



## **MTNL TRUSTLINE CERTIFICATE POLICY (CP)**

**VERSION -1.0**

**EFFECTIVE DATE: AUGUST 15, 2003**



**MAHANAGAR TELEPHONE NIGAM LIMITED**

**JEEVAN BHARATI, 124 CONNAUGHT CIRCUS, NEW DELHI – 110 001**



**NOTE**

The Capitalized and Underlined terms in this CP are defined terms with specific meanings. Please see 'List of Terms' (CP § [9](#)) for a list of definitions.

This Certificate Policy document assumes that the reader is generally familiar with Public Key Infrastructure (PKI), Digital Certificates, Digital Signatures, Indian IT-Act 2000, Encryption, and the MTNLTRUSTLINE PKI. If not, MTNLTRUSTLINE advises that the reader obtain some training in the use of Public Key Cryptography and Public Key Infrastructure as implemented in the MTNLTRUSTLINE PKI. General educational and training information is accessible from MTNLTRUSTLINE at <http://www.mtnltrustline.com/faq>. Also, a brief summary of the roles of the different MTNLTRUSTLINE PKI participants is set forth in CP § [1.3](#).

This latest version of this CP is available for viewing in electronic form within the MTNLTRUSTLINE Repository at <https://www.mtnltrustline.com/repository/cp>.

Updates to the CP are posted in the updates section of the MTNLTRUSTLINE Repository, at <https://www.mtnltrustline.com/repository/updates>.



MTNL

CERTIFICATE POLICY

---

---

## TABLE OF CONTENTS

<b>1 INTRODUCTION .....</b>	<b>1</b>
1.1 OVERVIEW .....	2
1.1.1 Compliance with IT-Act .....	2
1.1.2 Role of the CP and Other Documents .....	2
1.1.3 Relationship with Controller of Certifying Authority .....	4
1.1.4 Policy Overview .....	4
1.1.4.1 Class 1 Certificates .....	4
1.1.4.2 Class 2 Certificates .....	5
1.1.4.3 Class 3 Certificates .....	5
1.1.4.4 Test Certificates .....	6
1.2 IDENTIFICATION .....	6
1.3 COMMUNITY AND APPLICABILITY .....	7
1.3.1 Certifying Authorities (CAs) .....	7
1.3.2 Registration Authorities (RAs) .....	8
1.3.3 End Entities .....	8
1.3.3.1 Subscribers .....	8
1.3.3.2 Relying Parties .....	8
1.3.4 Applicability .....	9
1.3.4.1 Suitable Applications .....	9
1.3.4.1.1 Suitable Applications for Class 1 Certificates .....	9
1.3.4.1.2 Suitable Applications for Class 2 Certificates .....	10
1.3.4.1.3 Suitable Applications for Class 3 Certificates .....	11
1.3.4.2 Restricted Applications .....	11
1.3.4.3 Prohibited Applications .....	12
1.4 CONTACT DETAILS .....	12
<b>2 GENERAL PROVISIONS .....</b>	<b>13</b>
2.1 OBLIGATIONS .....	13
2.1.1 CA Obligations .....	13
2.1.2 RA Obligations .....	14
2.1.3 Subscriber Obligations .....	14
2.1.4 Relying Party Obligations .....	15
2.1.5 Repository Obligations .....	16
2.2 LIABILITY .....	16
2.2.1 CA Liability .....	16
2.2.1.1 Warranties to Subscribers and Relying Parties .....	16



2.2.1.2 Disclaimers of Warranties .....	17
2.2.1.3 Limitations of Liability .....	17
2.2.1.4 Force Majeure .....	18
2.2.2 RA Liability .....	18
2.2.3 Subscriber Liability .....	18
2.2.3.1 Subscriber Warranties.....	18
2.2.3.2 Private Key Compromise .....	19
2.2.4 Relying Party Liability.....	19
2.3 FINANCIAL RESPONSIBILITY .....	19
2.3.1 Indemnification by Subscribers and Relying Parties .....	19
2.3.1.1 Indemnification by Subscribers .....	19
2.3.1.2 Indemnification by Relying Parties.....	20
2.3.2 Fiduciary Relationships.....	20
2.3.3 Administrative Processes .....	20
2.4 INTERPRETATION AND ENFORCEMENT .....	21
2.4.1 Governing Law.....	21
2.4.2 Severability, Survival, Merger, Notice .....	21
2.4.3 Dispute Resolution Procedures .....	21
2.4.3.1 Role of the CCA.....	21
2.5 FEES.....	21
2.5.1 Certificate Issuance or Renewal Fees.....	21
2.5.2 Certificate Access Fees .....	22
2.5.3 Revocation or Status Information Access Fees .....	22
2.5.4 Fees for Other Services Such as Policy Information .....	22
2.5.5 Refund Policy.....	22
2.6 PUBLICATION AND REPOSITORIES .....	22
2.6.1 Publication of CA Information .....	22
2.6.2 Frequency of Publication.....	23
2.6.3 Access Controls.....	23
2.6.4 Repositories .....	23
2.7 COMPLIANCE AUDIT .....	23
2.7.1 Frequency of Compliance Audit.....	23
2.7.2 Identity/ Qualifications of Auditor .....	24
2.7.2.1 Self-Audits.....	24
2.7.3 Auditor's Relationship to Audited Party .....	24
2.7.4 Topics covered by audit.....	24



---

2.7.5 Actions Taken as a Result of Deficiency .....	25
2.7.6 Communications of Results .....	25
2.8 CONFIDENTIALITY POLICY .....	25
2.8.1 Types of Information to be Kept Confidential .....	26
2.8.2 Types of Information Not Considered Confidential .....	26
2.8.3 Disclosure of Certificate Revocation/Suspension Information.....	26
2.8.4 Release to Law Enforcement Officials.....	26
2.8.5 Release as part of Civil Discovery .....	27
2.8.6 Disclosure Upon Owner’s Request .....	27
2.8.7 Other Information Release Circumstances .....	27
2.9 INTELLECTUAL PROPERTY RIGHTS .....	27
2.9.1 Rights in Certificates.....	27
2.9.2 Rights in the CP & CPS.....	27
2.9.3 Rights in Names.....	28
2.9.4 Rights in Keys and Key Material.....	28
<b>3 IDENTIFICATION AND AUTHENTICATION .....</b>	<b>29</b>
3.1 INITIAL REGISTRATION.....	29
3.1.1 Types of Names .....	29
3.1.2 Meaning of Names.....	29
3.1.3 Rules for Interpreting Various Name Forms .....	30
3.1.4 Uniqueness of Names.....	30
3.1.5 Name Claim Dispute Resolution .....	30
3.1.6 Recognition, Authentication, and Role of Trademarks.....	30
3.1.7 Method to Prove Possession of Private Key.....	31
3.1.8 Authentication of Organization Identity.....	31
3.1.8.1 Authentication of Organization Identity .....	31
3.1.8.2 Class 2 Certificates for Devices .....	31
3.1.8.3 Class 3 Server Certificates.....	32
3.1.8.4 Authentication of the Identity of Sub-CAs and RAs .....	32
3.1.9 Authentication of Individual Identity.....	32
3.1.9.1 Class 1 Certificates.....	33
3.1.9.2 Class 2 Certificates.....	33
3.1.9.3 Class 3 Certificates.....	34
3.2 ROUTINE REKEY (RENEWAL) .....	34
3.2.1 Renewal of End User Subscriber Certificates.....	34
3.2.2 Renewal of Sub-CA Certificates.....	35



3.3 REKEY AFTER REVOCATION - NO KEY COMPROMISE .....	35
3.4 REVOCATION REQUESTS .....	36
<b>4 OPERATIONAL REQUIREMENTS .....</b>	<b>37</b>
4.1 CERTIFICATE APPLICATION .....	37
4.1.1 Enrollment for End User Subscriber Certificates .....	37
4.1.2 Enrollment for Sub-CA or RA Certificates .....	37
4.2 CERTIFICATE ISSUANCE .....	38
4.2.1 Issuance of End User Subscriber Certificates .....	38
4.2.2 Issuance of Sub-CA and RA Certificates .....	38
4.3 CERTIFICATE ACCEPTANCE .....	39
4.4 CERTIFICATE SUSPENSION AND REVOCATION .....	39
4.4.1 Circumstances for Revocation .....	39
4.4.1.1 Circumstances for Revoking End User Subscriber Certificates .....	39
4.4.1.2 Circumstances for Revoking Sub-CA or RA Certificates .....	40
4.4.2 Who Can Request Revocation .....	41
4.4.2.1 Who Can Request Revocation of an End User Subscriber Certificate .....	41
4.4.2.2 Who Can Request Revocation of a Sub-CA or RA Certificate .....	41
4.4.3 Procedure for Revocation Request .....	41
4.4.3.1 Procedure for Revocation Request of an End User Subscriber Certificate .....	41
4.4.3.2 Procedure for Revocation Request of a Sub-CA or RA Certificate .....	42
4.4.4 Revocation Request Grace Period .....	42
4.4.5 Circumstances for Suspension .....	42
4.4.6 Who Can Request Suspension .....	42
4.4.7 Procedure for Suspension Request .....	42
4.4.8 Limits on Suspension Period .....	43
4.4.9 CRL Issuance Frequency .....	43
4.4.10 Certificate Revocation List Checking Requirements .....	43
4.4.11 On-Line Revocation/Status Checking Availability .....	43
4.4.12 On-Line Revocation Checking Requirements .....	44
4.4.13 Other Forms of Revocation Advertisements Available .....	44
4.4.14 Checking Requirements for Other Forms of Revocation Advertisements .....	44
4.4.15 Special Requirements Regarding Key Compromise .....	44
4.5 SECURITY AUDIT PROCEDURES .....	44
4.5.1 Types of Events Recorded .....	44
4.5.1.1 Events Recorded by mtnlTrustLine CA .....	44
4.5.1.2 Events Recorded by mtnlTrustLine RAs .....	46



4.5.2	<i>Frequency with which audit logs are processed</i>	47
4.5.3	<i>Period for which audit logs are kept</i>	47
4.5.4	<i>Protection of Audit Log</i>	47
4.5.5	<i>Audit Log Backup Procedures</i>	47
4.5.6	<i>Audit Log Accumulation System (Internal or External)</i>	47
4.5.7	<i>Notification to Event-Causing Subject</i>	48
4.5.6	<i>Vulnerability Assessments</i>	48
4.6	RECORDS ARCHIVAL	48
4.6.1	<i>Types of Event Recorded</i>	48
4.6.2	<i>Retention Period for Archive</i>	49
4.6.3	<i>Protection of Archive</i>	49
4.6.4	<i>Archive Backup Procedures</i>	49
4.6.5	<i>Requirements for Time-Stamping of Records</i>	49
4.6.6	<i>Archive Collection System (Internal or External)</i>	49
4.6.7	<i>Procedures to Obtain and Verify Archive Information</i>	50
4.7	KEY CHANGEOVER	50
4.8	COMPROMISE AND DISASTER RECOVERY	50
4.8.1	<i>Computing Resources, Software, and/or Data Are Corrupted</i>	51
4.8.2	<i>Entity Public Key is Revoked</i>	51
4.8.3	<i>Entity Key is Compromised</i>	51
4.8.4	<i>Secure Facility After a Natural or Other Type of Disaster</i>	51
4.9	CA TERMINATION	52
<b>5</b>	<b>PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS</b>	<b>54</b>
5.1	PHYSICAL SECURITY CONTROLS	54
5.1.1	<i>Site Location and Construction</i>	54
5.1.2	<i>Physical Access</i>	55
5.1.3	<i>Power and Air Conditioning</i>	55
5.1.4	<i>Water Exposures</i>	55
5.1.5	<i>Fire Prevention and Protection</i>	56
5.1.6	<i>Media Storage</i>	56
5.1.7	<i>Waste Disposal</i>	56
5.1.8	<i>Off-Site Backup</i>	56
5.2	PROCEDURAL CONTROLS	57
5.2.1	<i>Trusted Roles</i>	57
5.2.2	<i>Number of Persons Required Per Task</i>	58
5.2.3	<i>Identification and Authentication for Each Role</i>	58



5.3 PERSONNEL SECURITY CONTROLS .....58

    5.3.1 Background, Qualifications, Experience, and Clearance Requirements ....58

    5.3.2 Background Check Procedures.....58

    5.3.3 Training Requirements and Training Procedures.....59

    5.3.4 Retraining Frequency and Requirements .....60

    5.3.5 Job Rotation Frequency and Sequence.....60

    5.3.6 Sanctions for Unauthorized Actions .....60

    5.3.7 Contracting Personnel Requirements .....61

    5.3.8 Documentation Supplied to Personnel.....61

**6 TECHNICAL SECURITY CONTROLS..... 62**

6.1 KEY PAIR GENERATION AND INSTALLATION .....62

    6.1.1 Key Pair Generation and Installation.....62

    6.1.2 Private Key Delivery to Entity.....63

    6.1.3 Public Key Delivery to Certificate Issuer.....63

    6.1.4 CA Public Key Delivery to Users .....63

    6.1.5 Key Sizes .....64

    6.1.6 Public Key Parameters Generation .....64

    6.1.7 Parameter Quality Checking.....64

    6.1.8 Hardware or Software Key Generation.....64

    6.1.9 Key Usage Purposes .....65

6.2 PRIVATE KEY PROTECTION.....66

    6.2.1 Standards for Cryptographic Modules .....66

    6.2.2 Private Key 'n out of m' Multi-Person Control.....66

    6.2.3 Private Key Escrow .....67

    6.2.4 Private Key Backup.....67

    6.2.5 Private Key Archival.....67

    6.2.6 Private Key Entry into Cryptographic Module .....68

    6.2.7 Method of Activating Private Key .....68

        6.2.7.1 End User Subscriber Private Keys .....68

        6.2.7.2 CA/Sub-CA Private Keys.....69

    6.2.8 Method of Deactivating Private Key.....69

    6.2.9 Method of Destroying Private Key .....70

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT.....70

    6.3.1 Public Key Archival .....70

    6.3.2 Usage Periods for the Public and Private Keys.....70

6.4 ACTIVATION DATA .....71



---

6.4.1 Activation Data Generation and Installation .....	71
6.4.2 Activation Data Protection.....	72
6.4.3 Other Aspects of Activation Data .....	73
6.5 COMPUTER SECURITY CONTROLS .....	73
6.5.1 Specific Computer Security Technical Requirements .....	73
6.5.2 Computer Security Rating.....	73
6.6 LIFE CYCLE SECURITY CONTROLS.....	74
6.6.1 System Development Controls.....	74
6.6.2 Security Management Controls .....	74
6.6.3 Life Cycle Security Ratings.....	74
6.7 NETWORK SECURITY CONTROLS .....	74
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	75
<b>7 CERTIFICATE AND CRL PROFILES .....</b>	<b>76</b>
7.1 CERTIFICATE PROFILE .....	76
7.1.1 Version Number(s) Supported .....	77
7.1.2 Certificate Extensions.....	77
7.1.2.1 Basic Constraints.....	78
7.1.2.2 Extended Key Usage.....	78
7.1.3 Algorithm Object Identifiers .....	79
7.1.4 Name Forms.....	79
7.1.5 Name Constraints.....	79
7.1.6 Certificate Policy Object Identifier .....	80
7.1.7 Usage of Policy Constraints Extension.....	80
7.1.8 Policy Qualifiers Syntax and Semantics.....	80
7.1.9 Processing Semantics for the Critical Certificate Policy Extension .....	80
7.2 CRL PROFILE.....	80
7.2.1 Version Number(s) Supported .....	80
7.2.2 CRL and CRL Entry Extensions.....	80
<b>8 SPECIFICATION ADMINISTRATION .....</b>	<b>81</b>
8.1 SPECIFICATION CHANGE PROCEDURES.....	81
8.1.1 Items that Can Change Without Notification .....	81
8.1.2 Items that Can Change with Notification .....	81
8.1.2.1 List of Items .....	81
8.1.2.2 Notification Mechanism .....	82
8.1.2.3. Comment Period .....	82
8.1.2.4. Mechanism to Handle Comments.....	82



8.1.3 Changes Requiring Changes in the Certificate Policy OID.....	82
8.2 PUBLICATION AND NOTIFICATION PROCEDURES .....	83
8.3 CPS APPROVAL PROCEDURES .....	83
<b>9 LIST OF TERMS .....</b>	<b>84</b>
9.1 LIST OF ACRONYMS.....	84
9.2 DEFINITIONS .....	85

## **1 INTRODUCTION**

This document is the Certificate Policy (CP) of MTNLTRUSTLINE, a service of Mahanagar Telephone Nigam Limited (MTNL). The CP is the principal statement of policy governing MTNLTRUSTLINE.

The Indian Information Technology Act – 2000 (IT-Act 2000) provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents.

To facilitate the authentication of electronic documents the IT-Act 2000 provides legal recognition<sup>1</sup> to Digital Signatures created using Digital Certificates issued by Certifying Authorities duly licensed by the 'Controller of Certifying Authorities'.

MTNLTRUSTLINE is a Public Key Infrastructure (PKI) established by Mahanagar Telephone Nigam Limited (MTNL) that provides Digital Certificates to entities including but not limited to Individuals, Organizations, Servers, Network Devices, and 'legal persons' within the framework of IT-Act 2000.

This CP establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing Digital Certificates in accordance to the requirements of the IT-Act 2000.

---

### **<sup>1</sup> 5. Legal recognition of Digital Signatures.**

"Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government." – IT Act 2000.

MTNLTRUSTLINE issues three Classes of Certificates: Class 1, Class 2, and Class 3. The CP describes how these three Classes correspond to three Classes of applications with common security requirements. The CP is a single document that defines three Certificate Policies, one for each of the Classes. The current version of the CP identifies the MTNLTRUSTLINE Standards applicable to each 'Class'.

## **1.1 OVERVIEW**

The CP establishes requirements for the entire MTNLTRUSTLINE community comprising of the MTNLTRUSTLINE, Certifying Authorities (CAs), Subordinate Certifying Authorities (Sub-CAs), Registration Authorities (RAs), Subscribers, Relying Parties, and other such entities as may be associated with MTNLTRUSTLINE.

### **1.1.1 COMPLIANCE WITH IT-ACT**

This CP shall always be interpreted in association with the IT-Act and any rules, regulations, and guidelines to the act gazetted by the Controller of Certifying Authorities from time to time.

This CP follows the framework provided in RFC 2527 [<http://www.ietf.org/rfc/rfc2527.txt>] as required by the IT-Act.

