



MTNLTRUSTLINE

CERTIFICATION PRACTICE STATEMENT (CPS)

VERSION -2.0

EFFECTIVE DATE: 15th December 2008



MAHANAGAR TELEPHONE NIGAM LIMITED

JEEVAN BHARATI, 124 CONNAUGHT CIRCUS, NEW DELHI - 110 001

**MTNLTRUSTLINE MTNL-CPS**

Document Version:	2.0
Date:	18 November 2008
Owner:	DGM (IT-CA)
Document ID:	MTNL-TL/PRO/V 1.0/210
File Name:	MTNL-CPS.pdf
Abstract:	AGM (IT-CA)
Prepared by:	STEERING COMMITTEE
Reviewed by	DGM (IT-CA)
Approved by:	GM (IT)
Effective Date:	15TH December 2008



LEGAL NOTICE

Unauthorized access to and use of this document is prohibited by law. Any individual attempting unauthorized access, copying, distributing, or exploiting information within this document will be subjected to legal prosecution. The MTNLTRUSTLINE operations, including the policies and procedures, the terms and conditions, shall be governed by relevant Indian Laws in force.



Document Control Matrix

Sr. No.	Version	Date	Prepared by	Reviewed by	Approved by
1	1.0	13/01/2004	Ms.Vandana Gupta (DGM CA)	Mr. Sanjay Padmane (DGM CA)	Mr. A K Bhargava (GM IT)
2	2.0	15/12/2008	STEERING COMMITTEE	DGM (IT-CA)	GM (IT)



NOTE

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

This Certification Practice Statement 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 CPS § 1.3.

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

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



TABLE OF CONTENTS

1 INTRODUCTION	1
1.1 OVERVIEW.....	2
1.1.1 COMPLIANCE WITH IT ACT.....	3
1.1.2 ROLE OF THE CPS AND OTHER DOCUMENTS	3
1.1.3 RELATIONSHIP WITH CONTROLLER OF CERTIFYING AUTHORITY	4
1.1.4 OVERVIEW OF CERTIFICATE CLASSES ISSUED BY MTNLTRUSTLINE	5
1.1.4.1 CLASS 1 CERTIFICATES.....	5
1.1.4.2 CLASS 2 CERTIFICATES.....	6
1.1.4.3 CLASS 3 CERTIFICATES.....	6
1.1.5 SERVICES OFFERED BY MTNLTRUSTLINE.....	7
1.1.6 MTNLTRUSTLINE PKI HIERARCHY.....	9
1.2 IDENTIFICATION	10
1.3 COMMUNITY AND APPLICABILITY.....	10
1.3.1 CERTIFYING AUTHORITIES (CAs)	10
1.3.2 REGISTRATION AUTHORITIES (RAs)	11
1.3.3 END ENTITIES.....	12
1.3.3.1 SUBSCRIBERS.....	12
1.3.3.2 RELYING PARTIES.....	13
1.3.4 APPLICABILITY.....	14
1.3.4.1 SUITABLE APPLICATIONS.....	14
1.3.4.1.1 SUITABLE APPLICATIONS FOR CLASS 1 CERTIFICATES	15
1.3.4.1.2 SUITABLE APPLICATIONS FOR CLASS 2 CERTIFICATES	15
1.3.4.1.3 SUITABLE APPLICATIONS FOR CLASS 3 CERTIFICATES	16
1.3.4.2 RESTRICTED APPLICATIONS.....	16
1.3.4.3 PROHIBITED APPLICATIONS.....	17
1.4 CONTACT DETAILS.....	17
2 GENERAL PROVISIONS	18
2.1 OBLIGATIONS	18
2.1.1 CA OBLIGATIONS.....	18
2.1.2 RA OBLIGATIONS.....	19
2.1.3 SUBSCRIBER OBLIGATIONS.....	19
2.1.4 RELYING PARTY OBLIGATIONS	20
2.1.5 REPOSITORY OBLIGATIONS.....	22
2.2 LIABILITY	22
2.2.1 CA LIABILITY.....	22
2.2.1.1 WARRANTIES TO SUBSCRIBERS AND RELYING PARTIES.....	22
2.2.1.2 DISCLAIMERS OF WARRANTIES.....	23
2.2.1.3 LIMITATIONS OF LIABILITY.....	23
2.2.1.4 FORCE MAJEURE.....	23
2.2.2 RA LIABILITY.....	24
2.2.3 SUBSCRIBER LIABILITY.....	24
2.2.3.1 SUBSCRIBER WARRANTIES.....	24
2.2.3.2 PRIVATE KEY COMPROMISE	25
2.2.4 RELYING PARTY LIABILITY	25
2.3 FINANCIAL RESPONSIBILITY	25
2.3.1 INDEMNIFICATION BY SUBSCRIBERS AND RELYING PARTIES.....	25
2.3.1.1 INDEMNIFICATION BY SUBSCRIBERS	25
2.3.1.2 INDEMNIFICATION BY RELYINGPARTIES.....	26
2.3.2 FIDUCIARY RELATIONSHIPS.....	26
2.3.3 ADMINISTRATIVE PROCESSES	27
2.4 INTERPRETATION AND ENFORCEMENT	27
2.4.1 GOVERNING LAW	27



