client site and hence requires no delivery.

The *(n)Code Solutions CA* Keys are generated in the highly secured storage device. The *(n)Code Solutions CA* private key is stored on the *(n)Code Solutions CA* system.

6.1.3 Public Key Delivery to Certificate Issuer

The *(n)Code Solutions CA* Public key shall be delivered to the National Root CA as a PKCS 10 request format to enable certificate issuance by the National Root CA.

For subscribers, the *(n)Code Solutions CA* PCS supports the requirements, where the public key is delivered to the *(n)Code Solutions CA* using PKIX-CMP or an equivalent secure online protocol.

6.1.4 *(n)Code Solutions CA* Public Key Delivery to Users

The *(n)Code Solutions CA* PCS supports the requirements where the CA public key certificate is available at the *(n)Code Solutions CA* website and can be downloaded from the *(n)Code Solutions CA* Repository.

6.1.5 Key Sizes

The asymmetric key pair in the *(n)Code Solutions CA* PCS will be at least 1024 bits for Subscribers. The *(n)Code Solutions CA* key pair will however be of 2048 bits.

6.1.6 ***(n)Code Solutions CA* Public Key Parameters Generation**

The *(n)Code Solutions CA* Application shall be configured to set parameters for CA public key & Subscriber Public key generation.

6.1.7 **Hardware/Software Key Generation**

6.1.7.1 The *(n)Code Solutions CA* 's key pairs shall be generated in a trustworthy hardware cryptographic module as described in section 6.8.

Key pair for all users shall be generated in a trustworthy software module.

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

6.1.8.1 Key usage purposes are incorporated in the *(n)Code Solutions CA* PCS as detailed in chapter 7 – Certificate and CRL profiles.

6.1.8.2 The *(n)Code Solutions CA* PCS ensures that CA signing key is the only key permitted to be used for signing Certificates and CRLs.

6.1.9 **Time Stamp**

All critical servers used in the *(n)Code Solutions CA* setup use the NTP suite of programs to keep themselves synchronised with time servers around the world. Accordingly, *(n)Code Solutions CA* will use time stamping services.

6.2 Private Key Protection

6.2.1 **Standards for Cryptographic Module**

The cryptographic module used by the *(n)Code Solutions CA* system to generate CA keys is designed to comply with FIPS 140-1 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 The *(n)Code Solutions 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 *(n)Code Solutions CA* trusted personnel is allowed to generate the CA private key. For accessing the HSM, minimum two (2) out of three (3) persons are required.

6.2.3 Private Key Escrow

Escrow of private key is not performed.

6.2.4 Private Key Backup

6.2.4.1 The *(n)Code Solutions CA* has backed-up its private keys. Backed-up keys are stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.

6.2.4.2 The Certifying Authority's private key backups are stored in a secure storage facility, away from where the original key is stored.

6.2.4.3 The *(n)Code Solutions CA* shall not backup the private key of the subscriber. The subscriber should ensure that his keys are securely protected.

6.2.5 Private Key Archival

The *(n)Code Solutions CA* Private Key shall be archived.

6.2.6 Private Key Entry into Cryptographic Module

(n)Code Solutions CA private key is generated in software, within the cryptographic module, and is not accessed by other entities. In all cases, private key is stored in an encrypted format in the *(n)Code Solutions CA* system and is decrypted only at the time of being used.

6.2.7 Method of Activating Private Key

All cryptographic functions are performed within the cryptographic module. The private key is never directly accessed by any other function. Each invocation of an algorithmic function requires activation with a valid PIN or pass phrase. Activation functions are supported on the HSMs and software based tokens. The activation code is input using the utilities provided with the HSM or software.

6.2.8 Method of Deactivating Private Key

The private keys remain active for the period of login.

6.2.9 Method of Destroying Private Key

Subscribers are advised to use the utility given in their application / CSP software for destroying their private as well as public key.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The *(n)Code Solutions CA* public key is archived as specified by the Information Technology Act.