### **1.1.2 ROLE OF THE CP AND OTHER DOCUMENTS**

The CP describes at a general level the overall business, legal, and technical infrastructure of the MTNLTRUSTLINE. More specifically, it describes, among other things:

Appropriate applications for, and the assurance levels associated with, each Class of Certificate,

Obligations of Certifying Authorities, Registration Authorities, Subscribers, and Relying Parties,

Legal matters that must be covered in MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement,

Requirements for audit and related security and practices reviews,

Methods to confirm the identity of Certificate Applicants for each Class of Certificate,

Operational procedures for Certificate Applications, Issuance, Acceptance, Revocation, and Renewal,

Operational security procedures for audit logging, records retention, and disaster recovery,

Physical, personnel, cryptographic private key, and logical security,

Certificate and Certificate Revocation List content, and

Administration of the CP, including methods of updating it.

The CP, however, is only the first in a set of documents relevant to the MTNLTRUSTLINE. These other documents include:

Security and operational policy documents and manuals that supplement the CP by providing more detailed requirements, such as:

- » The MTNLTRUSTLINE security policy and standards, which sets forth security principles governing the MTNLTRUSTLINE infrastructure,
- » The MTNLTRUSTLINE operating procedures manual, which details the procedures for carrying out various activities related to the MTNLTRUSTLINE infrastructure.

MTNLTRUSTLINE Certification Practice Statements. While the CP sets forth requirements, the CPS explains how MTNLTRUSTLINE employs practices and procedures to meet these requirements.

MTNLTRUSTLINE Subscriber Agreement that binds the Subscribers of MTNLTRUSTLINE Digital Certificates.

MTNLTRUSTLINE Relying Party Agreement that binds the MTNLTRUSTLINE Relying Parties.

### **1.1.3 RELATIONSHIP WITH CONTROLLER OF CERTIFYING AUTHORITY**

The CCA has established the Root Certifying Authority of India (RCAI) under section 18(b) of the IT-Act to digitally sign the Public Keys of licensed CAs in India.

The MTNLTRUSTLINE Public Key Infrastructure is designed to be subordinate to the RCAI. This is achieved by the RCAI issuing a digitally signed CA Certificate that authenticates the Public Key(s) of the MTNLTRUSTLINE certifying authority. This CA Certificate can be downloaded from the CCA's website [<http://www.cca.gov.in/>] as well as MTNLTRUSTLINE's website [<https://www.mtnltrustline.com/repository/ca/>].

The CCA has also established the National Repository of Digital Certificates (NRDC) under section 20 of the IT-Act to act as a directory of all Certificates and CRLs issued by all the licensed CAs in India. MTNLTRUSTLINE PKI Certificates and CRLs shall be published to the NRDC.

### **1.1.4 POLICY OVERVIEW**

In accordance to the guidelines of IT-Act, MTNLTRUSTLINE offers three distinct Classes of Certificates, Class 1, Class 2, and Class 3.

Each Class of Certificate is associated with specific security features and corresponds to a specific level of trust. MTNLTRUSTLINE Subscribers and Relying Parties choose which Classes of Certificates they need.

#### **1.1.4.1 CLASS 1 CERTIFICATES**

Class 1 Certificates are issued to Individuals with valid e-mail addresses. They assure that the Subscriber's distinguished name (DN) is unique and unambiguous within MTNLTRUSTLINE Repository and that the e-mail address in the DN is associated with the Public Key in the Certificate.

Class 1 Certificates are appropriate for Digital Signatures, encryption, and electronic access control for non-commercial transactions where proof of identity is not required.

#### **1.1.4.2 CLASS 2 CERTIFICATES**

Class 2 Certificates are issued to Individuals and Devices. They assure that the identity of the Subscriber based on information provided by the Subscriber in the Certificate Application does not conflict with the information in a MTNLTRUSTLINE approved and well-recognized business or consumer database(s) (Validating Database).

Class 2 Individual Certificates are appropriate for Digital Signatures, encryption, and electronic access control in transactions where proof of identity based on information in the Validating Database is sufficient.

Class 2 Device Certificates are appropriate for device authentication; message, software, and content integrity; and confidentiality encryption.

#### **1.1.4.3 CLASS 3 CERTIFICATES**

Class 3 Certificates are issued to Individuals, Organizations, Servers, Devices, and Administrators for CAs and RAs.

Class 3 Certificates issued to Individuals assure of the identity of the Subscriber based on the personal (physical) presence of the Subscriber before a MTNLTRUSTLINE authorized person that confirms the identity of the Subscriber using a well-recognized form of government issued identification and one other identification credential.

Class 3 Certificates issued to Organizations assure of the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so.

Class 3 Individual Certificates are appropriate for Digital Signatures, encryption, and access control in transactions requiring a high assurance about the Subscriber's identity.

Class 3 Server Certificates are appropriate for server authentication; message, software, and content integrity; and confidentiality encryption.

#### **1.1.4.4 TEST CERTIFICATES**

In addition to the three Classes of Certificates described above, MTNLTRUSTLINE also offers 'Test' certificates to its Subscribers.

These 'Test' certificates are solely intended for evaluating the technical implementation of MTNLTRUSTLINE PKI and ascertaining the interoperability of MTNLTRUSTLINE Certificates with various applications. 'Test' certificates shall not be used or relied upon for any other purposes.

MTNLTRUSTLINE shall disclaim all warranties whatsoever with respect to 'Test' Certificates and also disclaim any assurances of the accuracy, authenticity, integrity, or reliability of information contained in 'Test' Certificates.

MTNLTRUSTLINE shall require Subscribers and Users of 'Test' certificates to acknowledge that the identity of the Certificate Subject has not been authenticated for issuance of such 'Test' Certificates.

## **1.2 IDENTIFICATION**

This document is the MTNLTRUSTLINE Certificate Policy (CP) document and defines the Certificate Policies (CP) for MTNLTRUSTLINE issued three Classes of Certificates – Class 1, Class 2, and Class 3. The object identifiers assigned to this CP are:

1. MTNLTRUSTLINE CP (This Document) - 1.16.356.6865.754.0
2. MTNLTRUSTLINE Class 1 Certificates - 1.16.356.6865.754.1
3. MTNLTRUSTLINE Class 2 Certificates - 1.16.356.6865.754.2
4. MTNLTRUSTLINE Class 3 Certificates - 1.16.356.6865.754.3

The object identifiers used for End User Subscriber Certificates shall correspond to the appropriate Class.

## **1.3 COMMUNITY AND APPLICABILITY**

This CP governs the MTNLTRUSTLINE Public Key Infrastructure (PKI) that accommodates a large, public community of users with diverse needs for communications and information security. The participants in the MTNLTRUSTLINE PKI are:

1. Certifying Authorities (CAs)
2. Registration Authorities (RAs)
3. End entities
  - a) Subscribers
  - b) Relying Parties

### **1.3.1 CERTIFYING AUTHORITIES (CAs)**

The term Certifying Authority is an umbrella term that refers to all entities issuing Certificates within the MTNLTRUSTLINE PKI. The CA term encompasses two Sub-categories of issuers: Certifying Authority (CA) and Subordinate Certifying Authority (Sub-CA).

The MTNLTRUSTLINE CA is signed by the Root Certifying Authority of India (RCAI) and is at the top of the MTNLTRUSTLINE PKI hierarchy. Subordinate to the MTNLTRUSTLINE CA are Offline Subordinate Certifying Authorities (Offline Sub-CAs), one for each Class of Certificates. These Offline Sub-CAs issue Certificates to other Offline Sub-CAs or Online Sub-CAs. Online Sub-CAs issue Certificates to end entity Subscribers.

Sub-CAs also fall into two categories: MTNLTRUSTLINE Sub-CAs and MTNLTRUSTLINE Enterprise Customer Sub-CAs. MTNLTRUSTLINE Sub-CAs are MTNLTRUSTLINE entities whereas MTNLTRUSTLINE Enterprise Customer Sub-CAs are entities owned by MTNLTRUSTLINE Enterprise Customers.

### **1.3.2 REGISTRATION AUTHORITIES (RAs)**

Registration Authorities (RAs) evaluate and approve or reject Certificate Applications in accordance with this CP and relevant CPS.

MTNLTRUSTLINE PKI RAs fall into two categories: MTNLTRUSTLINE RAs and MTNLTRUSTLINE Enterprise Customer RAs. MTNLTRUSTLINE RAs are MTNLTRUSTLINE entities whereas MTNLTRUSTLINE Enterprise Customer RAs are MTNLTRUSTLINE Customer entities.

### **1.3.3 END ENTITIES**

#### **1.3.3.1 SUBSCRIBERS**

Subscribers are end entities identified in the subject name of a Certificate issued by a MTNLTRUSTLINE CA or Sub-CA. Subscribers hold the private key that corresponds to the Public Key listed in that Certificate.

In compliance with the requirements of the IT-Act this policy imposes a legal obligation upon the Subscriber to maintain the integrity of their private key(s).

#### **1.3.3.2 RELYING PARTIES**

Relying Parties are entities that rely on a Certificate(s) issued by MTNLTRUSTLINE in a manner consistent with this CP. A Relying Party is any entity using a MTNLTRUSTLINE PKI Certificate for one or a combination of the following:

1. To establish confidential communications with a Certificate Subscriber.
2. To verify a digital message was digitally signed by the Certificate Subscriber.
3. To verify the integrity of a digital message.
4. To authenticate the Certificate Subscriber in an online session based on proof of possession of the private key corresponding to the Public Key certified in the Digital Certificate.

### **1.3.4 APPLICABILITY**

The CP applies to all participants in the MTNLTRUSTLINE PKI - CAs, RAs, Subscribers, and Relying Parties. In general, Digital Certificates permit Subscribers to digitally sign electronic documents and permit Relying Parties to verify Digital Signatures.

The policies governing the use of each Class of Certificates in MTNLTRUSTLINE PKI is described in the next sub-section (CP § [1.3.4.1](#)). However, by contract and within specific environments (such as an intranet or an extranet), MTNLTRUSTLINE PKI participants may use Certificates for higher security applications than the ones described here. Any such usage, however, shall be limited to such entities, and subject to CP § [1.3.4.2](#) and CP § [1.3.4.3](#), and these entities shall be solely responsible for any liability arising out of such usage.

#### **1.3.4.1 SUITABLE APPLICATIONS**

The subsections within this section list suitable applications for each Class of MTNLTRUSTLINE PKI Certificates. This listing, however, is not intended to be exhaustive.

In general, MTNLTRUSTLINE PKI participants agree that where any transaction requires that information shall be authenticated by affixing the signature or any document shall be signed then such requirement shall be satisfied, if such information is authenticated by means of digital signature verifiable with reference to a suitable MTNLTRUSTLINE PKI Certificate.

##### **1.3.4.1.1 SUITABLE APPLICATIONS FOR CLASS 1 CERTIFICATES**

Class 1 Certificates are suitable for modestly enhancing the security of electronic communication through the use of Digital Signatures and encryption in transactions where proof of identity is not required.

A digital signature verifiable with reference to a MTNLTRUSTLINE Class 1 Certificate cannot be used for authentication purposes or to support non-repudiation as Class 1 Certificates do not assure about the identity of the Subscriber. Rather, the digital signature function is appropriate for providing continuity and integrity assurance in a series of ongoing communications.

Where used for e-mail, the digital signature also provides modest assurances that the e-mail originated from a sender with e-mail address mentioned in the subject Distinguished Name (DN) of the Certificate. The Certificate, however, provides no proof of who the sender(s) using that e-mail address actually is.

The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber, although the sending Relying Party cannot be sure that the recipient is in fact the person named in the Certificate.

Class 1 Certificates can also be used for client authentication during online sessions. The web site or other device can use the Certificate to ensure, over a series of sessions, that the sessions are being initiated by the same Subscriber having a certain e-mail address. Again, however, the Certificate provides no proof of who that Subscriber actually is.

#### 1.3.4.1.2 SUITABLE APPLICATIONS FOR CLASS 2 CERTIFICATES

Class 2 Certificates are suitable for moderately enhancing the security of electronic communication through the use of Digital Signatures and encryption in transactions where proof of identity of the Subscriber based on reliance on a MTNLTRUSTLINE approved business or consumer database(s) (Validating Database) is sufficient.

Where used for e-mail, the digital signature permits the authentication of the identity of email correspondents, message integrity, and support for non-repudiation.

The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber.

Class 2 Certificates are also appropriate for client authentication during online sessions.

In addition, Class 2 Certificates are also appropriate for enhancing the security of networks and other communication media by authenticating the identity/ownership of Devices.

#### 1.3.4.1.3 SUITABLE APPLICATIONS FOR CLASS 3 CERTIFICATES

Class 3 Certificates are suitable for enhancing the security of electronic communication through the use of Digital Signatures and encryption in transactions where a high assurance proof of identity is required.

Where used for e-mail, the digital signature permits the authentication of the identity of email correspondents, message integrity, and support for non-repudiation.

The encryption application enables a Relying Party to use the Subscriber's Certificate to encrypt messages to the Subscriber.

Class 3 Certificates are also appropriate for both client as well as server authentication during online sessions.

In addition, Class 3 Certificates are also appropriate for use with applications like time-stamping, OCSP, and software code signing.

#### 1.3.4.2 RESTRICTED APPLICATIONS

MTNLTRUSTLINE does not generally restrict the use of its PKI within any specific business environment.

With respect to X.509 version 3 Certificates, the key usage extension is intended to limit the technical purposes for which a private key corresponding to the Public Key in a Certificate may be used. In addition, End User Subscriber Certificates shall not be used as CA Certificates. This restriction is confirmed by the absence of a basic constraints extension. The effectiveness of extension-based limitations, however, is subject to the operation of software manufactured or controlled by entities other than MTNLTRUSTLINE.

### **1.3.4.3 PROHIBITED APPLICATIONS**

MTNLTRUSTLINE PKI Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapons control systems, where failure could lead directly to death, personal injury, or severe environmental damage. Also, subject to CP § [1.3.4.1.1](#), Class 1 Certificates shall not be used as proof of identity or for non-repudiation.

## **1.4 CONTACT DETAILS**

The organization responsible for the administration including registration, maintenance, and interpretation of this CP is Mahanagar Telephone Nigam Limited, with its registered office at:

**MAHANAGAR TELEPHONE NIGAM LIMITED  
JEEVAN BHARATI, 124 CONNAUGHT CIRCUS, NEW DELHI – 110 001  
TEL: +91 11 2374 2212, FAX: +91 11 2335 9425**

Address inquiries about the CP to [cp@mtnltrustline.com](mailto:cp@mtnltrustline.com) or to the following address:

**MTNLTRUSTLINE POLICY AND PROCEDURES COORDINATOR  
MAHANAGAR TELEPHONE NIGAM LIMITED  
JEEVAN BHARATI, 124 CONNAUGHT CIRCUS, NEW DELHI – 110 001  
TEL: +91 11 2374 2212, FAX: +91 11 2335 9425  
E-MAIL: CP@MTNLTRUSTLINE.COM**

## **2 GENERAL PROVISIONS**

### **2.1 OBLIGATIONS**

#### **2.1.1 CA OBLIGATIONS**

MTNLTRUSTLINE CAs shall ensure that all requirements, as detailed in this document, are implemented as applicable and perform the specific obligations described throughout this CP.

MTNLTRUSTLINE has the responsibility for conformance with this policy, IT-Act 2000, and other applicable laws of India, even when a part or whole of the CA functionality is undertaken by non MTNLTRUSTLINE entities.

MTNLTRUSTLINE shall make publicly available the Certification Practice Statement (CPS) describing the practices employed in issuing the Digital Certificates. All MTNLTRUSTLINE certification services shall be consistent with its published CPS.

MTNLTRUSTLINE shall maintain a Repository of all Certificates and CRLs in a X.500 compliant directory with LDAP access in accordance with the provisions of the IT-Act 2000.

MTNLTRUSTLINE shall update the 'National Repository of Digital Certificates' (NRDC) about the Issuance, Revocation, or suspension of a Digital Certificate in the manner and format agreed with the 'Controller of Certifying Authorities' (CCA).

MTNLTRUSTLINE shall use reasonable efforts to ensure that the Subscriber Agreement and Relying Party Agreement bind Subscribers and Relying Parties respectively. Examples of such efforts include, but are not limited to, requiring assent to Subscriber Agreement as a condition of enrollment or requiring assent to Relying Party Agreement as a condition of receiving Certificate status information. The Subscriber Agreement and Relying Party Agreement used by MTNLTRUSTLINE shall include the provisions required by CP §§ [2.2](#), [2.3](#), [2.4](#).

MTNLTRUSTLINE shall ensure appropriate technical and organizational measures are taken to prevent unauthorized or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.

MTNLTRUSTLINE must assure the users of its PKI that the information they provide is completely protected from disclosure unless with their agreement or by court order or other legal requirement.

MTNLTRUSTLINE shall make adequate arrangements to cover liabilities arising from its operations and/or activities, in particular to bear the risk of liability for damages.

MTNLTRUSTLINE shall ensure that organization concerned with Certificate generation and Revocation management shall be independent of other Organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides. Specifically, MTNLTRUSTLINE shall ensure that the organization concerned with Certificate generation and Revocation management shall have a documented structure which safeguards impartiality of operations.

### **2.1.2 RA OBLIGATIONS**

RAs assist MTNLTRUSTLINE PKI CAs and Sub-CAs by performing validation functions, approving or rejecting Certificate Applications, requesting Revocation of Certificates, and approving Renewal requests. MTNLTRUSTLINE PKI RAs shall perform the specific obligations appearing throughout this CP.

### **2.1.3 SUBSCRIBER OBLIGATIONS**

Certificate Applicants shall provide complete and accurate information on their Certificate Applications and shall manifest assent to the MTNLTRUSTLINE Subscriber Agreement as a condition of obtaining a Certificate.

Subscribers shall perform Subscriber functions in accordance with the specific obligations appearing throughout this CP. Subscribers shall use their Certificates in accordance with CP § [1.3.4](#).

Subscribers shall protect their private keys in accordance with CP §§ [6.1](#), [6.2](#), [6.4](#).

If a Subscriber discovers or has reason to believe there has been a compromise of the Subscriber's private key or the activation data protecting such private key, or the information within the Certificate is incorrect or has changed, the Subscriber shall promptly:

Notify the entity that approved the Subscriber's Certificate Application, either a MTNLTRUSTLINE PKI CA/Sub-CA or an RA, in accordance with CP § [4.4.1.1](#) and request Revocation of the Certificate in accordance with CP §§ [3.4](#), [4.4.3.1](#), and

Notify any person that may reasonably be expected by the Subscriber to rely on a digital signature verifiable with reference to the Subscriber's Certificate.

Subscribers shall cease use of their private keys at the end of their key usage periods under CP § [6.3.2](#).

Subscribers shall not intentionally compromise the security of the MTNLTRUSTLINE PKI.

#### **2.1.4 RELYING PARTY OBLIGATIONS**

Before any act of reliance, Relying Parties shall independently assess the appropriateness of the use of a Digital Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose.