2.4.2	SEVERABILITY, SURVIVAL, MERGER, NOTICE	27
2.4.3	DISPUTE RESOLUTION PROCEDURES	27
2.4.3.1	ROLE OF THE CCA	28
2.5	FEES.....	28
2.5.1	CERTIFICATE ISSUANCE OR RENEWAL FEES	28
2.5.2	CERTIFICATE ACCESS FEES.....	28
2.5.3	REVOCATION OR STATUS INFORMATION ACCESS FEES.....	28
2.5.4	FEES FOR OTHER SERVICES SUCH AS POLICY INFORMATION.....	29
2.5.5	REFUND POLICY.....	29
2.6	PUBLICATION AND REPOSITORIES	29
2.6.1	PUBLICATION OF CA INFORMATION.....	29
2.6.2	FREQUENCY OF PUBLICATION.....	30
2.6.3	ACCESS CONTROLS.....	30
2.6.4	REPOSITORIES	31
2.7	COMPLIANCE AUDIT	31
2.7.1	FREQUENCY OF COMPLIANCE AUDIT	31
2.7.2	IDENTITY/ QUALIFICATIONS OF AUDITOR.....	31
2.7.2.1	SELF-AUDITS.....	31
2.7.3	AUDITOR'S RELATIONSHIP TO AUDITED PARTY.....	31
2.7.4	TOPICS COVERED BY AUDIT.....	32
2.7.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY	33
2.7.6	COMMUNICATIONS OF RESULTS.....	33
2.8	CONFIDENTIALITY POLICY.....	33
2.8.1	TYPES OF INFORMATION TO BE KEPT CONFIDENTIAL	33
2.8.2	TYPES OF INFORMATION NOT CONSIDERED CONFIDENTIAL.....	34
2.8.3	DISCLOSURE OF CERTIFICATE REVOCATION/SUSPENSION INFORMATION.....	34
2.8.4	RELEASE TO LAW ENFORCEMENT OFFICIALS.....	34
2.8.5	RELEASE AS PART OF CIVIL DISCOVERY.....	35
2.8.6	DISCLOSURE UPON OWNER'S REQUEST.....	35
2.8.7	OTHER INFORMATION RELEASE CIRCUMSTANCES.....	35
2.9	INTELLECTUAL PROPERTY RIGHTS	35
2.9.1	RIGHTS IN CERTIFICATES.....	35
2.9.2	RIGHTS IN THE CP & CPS	35
2.9.3	RIGHTS IN NAMES	36
2.9.4	RIGHTS IN KEYS AND KEY MATERIAL.....	36
3	IDENTIFICATION AND AUTHENTICATION	37
3.1	INITIAL REGISTRATION.....	37
3.1.1	TYPES OF NAMES	37
3.1.2	MEANING OF NAMES.....	39
3.1.3	RULES FOR INTERPRETING VARIOUS NAME FORMS	39
3.1.4	UNIQUENESS OF NAMES	39
3.1.5	NAME CLAIM DISPUTE RESOLUTION.....	39
3.1.6	RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS	40
3.1.7	METHOD TO PROVE POSSESSION OF PRIVATE KEY.....	40
3.1.8	AUTHENTICATION OF ORGANIZATION IDENTITY.....	40
3.1.8.1	AUTHENTICATION OF ORGANIZATION IDENTITY.....	40
3.1.8.2	CLASS2 CERTIFICATES FOR DEVICES.....	41
3.1.8.3	CLASS3 SERVER CERTIFICATES.....	41
3.1.8.4	AUTHENTICATION OF THE IDENTITY OF SUB-CAS AND RAS.....	41
3.1.9	AUTHENTICATION OF INDIVIDUAL IDENTITY	42
3.1.9.1	CLASS1 CERTIFICATES.....	42
3.1.9.2	CLASS2 CERTIFICATES.....	43
3.1.9.3	CLASS3 CERTIFICATES.....	43



3.2 ROUTINE REKEY (RENEWAL)	44
3.2.1 RENEWAL OF END USER SUBSCRIBER CERTIFICATES	44
3.2.2 RENEWAL OF SUB-CA CERTIFICATES.....	44
3.3 REKEY AFTER REVOCATION -NO KEY COMPROMISE	44
3.4 REVOCATION REQUESTS	45
4 OPERATIONAL REQUIREMENTS	46
4.1 CERTIFICATE APPLICATION.....	46
4.1.1 ENROLLMENT FOR END USER SUBSCRIBER CERTIFICATES.....	46
4.1.2 ENROLLMENT FOR SUB-CA OR RA CERTIFICATES	46
4.2 CERTIFICATE ISSUANCE.....	47
4.2.1 ISSUANCE OF END USER SUBSCRIBER CERTIFICATES.....	47
4.2.2 ISSUANCE OF SUB-CA AND RA CERTIFICATES.....	47
4.3 CERTIFICATE ACCEPTANCE.....	48
4.4 CERTIFICATE SUSPENSION AND REVOCATION	48
4.4.1 CIRCUMSTANCES FOR REVOCATION.....	48
4.4.1.1 CIRCUMSTANCES FOR REVOKING END USER SUBSCRIBER CERTIFICATES.....	48
4.4.1.2 CIRCUMSTANCES FOR REVOKING SUB-CA OR RA CERTIFICATES.....	49
4.4.2 WHO CAN REQUEST REVOCATION	50
4.4.2.1 WHO CAN REQUEST REVOCATION OF AN END USER SUBSCRIBER CERTIFICATE.....	50
4.4.2.2 WHO CAN REQUEST REVOCATION OF A SUB-CA OR RA CERTIFICATE.....	50
4.4.3 PROCEDURE FOR REVOCATION REQUEST.....	50
4.4.3.1 PROCEDURE FOR REVOCATION REQUEST OF AN END USER SUBSCRIBER CERTIFICATE.....	50
4.4.3.2 PROCEDURE FOR REVOCATION REQUEST OF A SUB-CA OR RA CERTIFICATE.....	51
4.4.4 REVOCATION REQUEST GRACE PERIOD	51
4.4.5 CIRCUMSTANCES FOR SUSPENSION.....	51
4.4.6 WHO CAN REQUEST SUSPENSION	51
4.4.7 PROCEDURE FOR SUSPENSION REQUEST.....	51
4.4.8 LIMITS ON SUSPENSION PERIOD.....	51
4.4.9 CRL ISSUANCE FREQUENCY	52
4.4.10 CERTIFICATE REVOCATION LIST CHECKING REQUIREMENTS.....	52
4.4.11 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY	52
4.4.12 ON-LINE REVOCATION CHECKING REQUIREMENTS	52
4.4.13 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE	53
4.4.14 CHECKING REQUIREMENTS FOR OTHER FORMS OF REVOCATION ADVERTISEMENTS ..	53
4.4.15 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE.....	53
4.5 SECURITY AUDIT PROCEDURES	53
4.5.1 TYPES OF EVENTS RECORDED	53
4.5.1.1 EVENTS RECORDED BY MTNLTRUSTLINE CA	53
4.5.1.2 EVENTS RECORDED BY MTNLTRUSTLINE RAs.....	54
4.5.2 FREQUENCY WITH WHICH AUDIT LOGS ARE PROCESSED	55
4.5.3 PERIOD FOR WHICH AUDIT LOGS ARE KEPT	56
4.5.4 PROTECTION OF AUDIT LOG	56
4.5.5 AUDIT LOG BACKUP PROCEDURES	56
4.5.6 AUDIT LOG ACCUMULATION SYSTEM (INTERNAL OR EXTERNAL)	56
4.5.7 NOTIFICATION TO EVENT-CAUSING SUBJECT	56
4.5.8 VULNERABILITY ASSESSMENTS.....	56
4.6 RECORDS ARCHIVAL.....	57
4.6.1 TYPES OF EVENT RECORDED.....	57
4.6.2 RETENTION PERIOD FOR ARCHIVE	57
4.6.3 PROTECTION OF ARCHIVE.....	58
4.6.4 ARCHIVE BACKUP PROCEDURES.....	58
4.6.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS	58
4.6.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)	58
4.6.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION.....	58
4.7 KEY CHANGEOVER	59