6.3.2 Usage Periods for the Public and Private Keys

Keys have following usage periods:

a. Certifying Authority - Five years;

b. Subscriber – One year / Two years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The *(n)Code Solutions CA* PCS supports unique and unpredictable activation data such as the set of reference and authorisation codes and private key password.

6.4.2 Activation Data Protection

The *(n)Code Solutions CA* ensures that the activation data is protected from unauthorised use. This includes physical access control and cryptographic mechanism where locking is activated after a predetermined number of unauthorised attempts are made.

6.4.3 Other Aspects of Activation Data

In addition, for the *(n)Code Solutions CA* Security Officers and Administrators, user-names and password check values are stored in the CA database.

6.5 Computer/Systems Security Controls

6.5.1 Specific Computer Security Technical Requirements

The *(n)Code Solutions CA* PCS has fulfilled computer security technical requirements in accordance with the Act.

6.5.2 Computer Security Rating

All critical systems in the *(n)Code Solutions CA* PCS are as per the security rating prescribed by the Act.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The *(n)Code Solutions CA* PCS has established system development controls in accordance with the Act.

6.6.2 **Security Management Controls**

The *(n)Code Solutions CA* PCS system security controls are managed by the assigned trusted roles. It includes periodic execution of Operating System Scanners and Network Vulnerability Scanners. Also refer Trusted Roles

6.6.3 **Life Cycle Security Ratings**

All critical systems development life cycle in the *(n)Code Solutions CA* PCS has attained the security rating prescribed by the Act, if any.

6.7 Network Security Controls

6.7.1 Adequate network security measures like Firewall, Intrusion Detection System etc are used to protect the *(n)Code Solutions CA* operations environment against attacks from inside as well as from the Internet community.

6.8 Cryptographic Module Engineering Controls

6.8.1 The cryptographic operations controls in the *(n)Code Solutions CA* PCS are validated to FIPS 140-1 Level 3 functionality and assurance.

6.8.2 The cryptographic operations controls in the RA are validated to at least FIPS 140-1 Level 2 or equivalent level of functionality and assurance.

6.8.3 The cryptographic operations controls for the subscriber’s operations are validated to FIPS 140-1 Level 1 functionality and assurance.

7. CERTIFICATE AND CRL PROFILES

This section describes the certificate and certificate revocation list profile.

7.1 Certificate Profile

7.1.1 Version Number(s)

The *(n)Code Solutions 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

The support for Certificate extensions include —

a. *Subject Alternative Name*
b. *Private Key Usage Period*
c. *Authority Key Identifier*
d. *Subject Key Identifier*
e. *Basic Constraints*
f. *CRL Distribution Points*
g. *Key Usage*

7.1.3 Algorithm Object Identifiers

The *(n)Code Solutions CA* PCS supports the following algorithms —

a. RSA 1024 digital signature in accordance with PKCS#1
b. RSA 1024 key transfer in accordance with Internet RFC 1421 and 1423, and PKCS#1
c. SHA-1 in accordance with US FIPS PUB 180-1 and ANSI X9.30 (Part 2)
d. Triple-DES in accordance with ANSI X9.52
e. Message Authentication Code (MAC) in accordance with US FIPS PUB 113, ANSI X9.9 and X9.19
f. MD5, DSA, ECDSA, AES, DES, IDEA, CAST-128

7.1.4 Name Forms

The *(n)Code Solutions CA* PCS supports unique person name form for the following categories of Subscriber —

a. *Individual*
b. *Corporate/Corporate Representative*
c. *Government Organization /Agency*
d. *Server*
e. *VPN Device*

7.1.5 Name Constraints

Not stipulated

7.1.6 Certificate Policy Object Identifier (OID) based on the OID issued by the National Root CA of India.

Type	OID	Usage
Class I		(a) Secure E-Mail
Class IIa		(a) Web Form Signing (b) User Authentication (c) Other low Risk Transactions (d) Secure E-Mail
Class IIb		(a) Web Form Signing (b) User Authentication (c) Other low Risk Transactions (d) Secure E-Mail
Class IIIa		(a) VPN User (b) Code Signing (c) Web Form Signing (d) User Authentication (e) Secure E-Mail
Class IIIb		(a) VPN User (b) Code Signing (c) Web Form Signing (d) User Authentication (e) Secure E-Mail
Class IIIc		(a) SSL Server Authentication
Class IIId		(a) VPN Device Authentication