MTNLTRUSTLINE is not responsible for assessing the appropriateness of the use of a Certificate. Relying Parties shall not use Certificates beyond the limitations in CP § [1.3.4.2](#) and for purposes prohibited in CP § [1.3.4.3](#).

Assuming that the use of the Certificate is appropriate, Relying Parties shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate chain and verifying the Digital Signatures on all Certificates in the Certificate chain. Relying Parties shall not rely on a Certificate unless these verification procedures are successful.

Relying Parties shall also check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate chain in accordance with CP §§ [4.4.10](#), [4.4.12](#). If any of the Certificates in the Certificate chain have been revoked, the Relying Party shall not rely on the End User Subscriber Certificate or other revoked Certificate in the Certificate chain.

Finally, Relying Parties must assent to the terms of MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement as a condition of using or otherwise relying on Digital Certificates.

If all of the checks described above are successful, the Relying Party shall be entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable under the circumstances.

If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable.

Relying Parties shall not intentionally compromise the security of the MTNLTRUSTLINE PKI.

### **2.1.5 REPOSITORY OBLIGATIONS**

In the MTNLTRUSTLINE PKI the Repository services are provided by MTNLTRUSTLINE.

## **2.2 LIABILITY**

### **2.2.1 CA LIABILITY**

MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall contain warranties, disclaimers, and limitations of liability listed below.

#### **2.2.1.1 WARRANTIES TO SUBSCRIBERS AND RELYING PARTIES**

MTNLTRUSTLINE shall warrant to Subscribers that:

There are no material misrepresentations of fact in the Digital Certificate known to or originating from MTNLTRUSTLINE or its Sub-CAs or RAs.

There are no errors in the information in the Digital Certificate that were introduced by MTNLTRUSTLINE or its Sub-CAs or its RAs while approving the Certificate Application or issuing the Digital Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Digital Certificate,

Their Digital Certificates meet all material requirements of this CPS, and

Revocation services and use of the Repository conform to this CPS in all material aspects.

MTNLTRUSTLINE shall warrant to Relying Parties who reasonably rely on a Digital Certificate that:

All information in or incorporated by reference in such Certificate, except non-verified Subscriber Information, is accurate,

In the case of Certificates appearing in the MTNLTRUSTLINE Repository, that the Certificate has been issued to the individual or organization named in the Certificate as the Subscriber, and that the Subscriber has accepted the Certificate in accordance with CPS § 4.3, and

The entities approving the Certificate Application and issuing the Certificate have substantially complied with this CPS when issuing the Certificate.

#### **2.2.1.2 DISCLAIMERS OF WARRANTIES**

To the extent permitted by applicable law, MTNLTRUSTLINE shall disclaim any warranty of fitness for a particular purpose, outside the context of its CPS.

#### **2.2.1.3 LIMITATIONS OF LIABILITY**

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall limit the liability to exclude indirect, special, incidental, and consequential damages. For a specific Digital Certificate the CA liability shall be limited to the following liability caps:

**Table 1: CA Liability Caps**

CLASS OF CERTIFICATE	CLASS 1	CLASS 2	CLASS 3
LIABILITY CAP	INR 1,000	INR 5,000	INR 15,000

**2.2.1.4 FORCE MAJEURE**

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall include a force majeure clause protecting MTNLTRUSTLINE.

**2.2.2 RA LIABILITY**

The warranties, disclaimers of warranty, limitations of liability, and force majeure clauses required by CP §§ [2.2.1.1](#), [2.2.1.2](#), [2.2.1.3](#), [2.2.1.4](#) also apply to all RAs in the MTNLTRUSTLINE PKI.

**2.2.3 SUBSCRIBER LIABILITY****2.2.3.1 SUBSCRIBER WARRANTIES**

MTNLTRUSTLINE Subscriber Agreement shall require Subscribers to warrant that:

Each digital signature created using the private key corresponding to the Public Key listed in the Digital Certificate is the digital signature of the Subscriber and the Digital Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,

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

All representations made by the Subscriber in the Certificate Application are true,

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

The Digital Certificate is being used exclusively for authorized and legal purposes, consistent with the applicable CPS, and

The Subscriber is an End User Subscriber and not a CA, and is not using the private key corresponding to any Public Key listed in the Digital Certificate for purposes of digitally signing any Digital Certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise.

#### **2.2.3.2 PRIVATE KEY COMPROMISE**

CP § [6.2.7.1](#) sets forth standards for the protection of the private keys of Subscribers compliant with the IT-Act 2000. MTNLTRUSTLINE Subscriber Agreement shall state that Subscribers failing to meet these standards are solely responsible for any loss or damage resulting from such failure.

#### **2.2.4 RELYING PARTY LIABILITY**

MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Digital Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in CP § [2.1.4](#).

### **2.3 FINANCIAL RESPONSIBILITY**

#### **2.3.1 INDEMNIFICATION BY SUBSCRIBERS AND RELYING PARTIES**

##### **2.3.1.1 INDEMNIFICATION BY SUBSCRIBERS**

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement shall require Subscribers to indemnify MTNLTRUSTLINE for:

Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,

Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,

The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or

The Subscriber's use of a name (including without limitation within a common name, domain name, or e- mail address) that infringes upon the Intellectual Property Rights of a third party.

### **2.3.1.2 INDEMNIFICATION BY RELYING PARTIES**

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall require Relying Parties to indemnify MTNLTRUSTLINE for:

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

The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or

The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

### **2.3.2 FIDUCIARY RELATIONSHIPS**

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall disclaim any fiduciary relationship between MTNLTRUSTLINE or MTNLTRUSTLINE Enterprise Customer RA or MTNLTRUSTLINE Enterprise Customer Sub-CA on one hand and a Subscriber or Relying Party on the other hand.

### **2.3.3 ADMINISTRATIVE PROCESSES**

MTNLTRUSTLINE shall have sufficient financial resources to maintain the integrity of its PKI, and must be reasonably able to bear the risk of liability to Subscribers and Relying Parties. MTNLTRUSTLINE shall also maintain a reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self- insured retention.

## **2.4 INTERPRETATION AND ENFORCEMENT**

### **2.4.1 GOVERNING LAW**

The Information Technology Act, 2000, Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001 or any subsequent updates shall govern the validity of this CP, the construction of its terms, and the interpretation and enforcement of the rights and duties of the parties hereto.

### **2.4.2 SEVERABILITY, SURVIVAL, MERGER, NOTICE**

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement shall contain severability, survival, merger, and notice clauses.

### **2.4.3 DISPUTE RESOLUTION PROCEDURES**

To the extent permitted by applicable law, disputes among MTNLTRUSTLINE, Customers, End User Subscribers or Relying Parties shall be resolved pursuant to provisions in the applicable agreements among the parties.

#### **2.4.3.1 ROLE OF THE CCA**

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

## **2.5 FEES**

### **2.5.1 CERTIFICATE ISSUANCE OR RENEWAL FEES**

MTNLTRUSTLINE is entitled to charge End User Subscribers for the Issuance, Renewal, and Replacement of Digital Certificates.

### **2.5.2 CERTIFICATE ACCESS FEES**

MTNLTRUSTLINE shall not charge a fee as a condition of making a Certificate available in its Repository or otherwise making Certificates available to Relying Parties. However, MTNLTRUSTLINE reserves the right to amend this policy and charge such fees in future.

### **2.5.3 REVOCATION OR STATUS INFORMATION ACCESS FEES**

MTNLTRUSTLINE shall not charge a fee as a condition of making the CRLs required by CPS § 4.4.9 available in a Repository or otherwise available to Relying Parties. However, MTNLTRUSTLINE reserves the right to amend this policy and charge such fees in future.

MTNLTRUSTLINE is entitled to charge a fee for providing OCSF services, or other value-added Revocation and status information services.

### **2.5.4 FEES FOR OTHER SERVICES SUCH AS POLICY INFORMATION**

MTNLTRUSTLINE shall not charge a fee for on-line access to this CP or the CPS.

MTNLTRUSTLINE is entitled to charge a reasonable fee for providing a printed copy of this CP or the CPS.

### **2.5.5 REFUND POLICY**

To the extent permitted by applicable law MTNLTRUSTLINE shall implement a refund policy and publish it within its web sites in addition to placing it in the Subscriber Agreements and the CPS.

## **2.6 PUBLICATION AND REPOSITORIES**

### **2.6.1 PUBLICATION OF CA INFORMATION**

MTNLTRUSTLINE shall be responsible for publishing Certificates and CRLs in its Repository.

MTNLTRUSTLINE CPS, Subscriber Agreement, Relying Party Agreement and this CP shall be published in the MTNLTRUSTLINE web sites.

MTNLTRUSTLINE shall publish the URL of the applicable Relying Party Agreement within each Certificate it issues in accordance with CP §§ [3.1.1](#), [7.1.6](#), [7.1.8](#).

### **2.6.2 FREQUENCY OF PUBLICATION**

Relevant information shall be published promptly after it is available to MTNLTRUSTLINE. The CPS shall contain provisions relating to amendments, and CPS changes shall be published in accordance with such provisions.

CP §§ [4.4.9](#), [4.4.11](#) govern the frequency of the publication of Certificate status information.

### **2.6.3 ACCESS CONTROLS**

MTNLTRUSTLINE shall not intentionally use technical means of limiting access to this CP, the CPS, Certificates, Certificate status information, or CRLs. MTNLTRUSTLINE shall, however, require persons to agree to the Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs.

MTNLTRUSTLINE shall implement controls to prevent unauthorized persons from adding, deleting, or modifying Repository entries.

### **2.6.4 REPOSITORIES**

In the MTNLTRUSTLINE PKI the Repository services are provided by MTNLTRUSTLINE.

## **2.7 COMPLIANCE AUDIT**

MTNLTRUSTLINE shall perform regular audits in compliance with the requirements of the IT-Act 2000, and its associated rules and regulations. These audits shall be performed by an auditor empanelled with the Controller of Certifying Authorities (CCA).

In addition MTNLTRUSTLINE shall perform monthly self-audits.

### **2.7.1 FREQUENCY OF COMPLIANCE AUDIT**

Thorough statutory compliance audits shall be conducted annually in addition to quarterly and half-yearly audits.

## **2.7.2 IDENTITY/ QUALIFICATIONS OF AUDITOR**

Only a third party certified public auditing firm, empanelled by the Controller of Certifying Authorities (CCA), can perform the compliance audits of MTNLTRUSTLINE. MTNLTRUSTLINE auditors' possess demonstrated expertise in computer security and in the performance of IT security and PKI compliance audits.

### **2.7.2.1 SELF-AUDITS**

Self-audits shall be performed by a person within MTNLTRUSTLINE that is hierarchically independent of the system Administrators, network Administrators, PKI Administrators, or other Administrators performing CA/RA functions.

## **2.7.3 AUDITOR'S RELATIONSHIP TO AUDITED PARTY**

Compliance audits performed by third-party audit firms shall be conducted by firms independent of MTNLTRUSTLINE. Such firms shall not have a conflict of interest that hinders their ability to perform auditing services. With respect to self-audits, see CP § [2.7.2.1](#).

## **2.7.4 TOPICS COVERED BY AUDIT**

Compliance audit shall involve an examination of all procedures and operations of MTNLTRUSTLINE for compliance with the IT-Act 2000, the CPS and this CP.

The monthly self-audits shall focus on Subscriber validation and system administration.

The quarterly audits shall focus on the Repository.

The half-yearly audits shall focus on the security policy, physical security, and planning of MTNLTRUSTLINE operations.

The annual audits shall include:

1. Security policy and planning
2. Physical security
3. Technology evaluation

4. CA services administration
5. Compliance to MTNLTRUSTLINE CP & CPS
6. Contracts and agreements
7. Regulations prescribed by the controller
8. Policy requirements of Certifying Authority Rules, 2000
9. Changes/additions in physical controls such as site location, access, etc.
10. Re-deployment of personnel from an approved role/task to a new one
11. Appropriate security clearances for outgoing employees such as deletion of keys and revocation of access privileges

#### **2.7.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY**

After receiving a report based on the Compliance Audit, MTNLTRUSTLINE shall, in good faith, use reasonable efforts to work out a corrective action plan for correcting any identified problems or deficiencies and to implement the plan.

#### **2.7.6 COMMUNICATIONS OF RESULTS**

Results of the compliance audit of MTNLTRUSTLINE shall be submitted to the CCA and may be released to any other party at the discretion of MTNLTRUSTLINE management.

### **2.8 CONFIDENTIALITY POLICY**

MTNLTRUSTLINE shall implement a privacy policy in conforming to applicable laws. Specifically, MTNLTRUSTLINE and its RAs shall not disclose or sell the names of Certificate Applicants or other identifying information about them, subject to CP § 2.8.2 and the right of a terminating CA to transfer such information to a successor CA under CP § 4.9.

### **2.8.1 TYPES OF INFORMATION TO BE KEPT CONFIDENTIAL**

The following information shall, subject to CP § [2.8.2](#), be kept confidential ("Confidential Information"):

CA application records, whether approved or disapproved,

Certificate Application records (subject to CP § [2.8.2](#)),

Transactional records (both full records and the audit trail of transactions),

Audit trail records created or retained by MTNLTRUSTLINE,

Audit reports created by MTNLTRUSTLINE internal and external auditors

Contingency plans and disaster recovery plans and

Security measures controlling the operations of MTNLTRUSTLINE hardware and software and the administration of PKI services and designated Certificate Application services.

### **2.8.2 TYPES OF INFORMATION NOT CONSIDERED CONFIDENTIAL**

Digital Certificates, Certificate Revocation Lists and other Certificate status information, MTNLTRUSTLINE Repository, and information contained within them are not considered confidential information. Information not expressly deemed confidential information under CPS § [2.8.1](#) shall not be considered confidential.

### **2.8.3 DISCLOSURE OF CERTIFICATE REVOCATION/SUSPENSION INFORMATION**

Public Information as per CP § [2.8.2](#)

### **2.8.4 RELEASE TO LAW ENFORCEMENT OFFICIALS**

MTNLTRUSTLINE PKI participants shall acknowledge that MTNLTRUSTLINE is entitled to disclose confidential information if, in good faith, MTNLTRUSTLINE believes disclosure is necessary in response to order from a court or tribunal or any government or public authority having the power to compel the disclosure.

### **2.8.5 RELEASE AS PART OF CIVIL DISCOVERY**

MTNLTRUSTLINE PKI participants shall acknowledge that MTNLTRUSTLINE is entitled to disclose confidential information if MTNLTRUSTLINE is called upon to make such disclosure in response to judicial, administrative, or other legal process during any judicial, arbitration, litigation or administrative proceedings. MTNLTRUSTLINE shall make reasonable efforts to protect the disclosed information by restricting the disclosure of the information to the extent reasonably required by any such judicial, arbitration, litigation or administrative proceedings.

### **2.8.6 DISCLOSURE UPON OWNER'S REQUEST**

Privacy policies established pursuant to CP § [2.8](#) shall contain provisions relating to the disclosure of confidential information to the person disclosing it to MTNLTRUSTLINE.

### **2.8.7 OTHER INFORMATION RELEASE CIRCUMSTANCES**

No stipulation.

## **2.9 INTELLECTUAL PROPERTY RIGHTS**

### **2.9.1 RIGHTS IN CERTIFICATES**

MTNLTRUSTLINE retains all Intellectual Property Rights in and to the Certificates and Revocation information that it issues. MTNLTRUSTLINE shall grant permission to freely reproduce and distribute Certificates and Revocation information, provided that they are reproduced in full and their use is subject to the Relying Party Agreement.

### **2.9.2 RIGHTS IN THE CP & CPS**

MTNLTRUSTLINE retains all Intellectual Property Rights in and to this CP and the MTNLTRUSTLINE CPS.



### **2.9.3 RIGHTS IN NAMES**

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

### **2.9.4 RIGHTS IN KEYS AND KEY MATERIAL**

Key pairs corresponding to Certificates of CAs, Sub-CAs, and End User Subscribers are the property of the CAs, Sub-CAs, and End User Subscribers that are the respective subjects of these Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all intellectual property rights in and to these key pairs.

Secret Shares of a CA or Sub-CA's private key are the property of the CA or Sub-CA who retains all intellectual property right in and to such secret shares.

## **3 IDENTIFICATION AND AUTHENTICATION**

### **3.1 INITIAL REGISTRATION**

#### **3.1.1 TYPES OF NAMES**

End User Subscriber Digital Certificates shall contain an X.501 distinguished name (DN) in the subject name field.

Class 1 Certificates shall include an authenticated e-mail address (E) attribute in the subject distinguished name.

Class 2 and Class 3 Certificates shall include an authenticated common name (CN) attribute in the subject distinguished name.

Class 2 and Class 3 Certificates may contain an authenticated organization name (O) attribute in the subject distinguished name.

All End User Certificates may contain a serial number (SN) attribute in the subject distinguished name.

In addition, all End User Certificates may contain other authenticated attributes required to determine the identity of the Subscriber.

#### **3.1.2 MEANING OF NAMES**

End User Subscriber Digital Certificates shall include subject distinguished names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the subject of the Certificate.

For Certificates issued to Individuals the common name (CN) attribute shall represent the individual's generally accepted personal name. For Certificates issued to Devices this common name shall either be a domain name (for server Certificates) or the legal name of the organization, or unit within the organization or any other name identifying the device and legally owned or assigned to the organization.

The organization name (O) attribute type shall, when present in the subject distinguished name, represent the legal name of the Subscriber organization. This shall be used to only to determine the identity of the Subscriber and shall not imply any power-of-attorney or other rights.

The serial number (SN) attribute type shall, when present in the subject distinguished name, be used to distinguish the identity of the Subscriber. This attribute has no defined semantics beyond ensuring uniqueness of subject names. It may contain a number or code assigned by MTNLTRUSTLINE or an identifier assigned by a government or civil authority.

### **3.1.3 RULES FOR INTERPRETING VARIOUS NAME FORMS**

No stipulation.

### **3.1.4 UNIQUENESS OF NAMES**

The subject distinguished name listed in a Certificate shall be unambiguous and unique for all Certificates issued within the MTNLTRUSTLINE PKI, and conform to X.500 standards for name uniqueness.

### **3.1.5 NAME CLAIM DISPUTE RESOLUTION**

Certificate Applicants shall not use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

However, MTNLTRUSTLINE shall not be required to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark.

MTNLTRUSTLINE shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

### **3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS**

See CP § [3.1.5](#).

### **3.1.7 METHOD TO PROVE POSSESSION OF PRIVATE KEY**

The method to prove possession of a private key shall be PKCS #10 or another cryptographically equivalent and MTNLTRUSTLINE approved demonstration.