4.8	COMPROMISES AND DISASTER RECOVERY.....	59
4.8.1	COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED.....	60
4.8.2	ENTITY PUBLIC KEY IS REVOKED.....	60
4.8.3	ENTITY KEY IS COMPROMISED	60
4.8.4	SECURE FACILITY AFTER A NATURAL OR OTHER TYPE OF DISASTER.....	60
4.9	CA TERMINATION.....	61
5.	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	63
5.1	PHYSICAL SECURITY CONTROLS	63
5.1.1	SITE LOCATION AND CONSTRUCTION.....	63
5.1.2	PHYSICAL ACCESS	64
5.1.3	POWER AND AIR CONDITIONING.....	64
5.1.4	WATER EXPOSURES	64
5.1.5	FIRE PREVENTION AND PROTECTION.....	64
5.1.6	MEDIA STORAGE.....	65
5.1.7	WASTE DISPOSAL.....	65
5.1.8	OFF-SITE BACKUP.....	65
5.2	PROCEDURAL CONTROLS.....	65
5.2.1	TRUSTED ROLES	65
5.2.2	NUMBER OF PERSONS REQUIRED PER TASK	66
5.2.3	IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE	67
5.3	PERSONNEL SECURITY CONTROLS	67
5.3.1	BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS.....	67
5.3.2	BACKGROUND CHECK PROCEDURES	67
5.3.3	TRAINING REQUIREMENTS AND TRAINING PROCEDURES.....	68
5.3.4	RETRAINING FREQUENCY AND REQUIREMENTS	69
5.3.5	JOB ROTATION FREQUENCY AND SEQUENCE.....	69
5.3.6	SANCTIONS FOR UNAUTHORIZED ACTIONS	69
5.3.7	CONTRACTING PERSONNEL REQUIREMENTS	69
5.3.8	DOCUMENTATION SUPPLIED TO PERSONNEL.....	70
6	TECHNICAL SECURITY CONTROLS.....	71
6.1	KEY PAIR GENERATION AND INSTALLATION	71
6.1.1	KEY PAIR GENERATION AND INSTALLATION.....	71
6.1.3	PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER.....	71
6.1.4	CA PUBLIC KEY DELIVERY TO USERS	72
6.1.5	KEY SIZES.....	72
6.1.6	PUBLIC KEY PARAMETERS GENERATION.....	72
6.1.7	PARAMETER QUALITY CHECKING	72
6.1.8	HARDWARE OR SOFTWARE KEY GENERATION	73
6.1.9	KEY USAGE PURPOSES	73
6.2	PRIVATE KEY PROTECTION.....	74
6.2.1	STANDARDS FOR CRYPTOGRAPHIC MODULES.....	74
6.2.2	PRIVATE KEY 'N OUT OF M' MULTI-PERSON CONTROL.....	74
6.2.3	PRIVATE KEY ESCROW	75
6.2.4	PRIVATE KEY BACKUP.....	75
6.2.5	PRIVATE KEY ARCHIVAL.....	75
6.2.6	PRIVATE KEY ENTRY INTO CRYPTOGRAPHIC MODULE.....	75
6.2.7	METHOD OF ACTIVATING PRIVATE KEY.....	76
6.2.7.1	END USER SUBSCRIBER PRIVATE KEYS.....	76
6.2.7.2	CA/SUB-CA PRIVATE KEYS	77
6.2.8	METHOD OF DEACTIVATING PRIVATE KEY.....	77
6.2.9	METHOD OF DESTROYING PRIVATE KEY.....	78
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	78
6.3.1	PUBLIC KEY ARCHIVAL	78
6.3.2	USAGE PERIODS FOR THE PUBLIC AND PRIVATE KEYS.....	78
6.4	ACTIVATION DATA.....	79
6.4.1	ACTIVATION DATA GENERATION AND INSTALLATION.....	79
6.4.2	ACTIVATION DATA PROTECTION	79
6.4.3	OTHER ASPECTS OF ACTIVATION DATA	80