7.1.7 Usage of Policy Constraints Extension

Not stipulated

7.1.8 Policy Qualifiers Syntax and Semantics

Not stipulated

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Not stipulated

7.1.10 Certificate Profile Templates

7.1.10.1 Certificate Template Class I

Description	Details
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI

	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to
Time }
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = xxxxxx xxxxxxx Serial Number
	OU = Class I
	O = (n)Code Solutions CA
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806 3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B 5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
Private Key Usage Period	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
Enhanced Key Usage	Secure Email(1.3.6.1.5.5.7.3.4)
Subject Alternative Name	RFC822 Name= xxxxxx@xxxxx.xxx
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=(n)Code Solutions - A Division of GNFC LTD. OU=(n)Code Solutions CA O=India PKI C=IN [2]CRL Distribution Point Distribution Point Name: Full Name: URL=https://www.ncodesolutions.com/repository/ncodecrl.crl
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1

Thumbprint	C4B2 6B41 47C1 148A 62FD 4B26 B8DF B511 CDC1 2A75

7.1.10.2 Certificate Template Class IIa

Description	**Details**
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to Time }
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = xxxxxx xxxxxxx Serial Number
	OU = Class IIa
	OU = (n)Code solutions CA
	O = India PKI
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806 3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B 5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
Private Key Usage Period	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
Enhanced Key Usage	Client Authentication(1.3.6.1.5.5.7.3.2) Secure Email(1.3.6.1.5.5.7.3.4) Document Signing(1.3.6.1.4.1.311.10.3.12)
Certificate Policies	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
Subject Alternative Name	SSL Client Authentication, SMIME(a0)
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1

	CN=(n)Code Solutions - A Division of GNFC LTD.
	OU=(n)Code Solutions CA
	O=India PKI
	C=IN
	[2]CRL Distribution Point
	Distribution Point Name:
	Full Name:
	URL=https://www.ncodesolutions.com/repository/ncodecrl.crl

Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1
Thumbprint	C4B2 6B41 47C1 148A 62FD 4B26 B8DF B511 CDC1 2A75

7.1.10.3 Certificate Template Class IIb

Description	**Details**
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to Time }
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = xxxxxx xxxxxxx Serial Number
	OU = Class IIb
	OU = (n)Code solutions CA
	O = India PKI
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806 3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B 5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
Private Key Usage Period	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101

	33 34 39 5A 349Z
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
Enhanced Key Usage	Client Authentication(1.3.6.1.5.5.7.3.2) Secure Email(1.3.6.1.5.5.7.3.4) Document Signing(1.3.6.1.4.1.311.10.3.12)
Certificate Policies	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
Subject Alternative Name	SSL Client Authentication, SMIME(a0)
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=(n)Code Solutions - A Division of GNFC LTD. OU=(n)Code Solutions CA O=India PKI C=IN [2]CRL Distribution Point Distribution Point Name: Full Name: URL=https://www.ncodesolutions.com/repository/ncodecrl.crl
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1

7.1.10.4 Certificate Template Class IIIa

Description	**Details**
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to Time }
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = xxxxxx xxxxxxx Serial Number

	OU = Class IIIa
	OU = (n)Code solutions CA
	O = India PKI
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806 3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B 5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
Private Key Usage Period	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
Enhanced Key Usage	Client Authentication(1.3.6.1.5.5.7.3.2) Code Signing(1.3.6.1.5.5.7.3.3) Secure Email(1.3.6.1.5.5.7.3.4) IP security user(1.3.6.1.5.5.7.3.7) Document Signing(1.3.6.1.4.1.311.10.3.12)
Certificate Policies	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
Subject Alternative Name	SSL Client Authentication, SMIME(a0)
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=(n)Code Solutions - A Division of GNFC LTD. OU=(n)Code Solutions CA O=India PKI C=IN [2]CRL Distribution Point Distribution Point Name: Full Name: URL=https://www.ncodesolutions.com/repository/ncodecrl.crl
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None