### **3.1.8 AUTHENTICATION OF ORGANIZATION IDENTITY**

#### **3.1.8.1 AUTHENTICATION OF ORGANIZATION IDENTITY**

MTNLTRUSTLINE shall require all its RAs to confirm the identity of an organization, before issuing a Digital Certificate with the name of the organization in the subject distinguished name, in accordance with the procedures set forth below:

- » Determine that the organization exists by using organizational documentation issued by or filed with the applicable government that confirms the existence of the organization,
- » Confirm with an appropriate organizational contact by telephone, registered post, or comparable procedure certain information about the organization, that the organization has authorized the Certificate Application and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so.

In addition to the procedures above, the Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the Public Key to be listed in the Certificate in accordance with CPS § 3.1.7.

#### **3.1.8.2 CLASS 2 CERTIFICATES FOR DEVICES**

The authentication of Devices for Class 2 device Certificates shall consist of authenticating the existence of the organization pursuant to CP § 3.1.8.1. MTNLTRUSTLINE shall also, during such authentication process, confirm that the appropriate name(s) identifying the device(s) is legally owned by or assigned to the organization. Where it is not possible to confirm the legal right of the organization to the device names, confirm that the organization's use of such names does not conflict with generally accepted standards.

In addition, MTNLTRUSTLINE shall also confirm that the Certificate Applicant has taken reasonable measures to ensure the security of the device's private key.

### **3.1.8.3 CLASS 3 SERVER CERTIFICATES**

The authentication of Servers for Class 3 server Certificates shall consist of authenticating the existence of the organization pursuant to CP § [3.1.8.1](#). MTNLTRUSTLINE shall also, during such authentication process, determine that the organization is the record owner of the domain name(s) that is the subject of the Certificate or is otherwise authorized to use the domain name(s).

In addition, MTNLTRUSTLINE shall also confirm that the Certificate Applicant has taken reasonable measures to ensure the security of the server's private key.

### **3.1.8.4 AUTHENTICATION OF THE IDENTITY OF SUB-CAs AND RAs**

MTNLTRUSTLINE organizational Customers, before becoming Sub-CAs or RAs, shall enter into an agreement with MTNLTRUSTLINE.

MTNLTRUSTLINE shall authenticate the identity of the prospective Sub-CA or RA Customer before final approval of its status as Sub-CA or RA. This shall be confirmed by requiring the personal appearance of an authorized representative of the organization before authorized personnel of MTNLTRUSTLINE.

The checks required for the confirmation of the organization identity under CP § [3.1.8.1](#) shall also be performed, except that instead of a Certificate Application, the validation is of an application to become a Sub-CA or RA. Also, MTNLTRUSTLINE shall confirm that the person identified as an Administrator is authorized to act in the capacity.

### **3.1.9 AUTHENTICATION OF INDIVIDUAL IDENTITY**

MTNLTRUSTLINE shall require all its RAs to confirm the identity of an individual, before issuing a Digital Certificate, in accordance with the procedures of authentication set forth in this CP § [3.1.9](#) for each Class of Certificate.

The authentication procedures in common for all Class of Certificates shall include:

- » Verifying that the Certificate Applicant is the person identified in the Certificate Application (except for Certificate Applicants for Class 1 Certificates - CP § [3.1.9.1](#)),

- » Establishing that the Certificate Applicant rightfully holds the private key corresponding to the Public Key to be listed in the Certificate in accordance with CP § [3.1.7](#), and
- » Confirming that the information to be listed in the Certificate is accurate.

These procedures are in addition to the more detailed procedures described below for each Class of Certificate.

#### **3.1.9.1 CLASS 1 CERTIFICATES**

Authentication of Individuals for Class 1 Certificates shall consist of a check to ensure that the subject distinguished name is a unique and unambiguous subject name within the MTNLTRUSTLINE Class 1 Repository and only a limited confirmation of the Certificate Applicant's e- mail address.

MTNLTRUSTLINE shall not authenticate the identity of the Class 1 Certificate Applicant. As a result, the Certificate Applicant's own personal name shall not appear in the subject name of the Certificate. Instead the Certificates Subscriber Distinguished Name may be populated with a generic Common Name (CN).

#### **3.1.9.2 CLASS 2 CERTIFICATES**

Authentication of Individuals or Devices for Class 2 Certificates shall consist of determining if identifying information in the Certificate Application matches information residing in MTNLTRUSTLINE approved and well-recognized business or consumer database(s) (Validating Database). If the information in the Certificate Application matches the information in the database, MTNLTRUSTLINE or any of its RA may approve the Certificate.

MTNLTRUSTLINE may provide its RAs with an optional software module for automatic approval and Revocation of users or Devices directly from pre-existing databases, rather than requiring manual authentication for each Certificate Application. RA's using software to automate the processing of Certificate requests shall authenticate the identity of potential Certificate Applications before placing their information in the Validating Database.

### **3.1.9.3 CLASS 3 CERTIFICATES**

The authentication of Class 3 individual Certificates is based on the personal (physical) presence of the Certificate Applicant before an agent of MTNLTRUSTLINE, or before a notary public or other official with comparable authority as notified by MTNLTRUSTLINE from time to time. The agent, notary or other official shall check the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a passport, PAN card, or driver's license and one other identification credential.

The authentication of Administrators for Class 3 Administrator Certificates shall consist of authenticating the existence of the Administrator's employer and confirming the employment and authorization of the person named as Administrator. MTNLTRUSTLINE shall authenticate Certificate Applications first by authenticating the identity of the entity employing or retaining the Administrator pursuant to CP § 3.1.8.1. Such entity shall either be a MTNLTRUSTLINE Enterprise Customer RA or a MTNLTRUSTLINE Enterprise Customer Sub-CA. MTNLTRUSTLINE shall also, during such authentication process, confirm the authorization of the Certificate Applicant to act as Administrator.

## **3.2 ROUTINE REKEY (RENEWAL)**

### **3.2.1 RENEWAL OF END USER SUBSCRIBER CERTIFICATES**

MTNLTRUSTLINE shall require its RAs to authenticate a request for Renewal before approving a Certificate Renewal for the Subscriber of an End User Subscriber Certificate. MTNLTRUSTLINE approved Renewal procedures shall ensure that the person or organization seeking to renew an end- user Subscriber Certificate is in fact the Subscriber of the Certificate.

Other than MTNLTRUSTLINE approved Renewal procedure, the requirements for the authentication of an original Certificate Application in CP §§ 3.1.8, 3.1.9 shall be used for renewing an End User Subscriber Certificate.

### **3.2.2 RENEWAL OF SUB-CA CERTIFICATES**

A Sub-CAs superior entity approving an application for a Sub-CA Certificate shall be responsible for authenticating a request for Renewal. Renewal procedures shall ensure that an organization seeking to renew the Sub-CA Certificate is in fact the Subscriber of the Sub-CA Certificate. Authentication procedures shall be the same as original enrollment pursuant to CP § [3.1.8.4](#).

### **3.3 REKEY AFTER REVOCATION - NO KEY COMPROMISE**

MTNLTRUSTLINE shall not permit Renewal after Revocation if Revocation occurred because the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the subject of such Certificate, or the RA approving the Subscriber's Certificate Application discovers or has reason to believe that a material fact in the Certificate Application is false.

Subject to the foregoing paragraph, Renewal of an organizational or Sub-CA Certificate following Revocation of the Certificate is permissible as long as Renewal procedures ensure that the organization or Sub-CA seeking Renewal is in fact the Subscriber of the Certificate. Renewed organizational Certificates shall contain the same subject distinguished name as the subject distinguished name of the organizational Certificate being renewed.

Renewal of an individual Certificate following Revocation again must ensure that the person seeking Renewal is, in fact, the Subscriber. Other than MTNLTRUSTLINE approved Renewal procedure, the requirements for the validation of an original Certificate Application in CP §§ [3.1.8](#), [3.1.9](#) shall be used for renewing a Certificate following Revocation.

### **3.4 REVOCATION REQUESTS**

MTNLTRUSTLINE Revocation procedures shall ensure prior to any Revocation of any Certificate that the Revocation has in fact been requested by the Certificate's Subscriber or the RA that approved the Certificate Application. Acceptable procedures for authenticating the Revocation requests of a Subscriber shall include:

Having the Subscriber submit the Subscriber's challenge phrase, and revoking the Certificate automatically if it matches the challenge phrase on record,

Receiving a message purporting to be from the Subscriber that requests Revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and

Communication with the Subscriber providing reasonable assurances in light of the Class of Certificate that the person or organization requesting Revocation is, in fact the Subscriber. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e- mail, postal mail, or courier service.

## **4 OPERATIONAL REQUIREMENTS**

### **4.1 CERTIFICATE APPLICATION**

#### **4.1.1 ENROLLMENT FOR END USER SUBSCRIBER CERTIFICATES**

MTNLTRUSTLINE shall ensure that Subscribers all End User Certificate Applicants undergo an enrollment process consisting of:

Completing a Certificate Application and providing the requested information and evidence,

Generating, or arranging to have generated, a key pair in accordance with CP § [6.1](#) and ensure reasonable precautions to protect the private key from compromise in accordance with CP §§ [6.1](#), [6.2](#), [6.4](#).

The Certificate Applicant delivering his, her, or its Public Key to MTNLTRUSTLINE in accordance with CP § [6.1.3](#),

Demonstrating to MTNLTRUSTLINE pursuant to CP § [3.1.7](#) that the Certificate Applicant has possession of the private key corresponding to the Public Key submitted for certification, and

Manifesting assent to the MTNLTRUSTLINE Subscriber Agreement and accepting applicable terms and conditions regarding use of Certificates.

Certificate Applications shall be submitted either to a MTNLTRUSTLINE RA or web-RA.

#### **4.1.2 ENROLLMENT FOR SUB-CA OR RA CERTIFICATES**

MTNLTRUSTLINE does not require Sub-CA or RA Certificate Subscribers, to complete formal Certificate Applications. Instead, they enter into a contract with MTNLTRUSTLINE pursuant to CP § [3.1.8.4](#). Sub-CA and RA applicants shall provide their credentials as required by CP § [3.1.8.4](#) to demonstrate their identity.

## **4.2 CERTIFICATE ISSUANCE**

### **4.2.1 ISSUANCE OF END USER SUBSCRIBER CERTIFICATES**

After a Certificate Applicant submits a Certificate Application, the MTNLTRUSTLINE RA receiving the Certificate Application (CP § [4.1.1](#)) shall validate or refute the information in the Certificate Application pursuant to CP §§ [3.1.8](#), [3.1.9](#). Upon successful performance of all required authentication procedures pursuant to CP § [3.1](#), the RA receiving the Certificate Application shall approve the Certificate Application. If authentication is unsuccessful, the RA receiving the Certificate Application shall reject the Certificate Application.

A Certificate shall be created and issued following the approval of a Certificate Application by an RA.

The procedures of this section shall also be used for the Issuance of Certificates in connection with the submission of a request to renew the Certificate.

### **4.2.2 ISSUANCE OF SUB-CA AND RA CERTIFICATES**

MTNLTRUSTLINE shall authenticate the identity of entities wishing to become Sub-CA's or RA's as per CP § [3.1.8.4](#) and, if approved, issue the Certificates needed to perform their Sub-CA or RA functions in accordance with CP § [6.1](#).

MTNLTRUSTLINE shall ensure that before a contract is entered into with the Sub-CA or RA applicant under CP § [4.1.2](#), the identity of the potential Sub-CA or RA shall be confirmed based on the credentials it presents. The execution of such a contract shall indicate the complete and final approval of the application by MTNLTRUSTLINE.

The decision to approve or reject a Sub-CA or RA application shall be solely at the discretion of MTNLTRUSTLINE.

## **4.3 CERTIFICATE ACCEPTANCE**

MTNLTRUSTLINE shall, either directly or through an RA, notify Subscribers about the creation of the Subscriber's Digital Certificates, and provide the Subscribers with access to the Certificates by notifying them that their Certificates are available and notifying them of the means for obtaining them.

Upon Issuance, Certificates shall be made available to End User Subscribers, either by allowing them to receive the Certificate in person from an RA, or allowing them to download their Certificate from a web site or via a message sent to the Subscriber containing the Certificate.

Receiving a Certificate from an RA, or downloading a Certificate, or installing a Certificate from a message attaching it shall constitute the Subscriber's Acceptance of the Certificate.

## **4.4 CERTIFICATE SUSPENSION AND REVOCATION**

### **4.4.1 CIRCUMSTANCES FOR REVOCATION**

#### **4.4.1.1 CIRCUMSTANCES FOR REVOKING END USER SUBSCRIBER CERTIFICATES**

MTNLTRUSTLINE promptly revokes an End User Subscriber Certificate if:

1. The RA approving the Subscriber's Certificate Application has reason to believe that there has been a compromise of the Subscriber's private key,
2. The RA approving the Subscriber's Certificate Application has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CPS and the MTNLTRUSTLINE CP,
3. The RA approving the Subscriber's Certificate Application determines that the Certificate (other than a Class 1 Certificate) was issued to a person other than the one named as the subject of the Certificate, or the Certificate (other than a Class 1 Certificate) was issued without the authorization of the person named as the subject of such Certificate,

4. The RA approving the Subscriber's Certificate Application has reason to believe that a material fact in the Certificate Application is false,
5. The RA approving the Subscriber's Certificate Application determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived,
6. The information within the Certificate is incorrect or has changed,
7. In the case of organizational Certificates, the Subscriber's organization name changes,
8. The Subscriber has materially breached a material obligation, representation, or warranty under the applicable Subscriber Agreement,
9. The Subscriber Agreement with the Subscriber has been terminated, or
10. The Subscriber requests Revocation of the Certificate in accordance with CP § 3.4.

An Administrator Certificate shall also be revoked if the authority of the Administrator Subscriber of the Certificate to act as Administrator has been terminated or otherwise has been ended.

#### **4.4.1.2 CIRCUMSTANCES FOR REVOKING SUB-CA OR RA CERTIFICATES**

MTNLTRUSTLINE shall ensure that a Sub-CA or RA Certificate is promptly revoked if:

1. MTNLTRUSTLINE discovers or has reason to believe that there has been a compromise of the Sub-CA or RA private key,
2. The agreement between MTNLTRUSTLINE and the Sub-CA or RA has been terminated,
3. MTNLTRUSTLINE discovers or has reason to believe that the Certificate was issued in a manner not materially in accordance with the procedures required by this CP and the applicable CPS,

4. MTNLTRUSTLINE discovers that the Certificate was issued to an entity other than the one named as the subject of the Certificate, or the Certificate was issued without the authorization of the entity named as the subject of such Certificate,
5. MTNLTRUSTLINE determines that a material prerequisite to Certificate Issuance was neither satisfied nor waived, or
6. The Sub-CA or RA requests Revocation of the Certificate.

#### **4.4.2 WHO CAN REQUEST REVOCATION**

##### **4.4.2.1 WHO CAN REQUEST REVOCATION OF AN END USER SUBSCRIBER CERTIFICATE**

The only parties permitted to request Revocation of a Certificate issued pursuant to this policy shall be the individual Subscribers for their own individual Certificate, a duly authorized representative of the organization for organizational Certificates, or the RA that approved the Subscriber's Certificate Application.

##### **4.4.2.2 WHO CAN REQUEST REVOCATION OF A SUB-CA OR RA CERTIFICATE**

Only MTNLTRUSTLINE is entitled to request or initiate the Revocation of the Certificates issued to its own CAs, Sub-CAs, and RAs.

Non-MTNLTRUSTLINE Sub-CAs and RAs shall be entitled, through their duly authorized representatives, to request the Revocation of their own Certificates. MTNLTRUSTLINE shall also be entitled to request or initiate the Revocation of Non-MTNLTRUSTLINE Sub-CAs and RAs Certificates.

#### **4.4.3 PROCEDURE FOR REVOCATION REQUEST**

##### **4.4.3.1 PROCEDURE FOR REVOCATION REQUEST OF AN END USER SUBSCRIBER CERTIFICATE**

MTNLTRUSTLINE shall ensure that End User Subscriber Certificates are revoked in a timely manner based on authorized and validated Certificate Revocation requests.

An End User Subscriber or duly authorized representative, as applicable, requesting Revocation shall communicate the request to the RA that approved the Subscriber's Certificate Application. Such communication shall be in accordance with CP § 3.4. Upon receiving a valid Revocation request the RA shall promptly revoke the Certificate and notify the Subscriber about the Certificate Revocation.

A MTNLTRUSTLINE RA revoking an End User Subscriber Certificate upon its own initiative shall do so pursuant to CP § 3.4.

#### **4.4.3.2 PROCEDURE FOR REVOCATION REQUEST OF A SUB-CA OR RA CERTIFICATE**

A Sub-CA or RA requesting Revocation shall communicate the request to MTNLTRUSTLINE. Upon receiving a valid Revocation request MTNLTRUSTLINE shall promptly revoke that Certificate and notify the requester about the successful Revocation. In case of the Revocation of a Sub-CA, MTNLTRUSTLINE shall also notify the concerned RAs about the Sub-CA Revocation.

MTNLTRUSTLINE revoking a Sub-CA or RA Certificate upon its own initiative shall initiate Revocation in the same manner.

#### **4.4.4 REVOCATION REQUEST GRACE PERIOD**

The party requesting a Revocation shall do so as promptly as possible, but no later than within a reasonable time.

#### **4.4.5 CIRCUMSTANCES FOR SUSPENSION**

MTNLTRUSTLINE PKI does not at present offer suspension services for End User Subscriber Certificates.

#### **4.4.6 WHO CAN REQUEST SUSPENSION**

Not applicable.

#### **4.4.7 PROCEDURE FOR SUSPENSION REQUEST**

Not applicable.

#### **4.4.8 LIMITS ON SUSPENSION PERIOD**

Not applicable.

#### **4.4.9 CRL ISSUANCE FREQUENCY**

MTNLTRUSTLINE offers CRLs showing the Revocation of MTNLTRUSTLINE PKI Digital Certificates and offers status checking services through the MTNLTRUSTLINE PKI Repository.

MTNLTRUSTLINE shall update and publish the CRLs for End User Subscriber Certificates whenever an End User Subscriber Certificate is revoked, and at least every 24 hours, even if no changes to the CRLs have been made.

MTNLTRUSTLINE shall update and publish CRLs for Sub-CA Certificates whenever a Sub-CA Certificate is revoked and at least quarterly even if no changes to the CRLs have been made.

If a Certificate listed in a CRL expires, it shall be removed from later-issued CRLs starting thirty (30) days after the Certificate's expiration.

#### **4.4.10 CERTIFICATE REVOCATION LIST CHECKING REQUIREMENTS**

Relying Parties shall check the status of Certificates on which they wish to rely by referring to the most recent CRL from the CA/Sub-CA that issued the Certificate on which the Relying Party wishes to rely.

MTNLTRUSTLINE shall provide Relying Parties with information on how to find the appropriate CRL to check for Revocation status by publishing the URI to the appropriate CRL in the Digital Certificate.