6.5	COMPUTER SECURITY CONTROLS	80
6.5.1	SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS.....	80
6.5.2	COMPUTER SECURITY RATING.....	80
80	
6.6	LIFE CYCLE SECURITY CONTROLS.....	81
6.6.1	SYSTEM DEVELOPMENT CONTROLS	81
6.6.2	SECURITY MANAGEMENT CONTROLS.....	81
6.6.3	LIFE CYCLE SECURITY RATINGS.....	81
6.7	NETWORK SECURITY CONTROLS	81
6.8	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	82
7	CERTIFICATE AND CRL PROFILES	83
7.1	CERTIFICATE PROFILE.....	83
7.1.1	VERSION NUMBER(S) SUPPORTED.....	84
7.1.2	CERTIFICATE EXTENSIONS.....	84
7.1.2.1	BASIC CONSTRAINTS	85
7.1.2.2	EXTENDED KEY USAGE	85
7.1.3	ALGORITHM OBJECT IDENTIFIERS.....	86
7.1.4	NAME FORMS.....	86
7.1.5	NAME CONSTRAINTS	86
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIER.....	86
7.1.7	USAGE OF POLICY CONSTRAINTS EXTENSION	86
7.1.8	POLICY QUALIFIERS SYNTAX AND SEMANTICS.....	87
7.1.9	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION	87
7.2	CRL PROFILE.....	87
7.2.1	VERSION NUMBER(S) SUPPORTED.....	87
7.2.2	CRL AND CRL ENTRY EXTENSIONS	87
8	SPECIFICATION ADMINISTRATION	88
8.1	SPECIFICATION CHANGE PROCEDURES.....	88
8.1.1	ITEMS THAT CAN CHANGE WITHOUT NOTIFICATION.....	88
8.1.2	ITEMS THAT CAN CHANGE WITH NOTIFICATION.....	88
8.1.2.1	LIST OF ITEMS.....	88
8.1.2.2	NOTIFICATION MECHANISM.....	88
8.1.2.3	COMMENT PERIOD.....	89
8.1.2.4	MECHANISM TO HANDLE COMMENTS.....	89
8.1.3	CHANGES REQUIRING CHANGES IN THE CERTIFICATE POLICY OID	89
8.2	PUBLICATION AND NOTIFICATION POLICIES	89
8.2.1	ITEMS NOT PUBLISHED IN THE CPS	89
8.2.2	DISTRIBUTION OF THE CPS	90
8.3	CPS APPROVAL PROCEDURES.....	90
9	LIST OF TERMS.....	91
9.1	LIST OF ACRONYMS.....	91
9.2	DEFINITIONS	92
	ANNEXURE1 - MTNLTRUSTLINE SUBSCRIBER AGREEMENT.....	117
	ANNEXURE 2 - MTNLTRUSTLINE RELYING PARTY AGREEMENT	125



1 INTRODUCTION

This document is the Certification Practice Statement (CPS) of MTNLTRUSTLINE, a service of Mahanagar Telephone Nigam Limited (MTNL). It states the practices that MTNLTRUSTLINE employs in providing Digital Certificates and related services that include, but are not limited to, Certificate Application, Approval, Issuance, Revocation, Renewal, and use in accordance with the specific requirements of the MTNLTRUSTLINE Certificate Policy (CP). The CP is the principal statement of policy governing MTNLTRUSTLINE and establishes conformance to the requirements of the IT-Act 2000.

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 recognition¹ to Digital Signatures created using Digital Certificates issued by Certifying Authorities duly licensed by the 'Controller of Certifying Authorities'.

¹ 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 is Certifying Authority (CA) set up by Mahanagar Telephone Nigam Limited (MTNL) to provide Digital Certificates and related services to entities including Individuals, Organizations, Servers, Network Devices, and 'legal persons'.

Within the framework of the IT Act 2000, MTNLTRUSTLINE is recognized as a Certifying Authority in the Public Key Infrastructure set up by the CCA for the country. MTNLTRUSTLINE is recognized as Certifying Authority under which Sub-CAs and RAs are operating. As far as the Controller of Certifying Authorities (CCA) is concerned, operations of issuance, renewal, and revocation of Certificates are carried out by MTNLTRUSTLINE as a CA.

While the MTNLTRUSTLINE CP sets forth requirements that MTNLTRUSTLINE PKI Participants must meet, this CPS describes the practices that MTNLTRUSTLINE employs for:

- Securely managing the core infrastructure that supports the MTNLTRUSTLINE.
- Issuing, managing, revoking, and renewing certificates with legal validity under the IT-Act.

1.1 OVERVIEW

This CPS is applicable to MTNLTRUSTLINE including all Certifying Authorities (CAs) and Sub-Certifying Authorities (Sub-CAs) operating under the MTNLTRUSTLINE brand umbrella.

This CPS also governs the use of services by all individuals and entities identified as MTNLTRUSTLINE PKI Participants in CPS § 1.3.

In accordance to the guidelines of IT-Act, the CP defines 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.

While the CP (CP §§ [1.1.4](#), [1.2](#), [1.3.4](#), [3.1.8](#), [3.1.9](#)) describes in detail how these three classes correspond to three classes of Applications with common security requirements, this CPS describes how MTNLTRUSTLINE meets the CP and IT-Act requirements for each class of certificates.

The CPS, as a single document, covers practices and procedures concerning the issuance, revoking, and renewing certificates of all three classes.