1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1
Thumbprint	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b

7.1.10.5 Certificate Template Class IIIb

Description	**Details**
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to
Time }
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = xxxxxx xxxxxxx Serial Number
	OU = Class IIIb
	OU = (n)Code solutions CA
	O = India PKI
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806 3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B 5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
Private Key Usage Period	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
Enhanced Key Usage	Client Authentication(1.3.6.1.5.5.7.3.2) Code Signing(1.3.6.1.5.5.7.3.3) Secure Email(1.3.6.1.5.5.7.3.4) IP security user(1.3.6.1.5.5.7.3.7) Document Signing(1.3.6.1.4.1.311.10.3.12)
Certificate Policies	30 22 80 0F 32 30 30 34 0"..2004 30 38 30 35 30 39 34 33 08050943 34 39 5A 81 0F 32 30 30 49Z..200 35 30 38 30 35 31 30 31 50805101 33 34 39 5A 349Z
Subject Alternative	SSL Client Authentication, SMIME(a0)

Name	
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=(n)Code Solutions - A Division of GNFC LTD. OU=(n)Code Solutions CA O=India PKI C=IN [2]CRL Distribution Point Distribution Point Name: Full Name: URL=https://www.ncodesolutions.com/repository/ncodecrl.crl
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1
Thumbprint	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b

7.1.10.6 Certificate Template Class IIIc

Description	**Details**
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to
Time }
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = Web site url
	OU = Class IIIc
	OU = (n)Code solutions CA
	O = India PKI
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806 3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B

	5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
Enhanced Key Usage	Server Authentication(1.3.6.1.5.5.7.3.1)
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=(n)Code Solutions - A Division of GNFC LTD. OU=(n)Code Solutions CA O=India PKI C=IN [2]CRL Distribution Point Distribution Point Name: Full Name: URL=https://www.ncodesolutions.com/repository/ncodecrl.crl
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1
Thumbprint	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b

7.1.10.7 Certificate Template Class IIId

Description	**Details**
Version	(Version 3)
Serial Number	xxxx xxxx
Signature Algorithm	sha1RSA

Issuer	CN = (n)Code Solutions - A Division of GNFC LTD.
	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Validity ::= SEQUENCE {
Valid from Time,
Valid to
Time }
	
	Day, Month date, yyyy HH:MM:SS
	Day, Month date, yyyy HH:MM:SS

Subject	CN = xxxx xxxxxx
	OU = Class IIId
	OU = (n)Code solutions CA
	O = India PKI
	C = IN

Public key	3081 8902 8181 00B2 F7EB E8E1 F71E 3215 0C10 67C2 0806

	3191 F4F4 BAF6 C512 7D1E F28B 1EC6 441A 7A8C 0ADC C146 1C6C 8139 740E F1DA 575F 2777 60A1 561E E1E7 69AE 2A2F 1168 344F EA7D 9378 94A8 B0D8 0BDA 9230 EE02 DCB4 F0BA 3241 C679 8C79 88C3 B79D DE86 43F2 5CEF 0434 5B32 08D3 C73B 5E47 B537 6758 09D6 61A0 52D9 0F94 35FB 73B3 A09E 066B 5502 0301 0001
Key Usage	Digital Signature, Key Encipherment(a0)
NetscapeCertType	SSL Client Authentication, SMIME(a0)
NetscapeBaseURL	https://ncodesolutions.com/cda-cgi/
NetscapeRevocationURL	clientcgi.exe?action=checkRevocation&&CRL=cn=CRL1&serial=
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1 CN=(n)Code Solutions - A Division of GNFC LTD. OU=(n)Code Solutions CA O=India PKI C=IN [2]CRL Distribution Point Distribution Point Name: Full Name: URL=https://www.ncodesolutions.com/repository/ncodecrl.crl
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Subject Key Identifier	6d 1e 78 ef f0 be ac 06 9a e2 31 7a da fa 10 12 b8 db f4 0c
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
1.2.840.113533.7.65.0	30 0A 1B 04 56 36 2E 30 0...V6.0 03 02 03 A8 ....
Thumbprint algorithm	sha1
Thumbprint	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b

7.2 CRL Profile

Certificate Revocation List issued by the *(n)Code Solutions CA* under this CPS shall contain the list of the revoked Certificates.