#### **4.4.11 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY**

MTNLTRUSTLINE PKI does not at present offer OCSP services for End User Subscriber Certificates.

MTNLTRUSTLINE publishes all CRLs to its Repository which is available online and can be accessed using the LDAP or LDAPS or HTTP or HTTPS protocols.

#### **4.4.12 ON-LINE REVOCATION CHECKING REQUIREMENTS**

No stipulation.

#### **4.4.13 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE**

No stipulation.

#### **4.4.14 CHECKING REQUIREMENTS FOR OTHER FORMS OF REVOCATION ADVERTISEMENTS**

No stipulation.

#### **4.4.15 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE**

MTNLTRUSTLINE PKI participants shall be notified of an actual or suspected CA/Sub-CA private key compromise using reasonable efforts. MTNLTRUSTLINE shall use reasonable efforts to notify potential Relying Parties if they discover, or have reason to believe, that there has been a compromise of the private key of one of the CAs or one of the Sub-CAs within the MTNLTRUSTLINE PKI hierarchy.

### **4.5 SECURITY AUDIT PROCEDURES**

#### **4.5.1 TYPES OF EVENTS RECORDED**

MTNLTRUSTLINE shall ensure that all relevant information concerning its PKI is recorded for an appropriate period of time, as specified in the IT-ACT. The types of auditable events that must be recorded by each entity are set forth below. All logs, whether electronic or manual, shall contain the date and time of the event, and the identity of the entity that caused the event. MTNLTRUSTLINE shall ensure that the integrity of current and archived records is maintained.

##### **4.5.1.1 EVENTS RECORDED BY MTNLTRUSTLINE CA**

MTNLTRUSTLINE shall record in audit log files significant events in the MTNLTRUSTLINE system such as:

1. System start-up and shutdown,

2. CA application start-up and shutdown,
3. Attempts to create, remove, set passwords or change the system privileges of the privileged users,
4. Generation of a CA's and Sub-CA key pairs,
5. Changes to CA/Sub-CA details and/or keys,
6. Changes to Certificate creation policies,
7. Login and logoff attempts,
8. Unauthorized attempts at network access to the CA system,
9. Unauthorized attempts to access system files,
10. End User Subscriber Certificate Application, Issuance, Revocation, and Renewal,
11. Failed read and write operations on the Repository, and
12. Cryptographic module lifecycle management related events

MTNLTRUSTLINE shall also collect and consolidate, either electronically or manually, security information not CA system generated such as:

13. CA and Sub-CA key generation records,
14. Physical access logs,
15. System configuration changes and maintenance,
16. Personnel changes,
17. Discrepancy and compromise reports,
18. Records of the destruction of media containing key material, activation data, or personal Subscriber information, and
19. Possession of activation data for CA private key operations.

MTNLTRUSTLINE shall also record in audit log files and substantiate with manual records events related to the Key Generation System (KGS) optionally operated by MTNLTRUSTLINE for End User key pair generation on smart cards.

20. MTNLTRUSTLINE shall log all events relating to the life cycle of keys managed by the MTNLTRUSTLINE, including any Subscriber keys generated by the Key Generation System of MTNLTRUSTLINE.

21. MTNLTRUSTLINE shall record all events relating to the Subscriber smart card management including receipt of smart cards from vendors (with details about batch & serial number), card initialization, card personalization, card storage, card dispatch, and card destruction by MTNLTRUSTLINE.

#### **4.5.1.2 EVENTS RECORDED BY MTNLTRUSTLINE RAS**

MTNLTRUSTLINE PKI RAS shall record in audit log files events relating to the security of their systems such as:

1. System start-up and shutdown,
2. RA application start-up and shutdown,
3. Attempts to create, remove, set passwords or change the system privileges of the privileged users,
4. Changes to RA details and/or keys,
5. Changes to Certificate creation policies,
6. Login and logoff attempts,
7. Unauthorized attempts at network access to the RA system,
8. Unauthorized attempts to access system files,
9. Failed read and write operations on the Repository,
10. Certificate lifecycle management-related events including approval or denial of Certificate Applications, requests for Revocation, or requests for Renewal, and
11. Issuance of smart cards.

#### **4.5.2 FREQUENCY WITH WHICH AUDIT LOGS ARE PROCESSED**

MTNLTRUSTLINE Administrators and security Administrators shall routinely process the audit logs on a monthly basis.

MTNLTRUSTLINE security Administrators shall also review the audit logs in response to alerts based on irregularities and incidents within the CA/RA systems. MTNLTRUSTLINE security Administrators shall compare the CA system audit logs with audit logs from the RA system when any action is deemed suspicious.

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

#### **4.5.3 PERIOD FOR WHICH AUDIT LOGS ARE KEPT**

Audit logs shall be retained online for at least three (3) months after processing and thereafter archived in accordance with CP § [4.6.2](#).

#### **4.5.4. PROTECTION OF AUDIT LOG**

Only authorized MTNLTRUSTLINE personnel shall be allowed to view and process audit log files.

#### **4.5.5. AUDIT LOG BACKUP PROCEDURES**

Incremental backups of audit logs on physical removable media shall be created daily and full backups weekly. The backup media shall be stored in a safe storage.

#### **4.5.6 AUDIT LOG ACCUMULATION SYSTEM (INTERNAL OR EXTERNAL)**

The audit log accumulation system shall be internal to MTNLTRUSTLINE.

### **4.5.7 NOTIFICATION TO EVENT-CAUSING SUBJECT**

MTNLTRUSTLINE is not required to notify the event-causing subject about the logging of events.

### **4.5.6. VULNERABILITY ASSESSMENTS**

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

## **4.6 RECORDS ARCHIVAL**

### **4.6.1. TYPES OF EVENT RECORDED**

MTNLTRUSTLINE shall retain an archive of information and actions that are material to each Certificate Application and to the creation, Issuance, Revocation, expiration, and Renewal of each Certificate issued in the MTNLTRUSTLINE PKI. These records shall include all relevant evidence regarding:

1. The identity of the Subscriber named in each Certificate (except for Class 1 Certificates, for which only a record of the Subscriber's unambiguous name is maintained) including documentary evidence in support of the Certificate Application,
2. The identity of persons requesting Certificate Revocation (except for Class 1 Certificates, for which only a record of the Subscriber's unambiguous name is maintained),
3. other facts represented in the Certificate, and
4. certain foreseeable material facts related to issuing Certificates including, but not limited to, information relevant to successful completion of a compliance audit under CP § [2.7](#).

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete.

#### **4.6.2. RETENTION PERIOD FOR ARCHIVE**

Digital Certificates and CRLs issued in the MTNLTRUSTLINE PKI and the records associated with them shall be archived for at least seven years after expiration.

Audit information detailed in CP § [4.5.1](#), shall be archived pursuant to CP § [4.5.3](#) and retained for a period of three years but shall not be destroyed until the completion of two successive annual audits succeeding the record period.

#### **4.6.3 PROTECTION OF ARCHIVE**

Only MTNLTRUSTLINE authorized persons shall have access to the archive compiled under CP § [4.6.1](#).

MTNLTRUSTLINE shall protect the archive against unauthorized viewing, modification, deletion, or other tampering, by storage within a trustworthy system.

The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in CP § [4.6.2](#).

#### **4.6.4 ARCHIVE BACKUP PROCEDURES**

MTNLTRUSTLINE shall create back up copies of archives compiled under CP § [4.6.1](#) as and when the archives are created.

Backup copies of the archive and copies of paper-based records under CP § [4.6.1](#) shall be maintained in an off-site disaster recovery facility in accordance with CP § [4.8](#).

#### **4.6.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS**

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

#### **4.6.6. ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)**

The archive collection system shall be internal to MTNLTRUSTLINE.

#### **4.6.7. PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION**

Only MTNLTRUSTLINE trusted personnel shall be permitted to access the archived data. The archive information shall be made available to the CCA upon request.

#### **4.7 KEY CHANGEOVER**

Before the usage period of the MTNLTRUSTLINE CA private key expires (CP § [6.3.2](#)), key changeover shall take place. The old "CA" and its private key shall be deactivated, and a new "CA" with a different private key and distinguished name shall be put in use. The new MTNLTRUSTLINE CA Certificate issued by the RCAI shall be made available through the Repository (CP § [6.1.4](#)).

Before the usage period of any MTNLTRUSTLINE Sub-CA private key expires (CP § [6.3.2](#)), key changeover for that Sub-CA shall take place. The old "Sub-CA" and its private key shall be deactivated, and a new "Sub-CA" with a different private key and distinguished name shall be put in use. The new Sub-CA Certificate issued by the appropriate MTNLTRUSTLINE CA or Sub-CA shall be made available through the Repository (CP § [6.1.4](#)). However, before a Sub-CA Certificate can be renewed, MTNLTRUSTLINE should be able to reconfirms the identity of the Sub-CA under CP §§ [3.1.8.4](#), [3.2.2](#).

The distinguished name of the new CA or Sub-CA shall differentiate the new Certificate from the old Certificate by indicating information about the generation (version) of the CA/Sub-CA. All other information in the Certificate subject name shall remain the same.

#### **4.8 COMPROMISE AND DISASTER RECOVERY**

MTNLTRUSTLINE shall maintain off-site backups of the application logs, Certificate Application data, audit data (per CP § [4.5.1](#)), and records for all Certificates and CRLs issued. Backup of CA and Sub-CA private keys shall be generated and maintained in accordance with CP § [6.2.4](#). These backups shall be made available in the event of a compromise or disaster.

#### **4.8.1 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED**

Following corruption of computing resources, software, and/or data, a report of the event to MTNLTRUSTLINE security, and a response to the event, shall be promptly made by the affected CA or RA personnel in accordance with MTNLTRUSTLINE incident and compromise reporting and handling procedures. Such procedures shall require appropriate escalation, incident investigation, and incident response.

#### **4.8.2 ENTITY PUBLIC KEY IS REVOKED**

Upon Revocation of a CA or Sub-CA Certificate:

The Revocation shall be reported in accordance with CP § [4.4.9](#) in the MTNLTRUSTLINE Repository,

Reasonable efforts shall be used to provide additional notice of the Revocation to MTNLTRUSTLINE PKI participants, and

MTNLTRUSTLINE shall perform a key changeover in accordance with CP § [4.7](#), except following Revocation of a CA or Sub-CA Certificate in connection with the termination of a CA or Sub-CA under CP § [4.9](#).

#### **4.8.3 ENTITY KEY IS COMPROMISED**

If the private key of a MTNLTRUSTLINE PKI CA or Sub-CA is compromised, then all use of such private key shall cease immediately. The Certificate of that entity shall be revoked in accordance with CP § [4.4.3.2](#). Thereafter, reporting of the Revocation shall be made in accordance with CP § [4.8.2](#).

#### **4.8.4 SECURE FACILITY AFTER A NATURAL OR OTHER TYPE OF DISASTER**

MTNLTRUSTLINE shall develop, test, maintain, and, if necessary, implement a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans shall address the restoration of information systems services and key business functions.

MTNLTRUSTLINE shall install and test equipment at its primary site to support CA/RA functions following all but a major disaster that would render the entire facility inoperable. Such equipment shall ensure redundancy and fault tolerance.

MTNLTRUSTLINE shall maintain a disaster recovery site (DR site) with the capability of restoring or recovering operations within twenty-four (24) hours following a disaster with, at a minimum, support for the Certificate Issuance, Certificate Revocation, and Repository functions.

MTNLTRUSTLINE shall have the capability of declaring a disaster on its web sites and of re-directing Subscribers, Relying Parties, and other interested persons to the disaster recovery site.

MTNLTRUSTLINE disaster recovery database shall be synchronized with the production database within a time limit of eight hours.

MTNLTRUSTLINE disaster recovery site shall have equipment with the same security protections as the primary site equipment.

MTNLTRUSTLINE disaster recovery site shall have the same physical security protections as the primary site.

## **4.9 CA TERMINATION**

The termination of a MTNLTRUSTLINE Sub-CA or CA shall be at the discretion of MTNLTRUSTLINE management. The termination of a MTNLTRUSTLINE Enterprise Customer Sub-CA shall be subject to the contract between the terminating Sub-CA and MTNLTRUSTLINE.

In case of termination of a CA or Sub-CA MTNLTRUSTLINE shall, in good faith, use reasonable effort to create a termination plan that minimizes disruption to Customers, Subscribers, and Relying Parties. The termination plan may cover issues such as:

Providing notice to parties affected by the termination, such as Subscribers, Relying Parties, Customers, and the CCA,

In case of MTNLTRUSTLINE Enterprise Customer Sub-CAs, the termination cost sharing arrangement between the terminating Sub-CA and MTNLTRUSTLINE,

The Revocation of the Certificate issued to the Sub-CA by MTNLTRUSTLINE,

The preservation of the archives and records for the time periods required in CP § [4.6](#),

The continuation of Subscriber and Customer support services,

The continuation of Revocation services, such as the Issuance of CRLs,

The Revocation of Certificates of End User Subscribers and Sub-CAs, if necessary,

The payment of compensation (if necessary) to Subscribers whose Certificates are revoked under the termination plan or provision for the Issuance of substitute Certificates by a successor CA or Sub-CA,

Disposition of the CA's or Sub-CA's private key and the hardware token containing such private key, and

Provisions needed for the transition of services to a successor CA or Sub-CA.

---

## **5 PHYSICAL, PROCEDURAL, AND PERSONNEL**

### **SECURITY CONTROLS**

All entities performing CA and RA functions (MTNLTRUSTLINE, MTNLTRUSTLINE Enterprise Sub-CA Customers, and MTNLTRUSTLINE Enterprise RA Customers) shall draft, implement, and enforce a security policy compliant with the Schedules II and III of the Information Technology (Certifying Authorities) Rules, 2000.

#### **5.1 PHYSICAL SECURITY CONTROLS**

The requirements described in the sub-sections below apply equally to MTNLTRUSTLINE primary site as well as disaster recovery site (DR site).

##### **5.1.1 SITE LOCATION AND CONSTRUCTION**

All CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems. Any parts of the premises shared with other Organizations shall be outside this perimeter. This environment shall comply with the requirements in the Schedules II and III of the Information Technology (Certifying Authorities) Rules, 2000.

Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the CA and RA systems. The physical security perimeter shall be constructed with materials that will deter, prevent, and detect covert or overt penetration. The physical security perimeter shall permit physical access to authorized personnel through a barrier such as a locked door that provides mandatory access control for Individuals and requires a positive response (door unlocks) for each individual to cross the security perimeter.

The MTNLTRUSTLINE CA systems shall be housed in secure facilities that are protected by multiple physical security barriers, video monitoring, and two factor authentication including biometrics.

Online Cryptographic Signing Units (CSUs) shall be protected through the use of locked cabinets. Offline CSUs shall be protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material shall be restricted to MTNLTRUSTLINE trusted personnel. The opening and closing of cabinets or containers shall be logged for audit purposes.

MTNLTRUSTLINE RA operations shall be conducted within secure facilities that are protected by multiple tiers of physical security including badge access.

### **5.1.2. PHYSICAL ACCESS**

MTNLTRUSTLINE shall implement necessary physical security controls to restrict physical access to the CA and RA systems to MTNLTRUSTLINE authorized personnel only. All physical access to the secure facility shall be logged electronically or manually as applicable.

### **5.1.3 POWER AND AIR CONDITIONING**

MTNLTRUSTLINE CA and RA locations shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup air conditioning systems to control the temperature. Such systems shall meet the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000.

### **5.1.4 WATER EXPOSURES**

MTNLTRUSTLINE CA and RA locations shall be constructed and equipped, and procedures shall be implemented, to prevent floods or other damaging exposure to water in accordance with the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000.

### **5.1.5 FIRE PREVENTION AND PROTECTION**

MTNLTRUSTLINE CA and RA locations shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke in accordance with the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000. These measures shall also meet all applicable fire safety regulations.

### **5.1.6 MEDIA STORAGE**

MTNLTRUSTLINE shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media in accordance with the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000.

### **5.1.7 WASTE DISPOSAL**

MTNLTRUSTLINE shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing confidential information within the meaning of CP § [2.8.1](#) in accordance with the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000.

### **5.1.8 OFF-SITE BACKUP**

MTNLTRUSTLINE shall maintain back ups of critical system data or any other sensitive information, including audit data, in a secure off-site facility in accordance with the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000.

## **5.2 PROCEDURAL CONTROLS**

### **5.2.1 TRUSTED ROLES**

MTNLTRUSTLINE employees, contractors, consultants, and auditors that are designated to manage trustworthiness of the MTNLTRUSTLINE PKI shall be considered to be "Trusted Persons" serving in a "Trusted Role." Trusted persons include personnel that have access to or control authentication or cryptographic operations that may materially affect:

The validation of information in Certificate Applications;

The Acceptance, rejection, or other processing of Certificate Applications, Revocation requests, or Renewal requests, or enrollment information;

The Issuance, or Revocation of Certificates, including personnel having access to restricted portions of the MTNLTRUSTLINE Repository;

Or the handling of Subscriber information or requests.

Trusted persons include, but are not limited to:

Validation and RA operations personnel,

Cryptographic operations personnel,

System administration and operations personnel,

Security personnel, and

All personnel that are designated to manage infrastructure trustworthiness.

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

### **5.2.2 NUMBER OF PERSONS REQUIRED PER TASK**

MTNLTRUSTLINE shall establish, maintain, and enforce rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple trusted persons are required to perform sensitive tasks in accordance with the requirements of the Schedule III of the Information Technology (Certifying Authorities) Rules, 2000.

### **5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE**

MTNLTRUSTLINE shall authenticate the identity of all personnel seeking to become trusted persons by requiring personal (physical) presence of such personnel before trusted persons performing MTNLTRUSTLINE security functions and a check of well-recognized forms of identification like passports and driver's licenses. Identity shall be further confirmed through the background checking procedures in CP §§ [5.3.1](#), [5.3.2](#).

MTNLTRUSTLINE shall ensure that personnel have achieved trusted status and departmental approval has been given before such personnel are:

- Issued access Devices and granted access to the required facilities;

- Issued electronic credentials to access and perform specific functions on MTNLTRUSTLINE CA, RA, or other IT systems.

## **5.3 PERSONNEL SECURITY CONTROLS**

### **5.3.1 BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS**

MTNLTRUSTLINE shall require that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

### **5.3.2 BACKGROUND CHECK PROCEDURES**

Prior to commencement of employment in a Trusted Role, MTNLTRUSTLINE shall conduct background checks which include the following:

Confirmation of previous employment,

Check of professional reference,

Confirmation of the highest or most relevant educational degree obtained,

Check of a government issued identification like passport, driver's license and one other identification document.

Search of criminal records (local, state, and national), and

Check of credit/financial records.