1.1.1 COMPLIANCE WITH IT ACT

The practices specified in this CPS have been designed to meet or exceed the requirements of the Indian IT-Act 2000.

As required by the IT-Act this CPS conforms to the framework provided in RFC 2527 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework), [<http://www.ietf.org/rfc/rfc2527.txt>] in order to make policy mapping and comparisons, assessment, and interoperation easier for persons using or considering using MTNLTRUSTLINE services.

1.1.2 ROLE OF THE CPS AND OTHER DOCUMENTS

The CP describes at a general level the overall business, legal, and technical infrastructure requirements of the MTNLTRUSTLINE. This CPS then explains specific practices of MTNLTRUSTLINE in response to the requirements of the CP. 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 are covered in MTNLTRUSTLINE Subscriber Agreements and Relying Party Agreements,
- . • Audit and related security and practices reviews undertaken by MTNLTRUSTLINE
- . • Methods used by MTNLTRUSTLINE 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 (CRL) content, and
- . • Administration of the CPS, including methods of updating it.

The CPS, however, is only one of a set of documents relevant to the MTNLTRUSTLINE. These



other documents include:

- Security and operational policy and procedure documents and manuals that supplement the CP and CPS 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 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 by design subordinate to the RCAI.

As part of the CA licensing process defined in the IT-Act the CCA has issued a CA Certificate to MTNLTRUSTLINE.

This [CA Certificate](#) signed by the RCAI authenticates the Public Key of the MTNLTRUSTLINE CA and 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>].

All other [MTNLTRUSTLINE Sub-CAs](#) chain up to this CA issued by the CCA. Thus, the CCA only signs one CA certificate of MTNLTRUSTLINE, which in turn signs other [Sub-CAs](#).

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.

All MTNLTRUSTLINE issued Certificates and CRLs are published to the NRDC.

At present, this is done offline by MTNLTRUSTLINE sending a LDIF update of all changes in its directory to NRDC at regular intervals as required by the NRDC administrator.



1.1.4 OVERVIEW OF CERTIFICATE CLASSES ISSUED BY MTNLTRUSTLINE

MTNLTRUSTLINE issues three distinct Classes of Certificates: Class 1, Class 2, and Class 3 as defined in CP § 1.1.4.

Each Class of Certificate is associated with specific security features and corresponds to a specific level of trust.

MTNLTRUSTLINE Subscribers and Relying Parties choose the Classes of Certificates they need.

1.1.4.1 CLASS 1 CERTIFICATES

Class 1 Certificates are issued to Individuals with valid e-mail addresses.

Class 1 validation procedures are based on the assurance 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.

Class 2 validation procedures are based on the assurance that subscriber's Distinguished Name (DN) is unique and unambiguous within MTNLTRUSTLINE Repository and 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 applied for by authorized individuals (administrators) who are responsible for the security of the corresponding private keys and 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 and Administrators for CAs and RAs.

The validation procedures for Class 3 Certificates issued to Individuals are 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.

The validation procedures for Class 3 Certificates issued to Organizations are 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 is 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 applied for by authorized individuals (administrators) who



are responsible for the security of the corresponding private keys and are appropriate for server authentication; message, software, and content integrity; and confidentiality encryption.

1.1.5 SERVICES OFFERED BY MTNLTRUSTLINE

MTNLTRUSTLINE has two models of managing the Issuance, Renewal, Revocation, and other Certificate lifecycle functions.

1. **RETAIL MODEL:** MTNLTRUSTLINE issues Certificates signed by a MTNLTRUSTLINE Sub-CA to Individuals or Organizations applying one by one to MTNLTRUSTLINE on its web site or to one of its designated RAs (MTNLTRUSTLINE employee) based on validation done by MTNLTRUSTLINE.
2. **ENTERPRISE MODEL** – In this model the validation and Certificate lifecycle management functions of the RA are performed by a MTNLTRUSTLINE Enterprise Customer organization.

MTNLTRUSTLINE ensures by suitable contract and agreement that this CPS and the associated CP is binding on the customer organization for the purposes of performing such functions within the MTNLTRUSTLINE PKI.

Within the enterprise model there are two models of managing the Issuance, Renewal, Revocation, and other Certificate lifecycle functions.

- a) **ENTERPRISE RA:** MTNLTRUSTLINE issues Certificates, signed by a MTNLTRUSTLINE Sub-CA, based on approval by the MTNLTRUSTLINE Enterprise Customer organization that has entered into an agreement with MTNLTRUSTLINE for issuance of a certain quantity of Certificates.
- b) **ENTERPRISE SUB-CA:** MTNLTRUSTLINE issues Certificates, signed by a Sub-CA within the MTNLTRUSTLINE PKI Hierarchy created Specifically for the MTNLTRUSTLINE Enterprise Customer organization. The validation of these Certificates is based on approval by the MTNLTRUSTLINE customer organization that has entered into an agreement with MTNLTRUSTLINE for issuance of a certain quantity of Certificates.