7.2.1 Version Number(s)

The *(n)Code Solutions CA* CRL is x.509 Version 2 in accordance with ITU-T Rec. X.509 (2000) and common standard ISO/IEC 9594-8 (1997).

7.2.2 CRL and CRL Entry Extensions

The support for CRL extensions include —

- *Issuing Distribution Point*
- *CRL Number*
- *Authority Key Identifier*

7.2.3 Major Contents of CRL

Version 2 (value 1)

Issuer Issuer Distinguished Name

Effective Date This field contains the issue date of this CRL

Next Update This field indicates the date by which the next CRL will be issued.

Signature Algorithm The algorithm identifier for the algorithm used by the *(n)Code Solutions CA* for signing of the CRL.

Revoked Certificates This field contains the list of revoked Certificate serial numbers, the reason for revocation and the date on which the revocation has occurred.

7.2.4 *(n)Code Solutions CA* CRL Profile Template

Description	**Details**
Version	(Version 2)

Issuer	OU = (n)Code Solutions CA
	O = India PKI
	C = IN

Effective Date	Day, Month date, yyyy hh:mm:ss
Next Update	Day, Month date, yyyy hh:mm:ss
Signature algorithm	sha1RSA
CRL Number	CRL Number=20
Authority Key Identifier	KeyID=68 29 08 d4 f4 d0 10 5e 0c 92 f1 33 38 1e c2 3c d1 74 8f 4b
Revocation List	
Revoked Certificate	
Serial Number	40FB BA68
Revocation Date	Day, Month date, yyyy hh:mm:ss
Revocation entry	
Field	Serial Number Revocation Date CRL Reason code
Value	40FB BA68 Day, Month date, yyyy hh:mm:ss Superseded(4)

8. SPECIFICATION ADMINISTRATION

This section describes the change control, publications policies and CPS approval procedures.

8.1 Specification Change Procedure

8.1.1 A list of specification components, subcomponents, and/or elements thereof that can be changed after due approval from the CCA are Overview, Executive Summary, Contact details, Fees, Corrections of typographical errors and Changes to URL. Once approved, these changes shall be implemented immediately.

8.1.2 The list of specification components, subcomponents, and/or elements thereof that may change after approval from CCA following a 15 days notification period are :

The (n)Code Solutions CA Certification Infrastructure, Identification, Community & Applicability, Obligations, Liability, Financial Responsibilities, Interpretation & Enforcement, Publication & Repositories, Compliance Audit, Confidentiality Criteria, Intellectual Property Rights, Initial Registration, Renewal Process, Certificate Revocation, Certificate Application, Certificate Validation, Certificate issuance process, Certificate Acceptance, Certificate Profile, CRL Profile, Specification Change Procedure, Publication and Notification Policies, CPS Approval Procedures and Glossary.

Prior to making any of these changes in the *(n)Code Solutions CA* CPS, the *(n)Code Solutions CA* shall obtain comments from the relevant agency and these comments along with the proposed change(s) shall be submitted to the CCA for approval. The changes shall be adopted only after due approval from the CCA. The list will be circulated to appropriate regulatory government body, RAs, and CAs whom the *(n)Code Solutions CA* has directly cross-certified with, for comments. The comment period will be 15 days unless otherwise specified. All comments will be consolidated and reviewed by the *(n)Code Solutions CA* PCS management or any committee authorised by the former. The decision to implement the proposed changes is at the sole discretion of the *(n)Code Solutions CA* PCS management, subject to approval from CCA . A decision for the final change will be announced within 15 days of such approval from the CCA. The *(n)Code Solutions CA* will adhere to its change management control procedures such that all changes made to the CPS are tracked and version controls are in place. Changes to the CPS will be notified to the Controller of Certifying Authorities as and when they are made. Current version of the CPS will be available at the *(n)Code Solutions CA* website, and all the versions will be securely stored within the *(n)Code Solutions CA* archives.