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

Misrepresentations made by the candidate or trusted person,

Highly unfavorable or unreliable personal references,

Certain criminal convictions, and

Indications of a lack of financial responsibility.

Reports containing such information shall be evaluated by human resources and security personnel, and such personnel shall take actions that are reasonable in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for trusted positions or the termination of existing trusted persons. The use of information revealed in a background check to take such actions shall be subject to applicable law.

### **5.3.3 TRAINING REQUIREMENTS AND TRAINING PROCEDURES**

MTNLTRUSTLINE shall provide its personnel with the requisite training prior to being assigned to trusted roles, and shall provide the requisite on-the-job training, needed for them to perform their job responsibilities relating to CA or RA operations competently and satisfactorily.

MTNLTRUSTLINE shall also periodically review its training programs, and the training shall address the elements relevant to functions performed by its personnel. Training programs must address the elements relevant to the particular environment of the person being trained, including:

Basic PKI concepts,

Job responsibilities,

MTNLTRUSTLINE security and operational policies and procedures,

Use and operation of deployed hardware and software,

Incident and Compromise reporting and handling, and

Disaster recovery and business continuity procedures.

#### **5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS**

MTNLTRUSTLINE shall provide refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

#### **5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE**

No stipulation.

#### **5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS**

MTNLTRUSTLINE shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorized actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

### **5.3.7 CONTRACTING PERSONNEL REQUIREMENTS**

In limited circumstances, independent contractors or consultants may be used to fill trusted positions. Any such contractor or consultant shall be held to the same functional and security criteria that apply to a MTNLTRUSTLINE employee in a comparable position.

Independent contractors and consultants who have not completed the background check procedures specified in CP § 5.3.2 shall be permitted access to MTNLTRUSTLINE secure facilities only to the extent they are escorted and directly supervised by trusted persons.

### **5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL**

MTNLTRUSTLINE shall give its personnel (including trusted persons) the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

## **6 TECHNICAL SECURITY CONTROLS**

### **6.1 KEY PAIR GENERATION AND INSTALLATION**

#### **6.1.1 KEY PAIR GENERATION AND INSTALLATION**

MTNLTRUSTLINE shall ensure that all cryptographic key pairs related to the MTNLTRUSTLINE PKI are generated using trustworthy systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys.

CA and Sub-CA key pair generation shall be carried out within a FIPS 140-1 level 3 or higher device in a physically secured environment by personnel in trusted roles under, at least, dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the MTNLTRUSTLINE's practices. The activities performed for each CA/Sub-CA key pair generation shall be recorded, dated and signed by all individuals involved. These records shall be kept for audit and tracking in accordance with CP § [4.5.1](#) and CP § [4.6](#).

Generation of End User Subscriber key pairs shall be performed by the Subscriber or at a MTNLTRUSTLINE RA office in the presence of the Subscriber.

MTNLTRUSTLINE may optionally pre-generate key pairs for its End User Subscribers on secure hardware tokens (smart cards). MTNLTRUSTLINE shall ensure that:

1. Pre-generated Subscriber keys shall be generated using the RSA algorithm and shall have a key length of 1024 bits or more.
2. The hardware tokens (smart cards) and associated activation data (pass-phrases or PINs) shall be stored securely before delivery to the Subscriber.
3. MTNLTRUSTLINE shall not back-up or otherwise compromise the integrity and privacy of the private keys.

### **6.1.2 PRIVATE KEY DELIVERY TO ENTITY**

End User Subscribers' private keys are generally generated by the End User Subscribers themselves, and therefore private key delivery to a Subscriber is unnecessary.

Private keys shall be delivered to End User Subscribers only when their key pairs are pre-generated on hardware tokens, which are distributed to Certificate Applicants in connection with the enrollment process. MTNLTRUSTLINE shall ensure that the entities distributing such tokens shall take reasonable efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them.

### **6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER**

When a Public Key is transferred to be certified, it shall be delivered through a mechanism ensuring that the Public Key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred Public Key. The acceptable mechanism within the MTNLTRUSTLINE PKI for Public Key delivery is a PKCS#10 Certificate signing request package or an equivalent method ensuring that:

1. The Public Key has not been altered during transit; and
2. The Certificate Applicant possesses the private key corresponding to the transferred Public Key.

### **6.1.4 CA PUBLIC KEY DELIVERY TO USERS**

MTNLTRUSTLINE shall make its CA and Sub-CA Public Keys available to the Relying Parties via CA Certificates in a secure fashion. These CA Certificates shall be published in the MTNLTRUSTLINE Certificate Repository and the MTNLTRUSTLINE web site. MTNLTRUSTLINE CA and Sub-CA Certificates shall be verifiable by users with respect to the RCAI root Certificate.

### **6.1.5 KEY SIZES**

MTNLTRUSTLINE shall use key pairs of length (strength) sufficient to prevent the revelation of the private key using cryptanalysis during the expected lifetime of such key pairs.

The current MTNLTRUSTLINE standard for minimum key sizes is:

1. 2048 bit RSA keys for all CA and Sub-CA keys,
2. 1024 bit RSA keys for all RA keys, and
3. 1024 bit RSA keys for all End User Subscriber keys.

### **6.1.6 PUBLIC KEY PARAMETERS GENERATION**

No stipulation.<sup>2</sup>

### **6.1.7 PARAMETER QUALITY CHECKING**

No stipulation.<sup>3</sup>

### **6.1.8 HARDWARE OR SOFTWARE KEY GENERATION**

MTNLTRUSTLINE shall generate CA and Sub-CA key pairs, and the random numbers for such key pairs, in FIPS 140-1 Level 3 compliant hardware.

RA keys pairs shall be generated in hardware (smart cards).

---

<sup>2</sup> Public Key parameters are relevant in case of Digital Signature Algorithm (DSA). The DSA is not recognized by the Indian IT-Act and MTNLTRUSTLINE does not support DSA. MTNLTRUSTLINE supports the RSA Public Key algorithm for which this requirement is not relevant.

<sup>3</sup> See footnote above.

MTNLTRUSTLINE shall recommend that End User Subscribers generate their key pairs in hardware (smart cards), although such key pairs may be generated by the Subscriber in hardware or software.

End User Subscriber key pairs pre-generated by MTNLTRUSTLINE on behalf of the Subscriber shall always be generated in secure hardware (smart cards).

### **6.1.9 KEY USAGE PURPOSES**

MTNLTRUSTLINE shall set the KeyUsage extension of X.509 Version 3 Certificates in accordance with IETF RFC 2459 (Internet X.509 Public Key Infrastructure Certificate and CRL Profile). The KeyUsage extension shall be configured so as to set and clear bits and the criticality field in accordance with table below.

**Table 2: KeyUsage Extensions for X.509 V3 Certificates:**

		<b>CA'S AND SUB-CAs</b>	<b>CLASS 1</b>	<b>CLASS 2</b>	<b>CLASS 3</b>
<b>CRITICALITY</b>		<b>FALSE</b>	<b>FALSE</b>	<b>FALSE</b>	<b>FALSE</b>
<b>0</b>	<b>DIGITALSIGNATURE</b>	<b>CLEAR</b>	<b>SET</b>	<b>SET</b>	<b>SET</b>
<b>1</b>	<b>NONREPUDIATION</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>SET</b>	<b>SET</b>
<b>2</b>	<b>KEYENCIPHERMENT</b>	<b>CLEAR</b>	<b>SET</b>	<b>SET</b>	<b>SET</b>
<b>3</b>	<b>DATAENCIPHERMENT</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>
<b>4</b>	<b>KEYAGREEMENT</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>
<b>5</b>	<b>KEYCERTSIGN</b>	<b>SET</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>
<b>6</b>	<b>CRLSIGN</b>	<b>SET</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>
<b>7</b>	<b>ENCIPHERONLY</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>
<b>8</b>	<b>DECIPHERONLY</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>	<b>CLEAR</b>

WTLS Certificates and certain wireless application CA Certificates are not X.509 Version 3 Certificates and thus do not contain a KeyUsage extension.

## **6.2 PRIVATE KEY PROTECTION**

MTNLTRUSTLINE PKI participants, including CAs and Sub-CAs, RAs, and End User Subscribers, shall protect their own private keys by using a trustworthy system and shall take all necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such private keys.

### **6.2.1 STANDARDS FOR CRYPTOGRAPHIC MODULES**

MTNLTRUSTLINE shall perform all cryptographic operations with its own CA/Sub-CA private keys and client Sub-CA private keys on hardware cryptographic modules rated at a minimum of FIPS 140-1 level 3.

MTNLTRUSTLINE shall require all RAs (MTNLTRUSTLINE as well as non-MTNLTRUSTLINE) to perform all cryptographic operations with their own private keys on hardware cryptographic modules rated at a minimum of FIPS 140-1 level 1 or equivalent.

End User Subscribers have the option of protecting their private keys in a smart card or other hardware token. MTNLTRUSTLINE shall recommend that all End User Subscribers use hardware cryptographic modules rated at a minimum of FIPS 140-1 level 1 or equivalent.

### **6.2.2 PRIVATE KEY 'N OUT OF M' MULTI-PERSON CONTROL**

MTNLTRUSTLINE shall implement multi-person control to protect the activation data needed to activate CA/Sub-CA private keys within the MTNLTRUSTLINE PKI.

MTNLTRUSTLINE shall use 'secret sharing' to split the private key or activation data needed to operate the private key into separate parts called 'secret shares'. Each 'secret share' shall be held by distinct MTNLTRUSTLINE trusted personnel (custodian). Some threshold number of secret shares (n) out of the total number of secret shares (m) shall be required to operate the private key. MTNLTRUSTLINE shall also use secret sharing to protect the activation data needed to activate private keys located at its disaster recovery site.

MTNLTRUSTLINE shall implement secret sharing using the values for threshold and total number of shares specified below:

**Table 3: Secret Share Thresholds:**

TYPE OF ENTITY	PRIMARY			DISASTER RECOVERY	
	REQUIRED SECRET SHARES TO SIGN END USER CERTIFICATE	REQUIRED SECRET SHARES TO SIGN SUB-CA CERTIFICATE	MINIMUM TOTAL NUMBER OF SECRET SHARES CUSTODIANS	NEEDED	TOTAL
	<u>mtnlTrustLine</u> PRIMARY CA	N/A	3	5	3
<u>mtnlTrustLine</u> OFFLINE SUB-CA	N/A	3	5	3	5
<u>mtnlTrustLine</u> ONLINE SUB-CA	3	3	5	3	5

### **6.2.3 PRIVATE KEY ESCROW**

MTNLTRUSTLINE shall not escrow CA/Sub-CA or End User Subscriber private keys.

### **6.2.4 PRIVATE KEY BACKUP**

MTNLTRUSTLINE shall create backup copies of CA/Sub-CA private keys for routine recovery and disaster recovery purposes. Such keys shall be stored in encrypted form within hardware cryptographic modules and associated key storage Devices. Cryptographic modules used for CA/Sub-CA private key storage shall meet the requirements of CP § [6.2.1](#). CA/Sub-CA private keys shall be copied to backup hardware cryptographic modules in accordance with CP § [6.2.6](#). Modules containing backup copies of CA/Sub-CA private keys shall be subject to the requirements of CP §§ [5.1](#), [6.2.1](#).

MTNLTRUSTLINE shall not backup or archive End User Subscriber private keys.

### **6.2.5 PRIVATE KEY ARCHIVAL**

MTNLTRUSTLINE shall not archive CA/Sub-CA or End User Subscriber private keys.

### **6.2.6 PRIVATE KEY ENTRY INTO CRYPTOGRAPHIC MODULE**

MTNLTRUSTLINE shall generate CA/Sub-CA key pairs on the hardware cryptographic modules in which the keys will be used.

In addition, MTNLTRUSTLINE shall make copies of such CA/Sub-CA key pairs for routine recovery and disaster recovery purposes. Where CA/Sub-CA key pairs are backed up to another hardware cryptographic module, such key pairs shall be transported between modules in encrypted form.

### **6.2.7 METHOD OF ACTIVATING PRIVATE KEY**

All MTNLTRUSTLINE PKI participants shall protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

#### **6.2.7.1 END USER SUBSCRIBER PRIVATE KEYS**

This section states the MTNLTRUSTLINE recommended standards for protecting activation data for End User Subscribers' private keys, although Subscribers have the option of using enhanced private key protection mechanisms available today including the use of smart cards, biometric access Devices, and other hardware tokens to store private keys. The use of two factor authentication mechanisms (e.g., token and pass-phrase, biometric and token, or biometric and pass-phrase) shall be encouraged.

The MTNLTRUSTLINE PKI minimum standard protection of private keys of Individuals is for the Subscribers to use a smart card or security of equivalent strength to authenticate the Subscriber before the activation of the private key. In addition, the Subscriber shall take reasonable measures for the physical protection of the Subscriber's smart card to prevent use of the smart card and its associated private key without the Subscriber's authorization. Use of a password, along with a smart card or biometric access device, in accordance with CP § [6.4.1](#) is recommended.

The MTNLTRUSTLINE PKI minimum standard for protection of private keys of Servers and Devices is the use of a password in accordance with CP § [6.4.1](#) or security of equivalent strength to prevent the private key from unauthorized activation or use. In addition, the Subscriber (organization) shall take reasonable measures for the physical protection of the server or device to prevent unauthorized use of the server or device and the associated private key. When deactivated, private keys shall be kept in encrypted form only.

#### **6.2.7.2 CA/SUB-CA PRIVATE KEYS**

MTNLTRUSTLINE PKI CA and Sub-CA private keys shall be activated by a threshold number of custodians supplying their activation data (tokens or pass-phrases) in accordance with CP § [6.2.2](#).

For MTNLTRUSTLINE offline CAs/Sub-CAs, the CA private key shall be activated for one session (e.g., for the certification of a Sub-CA or signing a CRL) after which it shall be deactivated and the token returned to secure storage.

For MTNLTRUSTLINE Online Sub-CAs, the CA private key shall be activated for an indefinite period and the token shall remain online in the production data center until the Sub-CA is taken offline (e.g., for system maintenance).

MTNLTRUSTLINE custodians are required to safeguard their secret shares and sign an agreement acknowledging their custodian responsibilities.

#### **6.2.8 METHOD OF DEACTIVATING PRIVATE KEY**

End User Subscribers have an obligation to protect their private keys under CP § [6.2.7.1](#). Such obligations shall extend to protection of the private key after a private key operation has taken place.

MTNLTRUSTLINE CA/Sub-CA private keys shall be deactivated upon removal from the token reader.

When an Online Sub-CA is taken offline MTNLTRUSTLINE personnel shall remove the token containing such Sub-CA's private key from the reader in order to deactivate it.

With respect to the private keys of offline CAs/Sub-CAs, after each session in which such private keys are used for private key operations, MTNLTRUSTLINE personnel shall remove the token containing such private keys from the reader in order to deactivate it. Once removed from the reader, tokens shall be returned to secure storage.

### **6.2.9 METHOD OF DESTROYING PRIVATE KEY**

At the conclusion of a CA/Sub-CA's operational lifetime, MTNLTRUSTLINE personnel shall decommission the CA/Sub-CA's private key by deleting it using functionality of the token containing such CA/Sub-CA's private key so as to prevent its recovery following deletion, while not adversely affecting the private keys of other CAs/Sub-CAs contained on the token.

The activities performed during such decommissioning shall be recorded, dated and signed by all individuals involved. These records shall be kept for audit and tracking in accordance with CP § [4.5.1](#) and CP § [4.6](#).

## **6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT**

### **6.3.1 PUBLIC KEY ARCHIVAL**

MTNLTRUSTLINE CA, Sub-CA, RA, and End User Subscriber Certificates shall be archived as part of routine archival procedures (CP § [4.6](#)).

### **6.3.2 USAGE PERIODS FOR THE PUBLIC AND PRIVATE KEYS**

The usage period for End User Subscriber key pairs is the same as the validity period for their Certificates, except that private keys may continue to be used for decryption and Public Keys may continue to be used for signature verification. The validity period of a Certificate ends upon its expiration or Revocation.

The maximum validity periods for MTNLTRUSTLINE Certificates are set forth in the table below.

**Table 4: Certificate Validity Periods:**

TYPE OF CERTIFICATE (CLASS 1-3)	MAXIMUM VALIDITY PERIOD
MTNLTRUSTLINE PRIMARY CA	5 YEARS
MTNLTRUSTLINE OFFLINE SUB-CA	5 YEARS
MTNLTRUSTLINE ONLINE SUB-CA	3 YEARS
MTNLTRUSTLINE END USER SUBSCRIBER	1 YEAR

In addition, MTNLTRUSTLINE CAs/Sub-CAs shall stop issuing new Certificates at an appropriate date prior to the expiration of the CA/Sub-CA's Certificate such that no Certificate issued by a Sub-CA or End User Subscriber expires after the expiration of any superior CA/Sub-CA Certificates.

## **6.4 ACTIVATION DATA**

### **6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION**

MTNLTRUSTLINE PKI participants generating and installing activation data for their private keys shall use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

MTNLTRUSTLINE shall generate activation data for the CAs and Sub-CAs within the MTNLTRUSTLINE PKI in accordance with the secret sharing requirements of CP § [6.2.2](#).

To the extent passwords are used as activation data (CP § [6.2.7.1](#)), users shall generate passwords that cannot easily be guessed or cracked by dictionary attacks. MTNLTRUSTLINE shall provide information to its PKI participants, including End User Subscribers, concerning methods to choose secure passwords.

Where the End User Subscriber keys are pre-generated by MTNLTRUSTLINE (on smart cards), a pass-phrase or PIN shall be used to protect access to the private keys. The activation data shall be transmitted to the End User Subscriber via a channel of appropriate protection, and distributed separately from the associated key module. The Subscriber shall be required to acknowledge receipt of the key module (smart card) and activation data. In addition, Subscribers shall also receive (and acknowledge receipt of) information regarding the use of the key module and the procedure to change the activation data.

#### **6.4.2 ACTIVATION DATA PROTECTION**

MTNLTRUSTLINE shall utilize secret sharing in accordance with CP § [6.2.2](#) and shall provide the procedures and means to enable custodians to take the precautions necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of the secret shares that they possess. Custodians shall not:

Copy, disclose, or make the secret share available to a third party, or make any unauthorized use of it whatsoever; or

Disclose his, her, or any other person's status as a custodian to any third party.

The secret shares and any information disclosed to the custodian in connection with his or her duties as a custodian shall constitute confidential information under CP § [2.8.1](#).

Also, MTNLTRUSTLINE shall include in its disaster recovery plans provisions for custodians making their secret shares available at a disaster recovery site after a disaster.

MTNLTRUSTLINE shall maintain an audit trail of secret shares, and custodians shall participate in the maintenance of an audit trail.