**TABLE 1: SPECIFIC CERTIFICATE TYPES OFFERED BY MTNLTRUSTLINE**

TYPE	CLASS	ISSUED TO	MODEL
MTNLTRUSTLINE CLASS 1 INDIVIDUAL SUBSCRIBER	CLASS 1	INDIVIDUALS	RETAIL
<CUSTOMER> CLASS 1	CLASS 1	INDIVIDUALS	ENTERPRISE SUB- CA
MTNLTRUSTLINE CLASS 2 ENTERPRISE SUBSCRIBER	CLASS 2	INDIVIDUALS	ENTERPRISE RA
<CUSTOMER> CLASS 2	CLASS 2	INDIVIDUALS	ENTERPRISE SUB- CA
MTNLTRUSTLINE CLASS 2 DEVICES	CLASS 2	DEVICES	ENTERPRISE RA
<CUSTOMER> CLASS 2 DEVICES	CLASS 2	DEVICES	ENTERPRISE SUB- CA
MTNLTRUSTLINE CLASS 3 INDIVIDUAL SUBSCRIBER	CLASS 3	INDIVIDUALS	RETAIL
MTNLTRUSTLINE CLASS 3 SERVER	CLASS 3	SERVERS	RETAIL
<CUSTOMER> CLASS 3	CLASS 3	INDIVIDUALS	ENTERPRISE SUB- CA
MTNLTRUSTLINE CLASS 3 INTERNAL ADMINISTRATOR	CLASS 3	INDIVIDUALS (MTNLTRUSTLINE RAs)	N/A
MTNLTRUSTLINE CLASS 3 EXTERNAL ADMINISTRATOR	CLASS 3	INDIVIDUALS (MTNLTRUSTLINE ENTERPRISE CUSTOMER RAs)	N/A



1.2 IDENTIFICATION

This document is the MTNLTRUSTLINE Certification Practice Statement (CPS) document. The object identifier (OID) values assigned to the MTNLTRUSTLINE Certification Practice Statement (CPS) and Certificate Policy (CP) are:

1. MTNLTRUSTLINE CPS -2.16.356.100.1.5.2
2. MTNLTRUSTLINE CP -2.16.356.100.1.5.3

MTNLTRUSTLINE PKI Certificates contain object identifier (OID) values corresponding to the applicable class of certificate as indicated below:

1. MTNLTRUSTLINE Class 1 Certificates -2.16.356.100.1.5.3.1
2. MTNLTRUSTLINE Class 2 Certificates -2.16.356.100.1.5.3.2
3. MTNLTRUSTLINE Class 3 Certificates -2.16.356.100.1.5.3.3

1.3 COMMUNITY AND APPLICABILITY

The community governed by this CPS is 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 signing Certificates within the MTNLTRUSTLINE PKI. The CA term encompasses two Sub-Categories of signers: Certifying Authority (CA) and Subordinate Certifying Authority (Sub-CA).

As depicted in the MTNLTRUSTLINE PKI Hierarchy Diagram (CPS § 1.1.6), the "mtnlTrustLine Public Primary Certifying Authority" signed by the Root Certifying Authority of India (RCAI) is the Certifying Authority at the top of the MTNLTRUSTLINE PKI hierarchy.



Subordinate to this are Offline Subordinate Certifying Authorities (Offline Sub-CAs), at least one for each Class of Certificates.

These Offline Sub-CAs sign Certificates of other Offline Sub-CAs or Online Sub-CAs.

Only Online Sub-CAs sign Certificates of end entity Subscribers. Sub CAs also fall into two categories:

1. MTNLTRUSTLINE Sub-CAs – entities managed by MTNLTRUSTLINE that are not created for any specific customer.
2. MTNLTRUSTLINE Enterprise Customer Sub-CAs - entities managed by MTNLTRUSTLINE that are created specifically for a MTNLTRUSTLINE Enterprise Sub-CA Customer.

A list of all the current CA and Sub-CAs operated by MTNLTRUSTLINE is maintained at <http://www.mtnltrustline.com/repository/ca-list.html>.

1.3.2 REGISTRATION AUTHORITIES (RAs)

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

MTNLTRUSTLINE PKI RAs fall into two categories:

1. MTNLTRUSTLINE RAs – RAs that are managed by MTNLTRUSTLINE.
2. MTNLTRUSTLINE Enterprise Customer RAs – RAs that are managed by MTNLTRUSTLINE Enterprise RA Customers or MTNLTRUSTLINE Enterprise Sub-CA Customers.

A list of all the current operational RAs of the various MTNLTRUSTLINE Sub-CAs is maintained at <http://www.mtnltrustline.com/repository/ca-list.html>



1.3.3 END ENTITIES

1.3.3.1 SUBSCRIBERS

Subscribers are end entities identified in the subject name of a Certificate signed by a MTNLTRUSTLINE CA or Sub-CA.

CAs and Sub-CAs are themselves, as a technical matter, Subscribers of Certificates, as they are issued a Certificate by a superior CA or Sub-CA. References to "Subscribers" in this CPS, however, apply only to End User Subscribers.

Subscribers hold the private key that corresponds to the Public Key listed in that Certificate and as per the Indian IT-Act 2000 End User Certificate Subscribers are under legal obligation to maintain the integrity of their respective private keys (CP § 2.1.3).

The table below shows the type of Subscribers for each Class and type of Certificate:

TABLE 2: TYPES OF SUBSCRIBERS

CERTIFICATE TYPE	CLASS	CERTIFICATE SUBSCRIBER
MTNL CLASS 1 INDIVIDUAL SUBSCRIBER	CLASS 1	ANY INDIVIDUAL.
<CUSTOMER> CLASS 1	CLASS 1	INDIVIDUALS WHO ARE AN EMPLOYEE, BUSINESS PARTNER EMPLOYEE, OR CUSTOMER OF A MTNLTRUSTLINE ENTERPRISE SUBCA CUSTOMER ORGANIZATION.
MTNL CLASS 2 ENTERPRISE SUBSCRIBER	CLASS 2	INDIVIDUALS WHO ARE AN EMPLOYEE, BUSINESS PARTNER EMPLOYEE, OR CUSTOMER OF A MTNLTRUSTLINE ENTERPRISE RA CUSTOMER ORGANIZATION.
<CUSTOMER> CLASS 2	CLASS 2	INDIVIDUALS WHO ARE AN EMPLOYEE, BUSINESS PARTNER EMPLOYEE, OR CUSTOMER OF A MTNLTRUSTLINE ENTERPRISE SUBCA CUSTOMER ORGANIZATION.