8.2 Publication and Notification Policies

8.2.1 A list of components, subcomponents, and elements thereof that exist but that are not made publicly available:

8.2.2 System Security Audit Procedures, Records Archival, Disaster Recovery, CA Termination, Physical controls, Procedural controls, Personnel controls, Key Pair Generation and Installation, Private Key Protection, Other Aspects of Key Pair Management, Activation Data, Computer/Systems Security Controls, Life Cycle Technical Controls, Network Security Controls and Cryptographic Module Engineering Controls.

8.2.3 All items in the *(n)Code Solutions CA* CPS are subject to the publication and notification requirement.

8.2.4 All publication and notification will be done via the *(n)Code Solutions CA* web site at www.ncodesolutions.com unless the notification has great impact to The *(n)Code Solutions CA*, Sponsor, RA, Subscriber and Relying Party, e.g. termination of CA services.

8.2.5 The *(n)Code Solutions CA* may digitally sign each publication and notification before they are posted at the *(n)Code Solutions CA* secure web site.

8.2.6 The *(n)Code Solutions CA* will, from time to time, suggest and make available to, publish or will notify the Subscriber of what may be constituted as adequate private key protection measures.

8.2.7 *)Code Solutions CA* will make available to, publish or will notify the Subscriber of risks associated with the use of any Certificate, issued by the *(n)Code Solutions CA* to the Subscriber, based on any technologies used by the *(n)Code Solutions CA* which have been discontinued or superseded.

8.3 Approval Procedures

8.3.1 Once a revised CPS is ready ; the *(n)Code Solutions CA* shall submit the proposed changes to the CCA for approval. The changes will be adopted only after due approval from the CCA for its publication on the *(n)Code Solutions CA* website.

9. GLOSSARY

ABSTRACT SYNTAX NOTATION.1 (ASN.1)

ASN.1 is an abstract language representation used to describe data types in a machine-independent fashion.

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 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 entity 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."

ALIAS

A pseudonym.

APPLICANT

"A person who has applied to become a Key Holder, prior to the time at which Keys and Certificates are issued to and Accepted by them."

APPLICATION

A request from an Applicant (or an Organisation) for a Certificate to be issued to the 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 RA. ""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 analysing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.

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.

AUTHORISATION

"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."

CA DIRECTORY ADMINISTRATOR

Trusted *(n)Code Solutions CA* personnel responsible for day-to-day activities involved in administering an X.500 Directory

CA SECURITY OFFICERS

Highly trusted *(n)Code Solutions CA* personnel in a position to set the *(n)Code Solutions CA*'s security policies for the *(n)Code Solutions CA* operation.

CA ADMINISTRATORS

Trusted *(n)Code Solutions CA* personnel responsible for day-to-day activities involved in administering the *(n)Code Solutions CA* system

CA OPERATORS

Trusted *(n)Code Solutions CA* personnel responsible for day-to-day batch activities such as backup, restore and etc.

CERTIFICATE

A set of information which at a minimum:

(a) Identifies the Certification Authority issuing the Certificate.

(b) Unambiguously names or identifies the Certificate's holder (the Key Holder/organization);

(c) Contains the Public Key; and

(d) Is digitally signed by the Certificate Authority issuing it.

CERTIFICATE APPLICANT

A person or authorized agent that requests the issuance of a public key certificate by an IA.

CERTIFICATE APPLICATION

A request from a certificate applicant (or authorized agent) to an RA for the issuance of a 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 ISSUANCE

The actions performed by an RA 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 RA undertakes certificate management functions by serving as a registration authority for subscriber certificates. An RA designates issued and accepted certificates as valid by publication."