MTNLTRUSTLINE RAs shall generate and store their RA Private Keys in hardware (CP § [6.2.1](#)).

End User Subscribers shall protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure or unauthorized use of such activation data.

### **6.4.3 OTHER ASPECTS OF ACTIVATION DATA**

See CP §§ [6.4.1](#), [6.4.2](#).

## **6.5 COMPUTER SECURITY CONTROLS**

MTNLTRUSTLINE shall ensure that all CA and RA functions take place on trustworthy systems in accordance with the security policy of MTNLTRUSTLINE and the requirements of the IT-Act 2000.

### **6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS**

MTNLTRUSTLINE shall ensure that the systems maintaining CA and RA software and data files are trustworthy systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under CP § [2.7.4](#). In particular, MTNLTRUSTLINE shall deploy systems that provide the following functions:

- Identification and authentication of all users,
- Role-based access controls,
- Logically separated networks that prevent network access except through defined application processes,
- Dual control for certain security-related operations,
- Audit generation, audit review and archiving of all security related events,
- Backup and recovery.

### **6.5.2 COMPUTER SECURITY RATING**

No stipulation.

## **6.6 LIFE CYCLE SECURITY CONTROLS**

### **6.6.1 SYSTEM DEVELOPMENT CONTROLS**

MTNLTRUSTLINE presently does not develop PKI or other IT software. However, any applications implementation by MTNLTRUSTLINE shall be carried out in accordance with MTNLTRUSTLINE change management standards.

The software implemented by MTNLTRUSTLINE, when first loaded, shall provide a method to verify that the software on the system is as provided by the software vendor and is the correct version intended for use.

MTNLTRUSTLINE shall maintain separate production and development environments.

### **6.6.2 SECURITY MANAGEMENT CONTROLS**

Software for CA and RA functions shall be subject to checks to verify their integrity. MTNLTRUSTLINE shall require the software vendors to provide a hash of all software packages or software updates that they provide to MTNLTRUSTLINE. This hash can be used to verify the integrity of such software manually. MTNLTRUSTLINE shall also have mechanisms and/or policies in place to control and monitor the configuration of their CA systems. Upon installation, and at regular intervals, MTNLTRUSTLINE shall validate the integrity of the CA system.

### **6.6.3 LIFE CYCLE SECURITY RATINGS**

No stipulation.

## **6.7 NETWORK SECURITY CONTROLS**

MTNLTRUSTLINE shall perform all CA and RA functions using networks secured in accordance with the MTNLTRUSTLINE information systems security policy to prevent unauthorized access, tampering, denial-of-service attacks, and other malicious activities. MTNLTRUSTLINE shall protect the communications of sensitive information using point-to-point encryption for confidentiality and Digital Signatures for non-repudiation and authentication.



## **6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

Cryptographic modules used by MTNLTRUSTLINE shall meet the requirements specified in CP § [6.2.1](#).

## **7 CERTIFICATE AND CRL PROFILES**

### **7.1 CERTIFICATE PROFILE**

MTNLTRUSTLINE PKI Certificates, except for WTLS Certificates, shall conform to:

1. ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997
2. RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.

MTNLTRUSTLINE PKI X.509 Certificates shall contain the following basic fields with indicated prescribed values or value constraints:

**Table 5: Basic Certificate**

<b>BASIC FIELD</b>	<b>VALUE OR VALUE CONSTRAINT</b>
<b>VERSION</b>	<b>VERSION 3 (VALUE 2) (CP § <a href="#">7.1.1</a>)</b>
<b>SERIAL NUMBER</b>	<b>INTEGER VALUE, UNIQUE FOR EACH CERTIFICATE ISSUED BY THE ISSUER</b>
<b>SIGNATURE ALGORITHM</b>	<b>ALGORITHM IDENTIFIER FOR THE ALGORITHM USED BY THE ISSUER TO SIGN THE CERTIFICATE (CP § <a href="#">7.1.3</a>)</b>
<b>ISSUER DN</b>	<b>THE X.500 DISTINGUISHED NAME OF THE ENTITY SIGNING THE CERTIFICATE (CP § <a href="#">7.1.4</a>)</b>
<b>VALIDITY<sup>4</sup></b>	<b>THE CERTIFICATE VALIDITY PERIOD REPRESENTED BY TWO DATES:  VALIDITY NOT BEFORE - THE DATE ON WHICH THE CERTIFICATE VALIDITY PERIOD BEGINS, AND  VALIDITY NOT AFTER - THE DATE ON WHICH THE CERTIFICATE VALIDITY PERIOD ENDS.</b>

<sup>4</sup> In accordance with RFC 2459 the validity dates are encoded as UTC Time for dates through the year 2049 and Generalized Time for dates in 2050 or later.



BASIC FIELD	VALUE OR VALUE CONSTRAINT
SUBJECT DN	THE X.500 DISTINGUISHED NAME OF THE ENTITY ASSOCIATED WITH THE PUBLIC KEY CERTIFIED IN THE SUBJECT PUBLIC KEY FIELD OF THE CERTIFICATE (CP § <a href="#">7.1.4</a> )
SUBJECT PUBLIC KEY	ENCODED IN ACCORDANCE WITH RFC 2459
SIGNATURE	GENERATED AND ENCODED IN ACCORDANCE WITH RFC 2459

At present only X.509 version 3 Certificates are valid under the IT-Act 2000, hence no stipulation about the standards for WTLS Certificates is made in this CP. MTNLTRUSTLINE shall evaluate the standards for WTLS Certificates as and when the applicable standards are approved or notified by the appropriate government.

### **7.1.1 VERSION NUMBER(S) SUPPORTED**

All MTNLTRUSTLINE PKI Certificates, except for WTLS Certificates, shall be X.509 version 3 Certificates.

### **7.1.2 CERTIFICATE EXTENSIONS**

MTNLTRUSTLINE shall populate X.509 version 3 Certificates with the extensions listed in table below:

**Table 6: Certificate Extensions**

EXTENSION	VALUE OR VALUE CONSTRAINT	CRITICALITY
AUTHORITY KEY IDENTIFIER	SHA-1 HASH VALUE OF ISSUER'S PUBLIC KEY	FALSE
SUBJECT KEY IDENTIFIER	SHA-1 HASH VALUE OF SUBSCRIBER'S PUBLIC KEY	FALSE
KEY USAGE	AS PER CP § <a href="#">6.1.9</a>	
CERTIFICATE POLICIES POLICY IDENTIFIER POLICY QUALIFIERS	AS PER CP § <a href="#">7.1.6</a> AS PER CP § <a href="#">7.1.8</a>	FALSE
SUBJECT ALTERNATIVE NAME	AS PER RFC 2459	FALSE
ISSUER ALTERNATIVE	AS PER RFC 2459	FALSE



EXTENSION	VALUE OR VALUE CONSTRAINT	CRITICALITY
NAMES		
BASIC CONSTRAINTS	AS PER CP § <a href="#">7.1.2.1</a>	
EXTENDED KEY USAGE FIELD	AS PER CP § <a href="#">7.1.2.2</a>	
CRL DISTRIBUTION POINTS	URI OF THE CRL.	FALSE

#### **7.1.2.1 BASIC CONSTRAINTS**

MTNLTRUSTLINE shall populate X.509 version 3 CA and Sub-CA Certificates with a basic constraints extension with the CA field set to TRUE.

MTNLTRUSTLINE shall populate End User Subscriber Certificates with a basic constraints extension, but the extension shall be given a value of an empty sequence.

X.509 Version 3 Online Sub-CA Certificates issuing End User Subscriber Certificates shall have a path length constraint field of the basic constraints extension set to a value of zero (0).

MTNLTRUSTLINE CA and Offline Sub-CA Certificates shall have the path length constraint field of the basic constraints extension set to a value indicating the maximum number of Sub-CA Certificates that may follow this Certificate in a certification path.

The criticality field of this extension shall be set to TRUE for CA and Sub-CA Certificates, but otherwise set to FALSE.

#### **7.1.2.2 EXTENDED KEY USAGE**

MTNLTRUSTLINE shall populate X.509 version 3 Certificates with an extended key usage extension configured so as to set and clear bits and the criticality field in accordance with table below.

**Table 7: Extended Key Usage Extension Values:**

	CRITICALITY	SERVER AUTH	CLIENT AUTH	CODE SIGNING	EMAIL PROTECTION	TIME STAMPING
CA'S AND SUB-CAS	FALSE	CLEAR	CLEAR	CLEAR	CLEAR	CLEAR
CLASS 1 INDIVIDUAL	FALSE	CLEAR	SET	CLEAR	SET	CLEAR
CLASS 2 INDIVIDUAL	FALSE	CLEAR	SET	CLEAR	SET	CLEAR
CLASS 2 DEVICES	FALSE	SET	SET	CLEAR	CLEAR	CLEAR
CLASS 3 INDIVIDUAL	FALSE	CLEAR	SET	CLEAR	SET	CLEAR
CLASS 3 SERVER	FALSE	SET	SET	CLEAR	CLEAR	CLEAR
CLASS 3 SERVER (TIME STAMPING SERVER)	FALSE	SET	SET	CLEAR	CLEAR	SET

### **7.1.3 ALGORITHM OBJECT IDENTIFIERS**

MTNLTRUSTLINE CAs and Sub-CAs shall sign Certificates using sha-1WithRSAEncryption algorithm (OID: =1.2.840.113549.1.1.5).

The algorithm identifier of the subject Public Key shall be rsaEncryption (OID: = 1.2.840.113549.1.1.1).

### **7.1.4 NAME FORMS**

MTNLTRUSTLINE PKI Certificates shall be populated with an issuer and subject distinguished name in accordance with CP § [3.1.1](#).

### **7.1.5 NAME CONSTRAINTS**

No stipulation.

### **7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER**

The object identifier for the Certificate Policy corresponding to each Class of Certificate is set forth in CP § [1.2](#). MTNLTRUSTLINE shall populate the Certificate Policies extension in each X.509 version 3 Certificate with the object identifier of the Certificate Policy corresponding to the Certificate's Class set forth in CP § [1.2](#).

### **7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION**

No stipulation.

### **7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS**

MTNLTRUSTLINE shall populate all 'X.509 version 3 Certificates' with a CPS pointer policy qualifier having a value pointing to the URL of the MTNLTRUSTLINE CPS and/or Relying Party Agreement.

### **7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION**

No stipulation.

## **7.2 CRL PROFILE**

MTNLTRUSTLINE CAs and Sub-CAs shall issue CRLs that conform to RFC 2459.

### **7.2.1 VERSION NUMBER(S) SUPPORTED**

All MTNLTRUSTLINE PKI CRLs, except for WTLS CRLs, shall be X.509 version 2 CRLs.

### **7.2.2 CRL AND CRL ENTRY EXTENSIONS**

No stipulation.

---

## **8 SPECIFICATION ADMINISTRATION**

### **8.1 SPECIFICATION CHANGE PROCEDURES**

Updates to this CP shall be made by the MTNLTRUSTLINE Policy and Procedures Steering Committee and need to be approved by the CCA before they become effective. Updates shall either be in the form of a document containing a revised CP or an update. Proposed new versions or updates shall be posted to the Updates section of the MTNLTRUSTLINE Repository located at: <https://www.mtnltrustline.com/repository/updates>. Updates shall supersede any designated or conflicting provisions of the referenced version of the CP.

#### **8.1.1 ITEMS THAT CAN CHANGE WITHOUT NOTIFICATION**

The MTNLTRUSTLINE Policy and Procedures Steering Committee may make changes to this specification without notification for changes that are editorial or typographical corrections, or updates to the URLs or contact details.

Notwithstanding anything in the CP to the contrary, if MTNLTRUSTLINE Policy and Procedures Steering Committee believes that updates to the CP are necessary immediately to stop or prevent a breach of security, MTNLTRUSTLINE shall be entitled to make such updates by publication in the MTNLTRUSTLINE Repository. Such updates will be effective immediately upon publication.

MTNLTRUSTLINE reserves the right to obtain a post-facto approval from the CCA for such updates.

#### **8.1.2 ITEMS THAT CAN CHANGE WITH NOTIFICATION**

##### **8.1.2.1 LIST OF ITEMS**

All updates, except those covered in CP § [8.1.1](#), to the CP shall require notification prior to becoming effective.

#### **8.1.2.2 NOTIFICATION MECHANISM**

Except as noted under CP § [8.1.1](#), MTNLTRUSTLINE Policy and Procedures Steering Committee shall submit the proposed updates in electronic and/or paper form to the CCA for approval. After obtaining the CCA's approval the proposed updates to the CP shall be posted in the updates section of the MTNLTRUSTLINE Repository, which is located at <https://www.mtnltrustline.com/repository/updates>.

#### **8.1.2.3. COMMENT PERIOD**

Except as noted under CP § [8.1.1](#), the comment period for any changes to the CP shall be seven (07) days, starting on the date on which the changes are posted on the MTNLTRUSTLINE Repository. Any MTNLTRUSTLINE PKI participant shall be entitled to file comments with the MTNLTRUSTLINE Policy and Procedures Steering Committee up to the end of this comment period.

#### **8.1.2.4. MECHANISM TO HANDLE COMMENTS**

The MTNLTRUSTLINE Policy and Procedures Steering Committee will consider any comments on the proposed changes. MTNLTRUSTLINE will either (a) allow the proposed updates to become effective without further change, (b) change the proposed updates and republish them as a new updates under CP § [8.1.2.2](#), or (c) withdraw the proposed updates. MTNLTRUSTLINE is entitled to withdraw proposed updates by providing notice in the updates section of the MTNLTRUSTLINE Repository.

Unless proposed updates are changed or withdrawn, they shall become effective upon the expiration of the comment period under CP § [8.1.2.3](#).

#### **8.1.3 CHANGES REQUIRING CHANGES IN THE CERTIFICATE POLICY OID**

If the 'MTNLTRUSTLINE Policy and Procedures Steering Committee' determines that a change is necessary in the object identifier corresponding to a Certificate Policy, the update shall contain new object identifiers for the Certificate Policies corresponding to each Class of Certificate. Otherwise, updates shall not require a change in Certificate Policy object identifier.

## **8.2 PUBLICATION AND NOTIFICATION PROCEDURES**

This latest version of this CP is available for viewing in electronic form within the MTNLTRUSTLINE Repository at <https://www.mtnltrustline.com/repository/cp>.

The CP is also available for download in Adobe Acrobat (pdf) format. MTNLTRUSTLINE also makes the CP available upon request sent to [cp@mtnltrustline.com](mailto:cp@mtnltrustline.com).

The paper copy of the CP is available from MTNLTRUSTLINE upon requests sent to:

**Table 8: Contact for Obtaining Paper Copy of This CP**

<p><b>SUBJECT: CP REQUEST</b></p> <p><b>MTNLTRUSTLINE POLICY AND PROCEDURES COORDINATOR</b></p> <p><b>MAHANAGAR TELEPHONE NIGAM LIMITED</b></p> <p><b>JEEVAN BHARATI, 124 CONNAUGHT CIRCUS, NEW DELHI – 110 001</b></p> <p><b>TEL: +91 11 2374 2212, FAX: +91 11 2335 9425</b></p>
--

## **8.3 CPS APPROVAL PROCEDURES**

MTNLTRUSTLINE Policy and Procedures Steering Committee shall approve or reject the CPS pursuant to this policy. (See CPS § [8.1](#))



## **9 LIST OF TERMS**

### **9.1 LIST OF ACRONYMS**

**Table 9: List of Acronyms**

<b>ACRONYM</b>	<b>TERM</b>
CA	CERTIFYING AUTHORITY
CCA	CONTROLLER OF CERTIFYING AUTHORITIES
CN	COMMON NAME
CP	CERTIFICATE POLICY
CPS	CERTIFICATION PRACTICE STATEMENT
CRL	CERTIFICATE REVOCATION LIST
CSR	CERTIFICATE SIGNING REQUEST
DN	DISTINGUISHED NAME
FIPS	UNITED STATES FEDERAL INFORMATION PROCESSING STANDARDS
HTTP	HYPERTEXT TRANSFER PROTOCOL
HTTPS	HYPERTEXT TRANSFER PROTOCOL WITH SSL
IETF	INTERNET ENGINEERING TASK FORCE
ITU	INTERNATIONAL TELECOMMUNICATIONS UNION
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
LDIF	LDAP DIRECTORY INTERCHANGE FORMAT
NRDC	NATIONAL REPOSITORY OF DIGITAL CERTIFICATES
OID	OBJECT IDENTIFIER
PIN	PERSONAL IDENTIFICATION NUMBER
PKCS	PUBLIC-KEY CRYPTOGRAPHY STANDARD



ACRONYM	TERM
PKI	PUBLIC KEY INFRASTRUCTURE
RA	REGISTRATION AUTHORITY
RCAI	ROOT CERTIFYING AUTHORITY OF INDIA
RFC	REQUEST FOR COMMENT
S/MIME	SECURE MULTIPURPOSE INTERNET MAIL EXTENSIONS
SSL	SECURE SOCKETS LAYER
SUB-CA	SUBORDINATE CERTIFYING AUTHORITY
URI	UNIFORM RESOURCE INDICATOR
URL	UNIFORM RESOURCE LOCATOR

## **9.2 DEFINITIONS**

**Table 10: Defined Terms**

TERM	DEFINITION
ADMINISTRATOR	A TRUSTED PERSON THAT PERFORMS VALIDATION AND OTHER CA OR RA FUNCTIONS
ADMINISTRATOR SUB-CA	A SUBORDINATE CA ISSUING CERTIFICATES SOLELY TO PKI ADMINISTRATORS
CERTIFICATE	DIGITAL SIGNATURE CERTIFICATE ISSUED UNDER SUBSECTION (4) OF SECTION 35 OF THE INDIAN IT-ACT 2000.  A MESSAGE THAT, AT LEAST, IDENTIFIES THE CA, IDENTIFIES THE SUBSCRIBER, CONTAINS THE SUBSCRIBER'S PUBLIC KEY, IDENTIFIES THE CERTIFICATE'S OPERATIONAL PERIOD, CONTAINS A CERTIFICATE SERIAL NUMBER AND IS DIGITALLY SIGNED BY THE CA.