CERTIFICATE TYPE	CLASS	CERTIFICATE SUBSCRIBER
MTNL CLASS 2 DEVICES	CLASS 2	DEVICES OWNED/OPERATED/MANAGED BY MTNLTRUSTLINE ENTERPRISE RA CUSTOMER ORGANIZATION.
<CUSTOMER> CLASS 2 DEVICES	CLASS 2	DEVICES OWNED/OPERATED/MANAGED BY MTNLTRUSTLINE ENTERPRISE SUBCA CUSTOMER ORGANIZATION.
MTNL CLASS 3 INDIVIDUAL SUBSCRIBER	CLASS 3	ANY INDIVIDUAL.
MTNL CLASS 3 SERVER	CLASS 3	SERVERS OWNED OR OPERATED BY THE CUSTOMER ORGANIZATION.
<CUSTOMER> CLASS 3	CLASS 3	INDIVIDUALS WHO ARE AN EMPLOYEE, BUSINESS PARTNER EMPLOYEE, OR CUSTOMER OF A MTNLTRUSTLINE ENTERPRISE SUBCA CUSTOMER ORGANIZATION.
MTNL CLASS 3 INTERNAL ADMINISTRATOR	CLASS 3	A MTNLTRUSTLINE PKI ADMINISTRATOR PERFORMING RA FUNCTIONS OR CA ADMINISTRATION FUNCTIONS.
MTNL CLASS 3 EXTERNAL ADMINISTRATOR	CLASS 3	A MTNLTRUSTLINE ENTERPRISE CUSTOMER EMPLOYEE PERFORMING RA FUNCTIONS.

1.3.3.2 RELYING PARTIES

Relying Parties are entities that rely on a Certificate(s) issued by MTNLTRUSTLINE in a manner consistent with the IT-Act, the MTNLTRUSTLINE CP and this CPS. 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.



[MTNLTRUSTLINE PKI Relying Parties](#) can be any Individual or Organization including members of the general public.

1.3.4 APPLICABILITY

The CPS applies to all MTNLTRUSTLINE PKI participants - CAs, RAs, Subscribers, and [Relying Parties](#).

This CPS describes the practices governing the use of each Class of Certificates as described in the CP. Each Class of Certificate is generally appropriate for use with the applications set forth in CPS §§ [1.3.4.1](#) and [1.1.4](#). Nonetheless, 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 CPS §§ [1.3.4.2](#), [1.3.4.3](#), [2.2.1.2](#), and [2.2.2](#), 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 (CP § [1.3.4.1](#)). This listings, 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 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 secure 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 and message integrity.

The encryption application enables a Relying Party to use the Subscriber's Certificate to secure 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 and message integrity.

The encryption application enables a Relying Party to use the Subscriber's Certificate to secure 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 are not meant to be used as CA Certificates. This restriction is confirmed by the absence of a basic constraints extension. The effectiveness of such 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 CPS § 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 of this CPS 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 CPS to feedback@mtnltrustline.com or to the following address:

MTNLTRUSTLINE POLICY AND PROCEDURES COORDINATOR

MAHANAGAR TELEPHONE NIGAM LIMITED

Sanchar Haat, Eastern Court, Janpath, NEW DELHI – 110 050

TEL: +91 11 23718636, FAX: +91 11 23718637

E-MAIL: FEEDBACK@MTNLTRUSTLINE.COM



2 GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 CA OBLIGATIONS

MTNLTRUSTLINE performs the specific obligations described throughout this CPS.

In particular, MTNLTRUSTLINE is responsible for conformance with the IT-Act 2000, other applicable laws of India, and MTNLTRUSTLINE CP. MTNLTRUSTLINE is also responsible for ensuring the same level of compliance even when a part or whole of the CA functionality is undertaken by MTNLTRUSTLINE Enterprise Customer entities.

MTNLTRUSTLINE publishes this Certification Practice Statement (CPS) in accordance with CPS § 8.2 and an electronic copy of the current version of this CPS is available for public viewing at <https://www.mtnltrustline.com/repository/cps>.

MTNLTRUSTLINE maintains a Repository of all Certificates and CRLs in a 'X.500' compliant directory with LDAP access. This directory has a public read-only LDAP access available at the Internet host address [directory.mtnltrustline.com](http://www.mtnltrustline.com). For more information on how to access this directory refer to <http://www.mtnltrustline.com/repository/directory.html>.

MTNLTRUSTLINE regularly updates the 'National Repository of Digital Certificates' (NRDC) about the Issuance, Revocation, or suspension of Digital Certificates.

MTNLTRUSTLINE uses 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 include the provisions mentioned in CPS §§ 2.2, 2.3, 2.4.

MTNLTRUSTLINE also ensures appropriate technical and organizational measures to prevent unauthorized or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data.



MTNLTRUSTLINE does not disclose information provided by its PKI users to any third party unless the disclosure is with the prior approval of the concerned user or is forced by a court order or other legal requirement.

MTNLTRUSTLINE is adequately protected against the liabilities arising from its operations and/or activities; in particular MTNLTRUSTLINE has the capability to bear the risk of liability for damages. This protection is partly achieved through 'Bank Guarantees' and/or 'Insurance Cover' and partly through suitable provisions in the MTNLTRUSTLINE 'Book of Accounts'.

The part of Mahanagar Telephone Nigam Limited (MTNL) organization Concerned with MTNLTRUSTLINE operations management has a documented structure with built-in safeguards to ensure impartiality of operations. Also, MTNLTRUSTLINE senior executive, senior staff and staff in trusted roles go through a background check (CPS § 5.3.2) that provides reasonable assurance about their independence from any commercial, financial and other pressures which might adversely affect the trust in the services of MTNLTRUSTLINE.