CERTIFICATE POLICY (CP)

"A named set of rules that indicate 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 Certificate Type to the authentication of electronic transactions with a particular Agency or Government transactions up to a certain financial value. "

CERTIFICATE REVOCATION LIST (CRL)

A CRL is a signed list of entries corresponding to revoked public keys, with each entry indicating the serial number of the associated Certificate, the time the revocation was first made, and possibly other information such as the revocation reason.

CERTIFICATE SERIAL NUMBER

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

CERTIFICATE SIGNING REQUEST (CSR)

A request from a person generating Keys for a CA to generate a Certificate and sign that Certificate.

CERTIFICATION / CERTIFY

The process of issuing a certificate by an RA.

CERTIFICATION PRACTISE STATEMENT (CPS)

A statement of the practices that a Certifying Authority employs in issuing Certificates. The *(n)Code Solutions CA* CPS describes the operational practices of the *(n)Code Solutions CA* in relation to its CA and RA services and is published in the Repository.

"CLASS [1, 2, 3] CERTIFICATE"

A certificate of a specified level of trust.

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. "

CONFIDENTIALITY

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

CONFIRM

To ascertain through appropriate inquiry and investigation.

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 the *(n)Code Solutions CA* and a non-*(n)Code Solutions CA* 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.

CRYPTOGRAPHIC MODULE

"A Cryptographic Module is hardware, software, or firmware or any combination of them which using Cryptography can be used to protect the information stored therein."

CRYPTOGRAPHY

(a)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.

"(b) 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 use."

DATA

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

DATA INTEGRITY

A condition in which data has not been altered or destroyed in an unauthorized manner.

DATABASE

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

DEMO CERTIFICATE

A certificate issued by an CA 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.

DIGITAL SIGNATURE

"An electronic signature created using a Private Key consisting of data appended to, or a Cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery."

DISTINGUISHED NAME

"A unique identifier of a person or thing having the structure required by the relevant Certificate Profile. A Distinguished Name is assigned to each Key Holder, Organization or other entity."

DOCUMENT

A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information.

"ELECTRONIC MAIL (""E-MAIL"")"

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

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).

ENROLLMENT

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

EXPIRATION DATE

"The time and date stated in a Certificate as the end of the Operational Period, after which the Certificate will expire."

EXPIRY

When the current date passes the Expiration Date a Certificate is said to have expired.

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.

GOVERNING LAW

The laws of the Republic of India.

GRACE PERIOD

The time period under which the *(n)Code Solutions CA* will take to respond to an action.

THE *(n)Code Solutions CA*

The *(n)Code Solutions CA* is a trusted third party ("TTP") to issue and sign the *(n)Code Solutions CA* Certificate.

THE *(n)Code Solutions CA* CERTIFICATE MANAGER

A software system that manages cryptographic keys for the *(n)Code Solutions CA* users.

THE *(n)Code Solutions CA* CPS

The *(n)Code Solutions CA* CPS is a detailed statement of the practices and operational procedures that supports multiple CP, of the *(n)Code Solutions CA*.

THE *(n)Code Solutions CA* PUBLIC CERTIFICATION SERVICES FRAMEWORK ("PCS")

The *(n)Code Solutions CA* PCS is the Certificate-based Public Key Infrastructure (PKI)that issues, manages, revokes and renews the *(n)Code Solutions CA* Certificate in accordance with the practices set out in the *(n)Code Solutions CA* CPS. Please see the *(n)Code Solutions CA* CPS.

IDENTIFICATION/IDENTITY

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.

ISSUE

"A process whereby the CA, based on the Registration Information, generates a Certificate and distributes this to the customer."

KEY

"A data element used to encrypt or decrypt a message - includes both Public Keys and Private Keys. A sequence of symbols that controls the operation of a Cryptographic transformation (e.g. encipherment, decipherment, Cryptographic check function computation, signature generation, or signature authentication)."