TERM	DEFINITION
<b>CERTIFICATE ACCEPTANCE</b>	<p><b>THE SUBSCRIBER’S ACT OF DEMONSTRATING APPROVAL OF THE CERTIFICATE.</b></p> <p><b>AS PER THE IT-ACT 2000: “A SUBSCRIBER SHALL BE DEEMED TO HAVE ACCEPTED A DIGITAL CERTIFICATE IF HE PUBLISHES OR AUTHORIZES THE PUBLICATION OF A DIGITAL SIGNATURE CERTIFICATE-</b></p> <p><b>(A) TO ONE OR MORE PERSONS;</b></p> <p><b>(B) IN A REPOSITORY, OR OTHERWISE DEMONSTRATES HIS APPROVAL OF THE DIGITAL SIGNATURE CERTIFICATE IN ANY MANNER.”</b></p>
<b>CERTIFICATE APPLICANT</b>	<p><b>AN INDIVIDUAL OR ORGANIZATION THAT REQUESTS THE ISSUANCE OF A CERTIFICATE BY A MTNLTRUSTLINE CA OR SUB-CA.</b></p>
<b>CERTIFICATE APPLICATION</b>	<p><b>A REQUEST FROM A CERTIFICATE APPLICANT (OR AUTHORIZED AGENT OF THE CERTIFICATE APPLICANT) TO A CA OR SUB-CA FOR THE ISSUANCE OF A CERTIFICATE.</b></p>
<b>CERTIFICATE CHAIN</b>	<p><b>AN ORDERED LIST OF CERTIFICATES CONTAINING AN END USER SUBSCRIBER CERTIFICATE AND CA CERTIFICATES, WHICH TERMINATES IN A ROOT CERTIFICATE.</b></p>
<b>CERTIFICATE ISSUANCE</b>	<p><b>THE SIGNING OF A CERTIFICATE BY A CA OR SUB-CA.</b></p>
<b>CERTIFICATE POLICY (CP)</b>	<p><b>AN EXPLICIT SET OF RULES GOVERNING THE APPLICATION OF A CERTIFICATE TO A SPECIFIC APPLICATION OR COMMUNITY WITHIN THE MTNLTRUSTLINE PKI. THIS DOCUMENT.</b></p>
<b>CERTIFICATE RENEWAL</b>	<p><b>RENEWAL OF A CERTIFICATE WITHIN ITS VALIDITY PERIOD GENERALLY TO EXTEND THE VALIDITY.</b></p>
<b>CERTIFICATE REPLACEMENT</b>	<p><b>REPLACEMENT OF A CERTIFICATE WITHIN ITS VALIDITY PERIOD WITHOUT EXTENDING THE CERTIFICATE VALIDITY PERIOD.</b></p>
<b>CERTIFICATE REVOCATION</b>	<p><b>THE ACT OF INVALIDATING A CERTIFICATE AS A TRUSTED SECURITY CREDENTIAL PRIOR TO THE NATURAL EXPIRATION OF ITS VALIDITY PERIOD.</b></p>



TERM	DEFINITION
<b>CERTIFICATE REVOCATION LIST (CRL)</b>	<p>A PERIODICALLY (OR EXIGENTLY) ISSUED LIST, DIGITALLY SIGNED BY A CA OR SUB-CA, OF IDENTIFIED CERTIFICATES THAT HAVE BEEN REVOKED PRIOR TO THEIR EXPIRATION DATES. THE LIST GENERALLY INDICATES THE CRL ISSUER'S NAME, THE DATE OF ISSUE, THE DATE OF THE NEXT SCHEDULED CRL ISSUE, THE REVOKED CERTIFICATES' SERIAL NUMBERS, AND THE SPECIFIC TIMES AND REASONS FOR REVOCATION.</p>
<b>CERTIFICATE SIGNING REQUEST (CSR)</b>	<p>A MESSAGE CONVEYING A REQUEST TO HAVE A CERTIFICATE ISSUED.</p>
<b>CERTIFICATE SUBJECT</b>	<p>THE ENTITY IDENTIFIED AS THE OWNER OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY LISTED IN THE CERTIFICATE.</p>
<b>CERTIFICATE SUBSCRIBER</b>	<p>SEE CERTIFICATE SUBJECT.</p>
<b>CERTIFICATION PRACTICE STATEMENT (CPS)</b>	<p>A STATEMENT OF THE PRACTICES THAT MTNLTRUSTLINE OR A CUSTOMER EMPLOYS IN APPROVING OR REJECTING CERTIFICATE APPLICATIONS AND ISSUING, REVOKING, AND RENEWING CERTIFICATES.</p>
<b>CERTIFYING AUTHORITY (CA)</b>	<p>MEANS A PERSON WHO HAS BEEN GRANTED A LICENCE TO ISSUE A DIGITAL SIGNATURE CERTIFICATE UNDER SECTION 24 OF THE INDIAN IT-ACT 2000.</p> <p>AN ENTITY AUTHORIZED TO ISSUE, MANAGE, REVOKE, AND RENEW CERTIFICATES IN THE MTNLTRUSTLINE PKI.</p>
<b>CLASS</b>	<p>A SPECIFIED LEVEL OF ASSURANCES AS DEFINED WITHIN CP § <a href="#">1.1.4</a>.</p>
<b>COMPLIANCE AUDIT</b>	<p>A PERIODIC AUDIT THAT THE MTNLTRUSTLINE OR ITS CUSTOMER UNDERGOES TO DETERMINE ITS CONFORMANCE WITH MTNLTRUSTLINE PKI REQUIREMENTS THAT APPLY TO IT.</p>
<b>COMPROMISE</b>	<p>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.</p> <p>WITH RESPECT TO PRIVATE KEYS, A COMPROMISE IS A LOSS, THEFT, DISCLOSURE, MODIFICATION, UNAUTHORIZED USE, OR OTHER COMPROMISE OF THE SECURITY OF SUCH PRIVATE KEY.</p>

TERM	DEFINITION
<b>CONFIDENTIAL INFORMATION</b>	<b>INFORMATION REQUIRED TO BE KEPT CONFIDENTIAL PURSUANT TO CP § <a href="#">2.8.1</a>.</b>
<b>CUSTODIAN</b>	<b>A MTNLTrustLine Trusted Person who holds a Secret Share.</b>
<b>CUSTOMER</b>	<p><b>AN INDIVIDUAL OR ORGANIZATION THAT HAS PURCHASED A PRODUCT OR SERVICE FROM MTNLTrustLine AND/OR ITS REPRESENTATIVES.</b></p> <p><b>ORGANIZATIONAL CUSTOMERS INCLUDE ORGANIZATIONS THAT ARE SUB-CAs AND/ OR RAs WITHIN THE MTNLTrustLine PKI.</b></p>
<b>DIGITAL CERTIFICATE</b>	<b>SEE CERTIFICATE.</b>
<b>DIGITAL SIGNATURE</b>	<b>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 INDIAN IT-ACT 2000.</b>
<b>ENCRYPTION</b>	<p><b>THE TRANSLATION OF DATA INTO A SECRET CODE. ENCRYPTION IS THE MOST EFFECTIVE WAY TO ACHIEVE DATA SECURITY. TO READ ENCRYPTED DATA, YOU MUST HAVE ACCESS TO A SECRET KEY THAT ENABLES YOU TO DECRYPT IT. UNENCRYPTED DATA IS CALLED PLAIN TEXT; ENCRYPTED DATA IS REFERRED TO AS CIPHER TEXT.</b></p> <p><b>THERE ARE TWO MAIN TYPES OF ENCRYPTION: ASYMMETRIC ENCRYPTION (ALSO CALLED PUBLIC-KEY ENCRYPTION) AND SYMMETRIC ENCRYPTION.</b></p>
<b>INDIAN IT-ACT 2000</b>	<b>THE TERM IT-ACT REFERS TO THE ACT OF PARLIAMENT OF INDIA AND ITS ASSOCIATED RULES, REGULATIONS, AND GUIDELINES. THE 'IT-ACT' PROVIDES THE LEGAL FRAMEWORK FOR OFFERING CA SERVICES IN INDIA.</b>
<b>MTNLTrustLine</b>	<b>A UNIT OF MAHANAGAR TELEPHONE NIGAM LIMITED (MTNL), ONE OF INDIA'S LEADING TELECOM SERVICE PROVIDER, OPERATING THE MTNLTrustLine PKI – A CA LICENSED UNDER THE 'IT-ACT'.</b>
<b>MTNLTrustLine PKI PARTICIPANTS</b>	<b>AN INDIVIDUAL OR ORGANIZATION THAT IS ONE OR MORE OF THE FOLLOWING WITHIN THE MTNLTrustLine PKI: MTNLTrustLine, A CUSTOMER (SUB-CA AND/OR RA), A SUBSCRIBER, OR A RELYING PARTY.</b>
<b>MTNLTrustLine Security Policy</b>	<b>THE HIGHEST-LEVEL DOCUMENT DESCRIBING MTNLTrustLine'S SECURITY POLICIES.</b>



TERM	DEFINITION
<b>MTNLTRUSTLINE REPOSITORY</b>	<b>MTNLTRUSTLINE'S DATABASE OF RELEVANT MTNLTRUSTLINE PKI INFORMATION ACCESSIBLE ONLINE.</b>
<b>NON-REPUDIATION</b>	<p><b>AN ATTRIBUTE OF A COMMUNICATION THAT PROVIDES PROTECTION AGAINST A PARTY TO A COMMUNICATION FALSELY DENYING ITS ORIGIN, DENYING THAT IT WAS SUBMITTED, OR DENYING ITS DELIVERY. DENIAL OF ORIGIN INCLUDES THE DENIAL THAT A COMMUNICATION ORIGINATED FROM THE SAME SOURCE AS A SEQUENCE OF ONE OR MORE PRIOR MESSAGES, EVEN IF THE IDENTITY ASSOCIATED WITH THE SENDER IS UNKNOWN.</b></p> <p><b>NOTE: ONLY ADJUDICATION BY A COURT, ARBITRATION PANEL, CCA, OR OTHER TRIBUNAL CAN ULTIMATELY PREVENT REPUDIATION.</b></p> <p><b>FOR EXAMPLE, A DIGITAL SIGNATURE VERIFIED WITH REFERENCE TO A MTNLTRUSTLINE CERTIFICATE MAY PROVIDE PROOF IN SUPPORT OF A DETERMINATION OF NON REPUDIATION, BUT DOES NOT BY ITSELF CONSTITUTE NON REPUDIATION.</b></p>
<b>OFFLINE SUBORDINATE CERTIFYING AUTHORITY (OFFLINE SUB-CA)</b>	<b>A CERTIFYING AUTHORITY WHOSE CERTIFICATE IS LOCATED WITHIN A CERTIFICATE CHAIN BETWEEN THE CERTIFICATE OF THE MTNLTRUSTLINE PRIMARY CA AND THE CERTIFICATE OF THE MTNLTRUSTLINE ONLINE SUB-CA THAT ISSUED THE END USER SUBSCRIBER'S CERTIFICATE.</b>
<b>ONLINE SUBORDINATE CERTIFYING AUTHORITY (ONLINE SUB-CA)</b>	<b>A CERTIFYING AUTHORITY THAT ISSUES THE END USER SUBSCRIBER CERTIFICATES.</b>
<b>PKCS #10</b>	<b>PUBLIC-KEY CRYPTOGRAPHY STANDARD #10, DEVELOPED BY RSA SECURITY INC., WHICH DEFINES A STRUCTURE FOR A CERTIFICATE SIGNING REQUEST.</b>
<b>PKCS #12</b>	<b>PUBLIC-KEY CRYPTOGRAPHY STANDARD #12, DEVELOPED BY RSA SECURITY INC., WHICH DEFINES A SECURE MEANS FOR THE TRANSFER OF PRIVATE KEYS.</b>
<b>PRIMARY CERTIFYING AUTHORITY</b>	<b>A MTNLTRUSTLINE PKI CERTIFYING AUTHORITY WHOSE CERTIFICATE IS SIGNED BY THE RCAI.</b>



TERM	DEFINITION
<b>PUBLIC KEY CRYPTOGRAPHY</b>	A CRYPTOGRAPHIC SYSTEM THAT USES TWO KEYS - A PUBLIC KEY KNOWN TO EVERYONE AND A PRIVATE KEY KNOWN ONLY TO THE SUBSCRIBER. AN IMPORTANT ELEMENT TO THE PUBLIC KEY SYSTEM IS THAT THE PUBLIC AND PRIVATE KEYS ARE RELATED IN SUCH A WAY THAT ONLY THE PRIVATE KEY CAN BE USED TO SIGN MESSAGES AND ONLY THE CORRESPONDING PUBLIC KEY CAN BE USED TO VERIFY THE DIGITAL SIGNATURES. MOREOVER, IT IS VIRTUALLY IMPOSSIBLE TO DEDUCE THE PRIVATE KEY FROM THE PUBLIC KEY.
<b>PUBLIC KEY INFRASTRUCTURE (PKI)</b>	REFERS TO THE SOFTWARE, HARDWARE, NETWORKS, SERVICES AND OPERATIONAL/ADMINISTRATIVE PROCESSES THAT MANAGE PUBLIC KEY CERTIFICATES AND ASYMMETRIC KEY PAIRS
<b>REGISTRATION AUTHORITY (RA)</b>	AN ENTITY APPROVED BY MTNLTRUSTLINE TO ASSIST CERTIFICATE APPLICANTS IN APPLYING FOR CERTIFICATES, AND TO APPROVE OR REJECT CERTIFICATE APPLICATIONS, REVOKE CERTIFICATES, OR RENEW CERTIFICATES.
<b>RELYING PARTY</b>	AN INDIVIDUAL OR ORGANIZATION THAT ACTS IN RELIANCE ON A CERTIFICATE AND/OR A DIGITAL SIGNATURE.
<b>RELYING PARTY AGREEMENT</b>	AN AGREEMENT USED BY MTNLTRUSTLINE SETTING FORTH THE TERMS AND CONDITIONS UNDER WHICH AN INDIVIDUAL OR ORGANIZATION ACTS AS A RELYING PARTY.
<b>RSA</b>	A PUBLIC KEY CRYPTOGRAPHIC SYSTEM INVENTED BY RIVEST, SHAMIR, AND ADELMAN.
<b>SECRET SHARE</b>	A PORTION OF A CA PRIVATE KEY OR A PORTION OF THE ACTIVATION DATA NEEDED TO OPERATE A CA PRIVATE KEY UNDER A SECRET SHARING ARRANGEMENT.
<b>SECRET SHARING</b>	THE PRACTICE OF SPLITTING A CA PRIVATE KEY OR THE ACTIVATION DATA TO OPERATE A CA PRIVATE KEY IN ORDER TO ENFORCE MULTI-PERSON CONTROL OVER CA PRIVATE KEY OPERATIONS UNDER CPS § <a href="#">6.2.2</a> .
<b>SUBJECT</b>	THE HOLDER OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY. THE TERM "SUBJECT" CAN, IN THE CASE OF AN ORGANIZATIONAL CERTIFICATE, REFER TO THE EQUIPMENT OR DEVICE THAT HOLDS A PRIVATE KEY. A SUBJECT IS ASSIGNED AN UNAMBIGUOUS NAME, WHICH IS BOUND TO THE PUBLIC KEY CONTAINED IN THE SUBJECT'S CERTIFICATE.



TERM	DEFINITION
<b>SUBSCRIBER</b>	<b>IN THE CASE OF AN INDIVIDUAL CERTIFICATE, A PERSON WHO IS THE SUBJECT OF, AND HAS BEEN ISSUED, A CERTIFICATE. IN THE CASE OF AN ORGANIZATIONAL CERTIFICATE, AN ORGANIZATION THAT OWNS THE EQUIPMENT OR DEVICE THAT IS THE SUBJECT OF, AND THAT HAS BEEN ISSUED, A CERTIFICATE. A SUBSCRIBER IS CAPABLE OF USING, AND IS AUTHORIZED TO USE, THE PRIVATE KEY THAT CORRESPONDS TO THE PUBLIC KEY LISTED IN THE CERTIFICATE.</b>
<b>SUBSCRIBER AGREEMENT</b>	<b>AN AGREEMENT USED BY A MTNLTRUSTLINE SETTING FORTH THE TERMS AND CONDITIONS UNDER WHICH AN INDIVIDUAL OR ORGANIZATION ACTS AS A SUBSCRIBER.</b>
<b>SUPERIOR ENTITY</b>	<b>AN ENTITY ABOVE A CERTAIN ENTITY WITHIN THE MTNLTRUSTLINE PKI.</b>
<b>TRUSTED PERSON</b>	<b>AN EMPLOYEE, CONTRACTOR, OR CONSULTANT OF AN ENTITY WITHIN THE MTNLTRUSTLINE PKI RESPONSIBLE FOR MANAGING INFRASTRUCTURAL TRUSTWORTHINESS OF THE ENTITY, ITS PRODUCTS, ITS SERVICES, ITS FACILITIES, AND/OR ITS PRACTICES AS FURTHER DEFINED IN CP § <a href="#">5.2.1</a>.</b>
<b>TRUSTED POSITION</b>	<b>THE POSITIONS WITHIN A MTNLTRUSTLINE PKI ENTITY THAT MUST BE HELD BY A TRUSTED PERSON.</b>
<b>TRUSTWORTHY SYSTEM</b>	<b>COMPUTER HARDWARE, SOFTWARE, AND PROCEDURES THAT ARE REASONABLY SECURE FROM INTRUSION AND MISUSE; PROVIDE A REASONABLE LEVEL OF AVAILABILITY, RELIABILITY, AND CORRECT OPERATION; ARE REASONABLY SUITED TO PERFORMING THEIR INTENDED FUNCTIONS; AND ENFORCE THE APPLICABLE SECURITY POLICY.</b>
<b>VALIDITY PERIOD</b>	<b>THE PERIOD STARTING WITH THE DATE AND TIME A CERTIFICATE IS ISSUED (OR ON A LATER DATE AND TIME CERTAIN IF STATED IN THE CERTIFICATE) AND ENDING WITH THE DATE AND TIME ON WHICH THE CERTIFICATE EXPIRES OR IS EARLIER REVOKED.</b>
<b>WIRELESS APPLICATION PROTOCOL (WAP)</b>	<b>A STANDARD FOR THE PRESENTATION AND DELIVERY OF WIRELESS INFORMATION AND TELEPHONY SERVICES ON MOBILE PHONES AND OTHER WIRELESS TERMINALS.</b>



TERM	DEFINITION
<b>WIRELESS TRANSPORT LAYER SECURITY (WTLS)</b>	<b>A PROTOCOL THAT PROTECTS THE COMMUNICATION OF APPLICATIONS THAT OPERATE USING THE WIRELESS APPLICATION PROTOCOL, SUCH AS COMMUNICATIONS BETWEEN A WIRELESS HANDSET AND A SERVER.</b>
<b>WIRELESS TRANSPORT LAYER SECURITY CERTIFICATE (WTLS CERTIFICATE)</b>	<b>A CERTIFICATE WHOSE FORMAT IS DEFINED AS PART OF THE WIRELESS APPLICATION PROTOCOL, WHICH AUTHENTICATES A WIRELESS TRANSPORT LAYER SECURITY SERVER TO A WTLS CLIENT AND FACILITATES ENCRYPTED COMMUNICATION BETWEEN THE WTLS SERVER AND THE WTLS CLIENT.</b>