KEY GENERATION

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

KEY PAIR

A pair of asymmetric cryptographic Keys (ie. one decrypts messages which have been encrypted using the other) consisting of a Public Key and a Private Key.

MESSAGE

A digital representation of information; a computer-based record. A subset of RECORD.

NAME

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

NON REPUDIATION

"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.

NOTICE

The result of notification in accordance with this CPS.

NOTIFY

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

OBJECT IDENTIFIER ("OID")

An OID is a value, comprising a sequence of integer components, which can be conveniently assigned for some specific purpose, and which has the property of being unique within the space of all OIDs.

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. "

PASSWORD (PASS PHRASE; PIN NUMBER)

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

PERSON

"A human being or an organisation (or a device under the control of a human being or organisation) 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 ENTITY

"The *(n)Code Solutions CA*, Subordinate CAs, RAs, Key Holders, Relying Parties and the entity which provides Repository services (if it is not one of these entities)."

PRIVATE KEY

"The half of a Key Pair which must be kept secret to ensure confidentiality, integrity, authenticity and non-repudiation of messages."

PUBLIC KEY

"The half of a Key Pair which may be made public, and is published in the Certificate."

PUBLIC KEY INFRASTRUCTURE (PKI)

"The combination of hardware, software, people, policies and procedures needed to create, manage, store, distribute and revoke Public Key Certificates based on public key Cryptography."

PUBLISH / PUBLICATION

To record or file information in a repository in order to disclose and make publicly available such information in a manner that is consistent with this CPS and applicable law.

RA AGREEMENT

RA agreement is a contract which provides detailed outline of procedures, obligation and liabilities for each *(n)Code Solutions CA* appointed RA.

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. "

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"".

REGISTRATION

"The process for receiving and processing applications for Keys and Certificates, including collection of Registration Information."

REGISTRATION AUTHORITY (RA)

"An entity which registers Applicants for Keys and Certificates (see Registration). RAs may have other functions or obligations specified in the relevant CP.

REGISTRATION FIELD INFORMATION

"Country, postcode, age, and gender data included within designated certificates at the option of the Subscriber."

REGISTRATION INFORMATION

"Information about Key Holders or Organizations which is reasonably required for the issue and use of Keys and Certificates, including information needed to: verify the identity of the Key Holder; verify the identity of and the Organization; confirm that the Key Holder has authority to hold and use Keys and Certificates on behalf of the Organization; and confirm that the Organization is a member of the Community of Interest"

RELATIVE DISTINGUISHED NAME (RDN)

A set of attributes compromising 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.

RELYING PARTY

Relying Party is a recipient of a Subscriber's Certificate in the *(n)Code Solutions CA* PCS who acts in reliance on that *(n)Code Solutions CA* Certificate.

RENEW

The process whereby a new Certificate is issued to a Key Holder/organization at the end of the Operational Period of a Certificate.

RENEWAL

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

REPUDIATION (SEE ALSO NON REPUDIATION)

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

REVOKE

To terminate the effectiveness of a Certificate before the end of the Operational Period of a Certificate.

ROOT

"The CA 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/MIME

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

SECRET SHARE

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

SECRET SHARING

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

The *(n)Code Solutions CA*'s Accredited Document which sets out its various policies and procedures that relate to security of its premises and infrastructure.

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. "

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. "

SUBSCRIBER

An individual, partnership, corporation, server or such other categories of person who is a holder of any *(n)Code Solutions CA* Certificate.

SUBSCRIBER INFORMATION

Information supplied to a certification authority as part of a certificate application.

TEST CERTIFICATE

A certificate issued by an CA for the limited purpose of internal technical testing. Test certificates may be used by authorized persons only.

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 Time Stamp is a record 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.

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 RA entity and an CA. A RA entity must be certain that it can trust the CA 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 CPS.

TYPE (OF CERTIFICATE)

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

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 CA issuing the certificate."

VALID CERTIFICATE

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

VERIFY

The process whereby the identity of a person or thing or relationship is confirmed by reference to external documentation.

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.