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 perform the specific obligations appearing throughout this CPS.

2.1.3 SUBSCRIBER OBLIGATIONS

Certificate Applicants are required to provide complete and accurate information on their Certificate Applications. They are also required to manifest assent to the MTNLTRUSTLINE Subscriber Agreement as a condition of obtaining a Certificate. The current version of the Subscriber Agreement is available at <https://www.mtnltrustline.com/repository/subscriber.html>.

MTNLTRUSTLINE Subscriber Agreement requires Subscribers to perform Subscriber functions in accordance with the specific obligations appearing throughout this CPS.

MTNLTRUSTLINE Subscriber Agreement requires the Subscribers to use their Certificates in accordance with CPS § 1.3.4.



MTNLTRUSTLINE Subscriber Agreement requires Subscribers to protect their private keys in accordance with CPS §§ 6.1, 6.2, 6.4.

MTNLTRUSTLINE Subscriber Agreement requires that, if a Subscriber discovers or has reason to believe that 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, then the Subscriber must promptly:

- . • Notify the entity that approved the Subscriber's Certificate Application, either a MTNLTRUSTLINE PKI CA/Sub-CA or an RA, in accordance with CPS § 4.4.1.1 and request Revocation of the Certificate in accordance with CPS §§ 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.

MTNLTRUSTLINE Subscriber Agreement requires that the Subscribers cease use of their private keys at the end of their key usage periods under CPS § 6.3.2.

MTNLTRUSTLINE Subscriber Agreement states that the Subscribers shall not intentionally monitor, interfere with, or reverse engineer the technical implementation of MTNLTRUSTLINE or otherwise intentionally compromise the security of the MTNLTRUSTLINE PKI.

2.1.4 RELYING PARTY OBLIGATIONS

Relying Party obligations apply to Relying Parties by way of MTNLTRUSTLINE Relying Party Agreement. The current version of the Relying Party Agreement is available at <https://www.mtnltrustline.com/repository/rpa.html>.

MTNLTRUSTLINE Relying Party Agreement requires that before any act of reliance, Relying Parties must 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.

The Relying Party Agreement states that MTNLTRUSTLINE, its Sub-CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate.



The Relying Party Agreement specifically states that the Relying Parties must not use Certificates beyond the limitations in CPS § 1.3.4.2 and for purposes prohibited in CPS § 1.3.4.3.

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

MTNLTRUSTLINE Relying Party Agreement also requires that the Relying Parties must check the status of a Certificate on which they wish to rely, as well as all the Certificates in its Certificate Chain in accordance with CPS §§ 4.4.10, 4.4.12. If any of the Certificates in the Certificate Chain have been revoked, then according to the MTNLTRUSTLINE Relying Party Agreement the Relying Party must not rely on the End User Subscriber Certificate or other revoked Certificate in the Certificate Chain.

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

MTNLTRUSTLINE Relying Party Agreement states that only if all of the checks described above are successful, the Relying Party is entitled to rely on the Certificate, provided that reliance upon the Certificate is reasonable (as detailed in CPS § 1.3.4) 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.

MTNLTRUSTLINE Relying Party Agreement states that the Relying Party shall not intentionally monitor, interfere with, or reverse engineer the technical implementation of MTNLTRUSTLINE or otherwise intentionally compromise the security of the MTNLTRUSTLINE PKI.



2.1.5 REPOSITORY OBLIGATIONS

MTNLTRUSTLINE is responsible for the repository functions of all CAs and Sub-CAs in the MTNLTRUSTLINE PKI. All Certificates and CRLs (or other Certificate status information), whether they are issued by MTNLTRUSTLINE RAs or MTNLTRUSTLINE Enterprise Customers RAs (for MTNLTRUSTLINE Enterprise Sub-CA Customers or MTNLTRUSTLINE Enterprise RA Customers) are published by MTNLTRUSTLINE to the MTNLTRUSTLINE Repository.

2.2 LIABILITY

2.2.1 CA LIABILITY

MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement cover warranties, disclaimers, and limitations of liability required by CP § 2.2.1. The terms applicable to Relying Parties are also included in the Subscriber Agreement, in addition to the Relying Party Agreement, because Subscribers often act as Relying Parties as well.

2.2.1.1 WARRANTIES TO SUBSCRIBERS AND RELYING PARTIES

MTNLTRUSTLINE Subscriber Agreement includes a warranty 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 Relying Party Agreement includes a warranty to Relying Parties who reasonably rely on a Digital Certificate that:

- . • All information in or incorporated by reference in such Certificate 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

- MTNLTRUSTLINE has complied with this CPS when issuing the Certificate.

2.2.1.2 DISCLAIMERS OF WARRANTIES

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement disclaim any warranty of fitness for a particular purpose, outside the context of this CPS.

2.2.1.3 LIMITATIONS OF LIABILITY

To the extent permitted by applicable law, MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement limit the liability to exclude indirect, special, incidental, and consequential damages.

For a specific Digital Certificate MTNLTRUSTLINE's liability is limited to the following liability caps:

TABLE 3: MTNLTRUSTLINE CA LIABILITY CAPS

CLASS OF CERTIFICATE	CLASS 1	CLASS 2	CLASS 3
LIABILITY CAP PER CERTIFICATE	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 include a force majeure clause protecting MTNLTRUSTLINE.



2.2.2 RA LIABILITY

The warranties, disclaimers of warranty, and limitations of liability between an RA and the Sub-CA it is assisting to issue Certificates are set forth and governed by the agreements between them.

MTNLTRUSTLINE on behalf of its MTNLTRUSTLINE Enterprise Sub-CA/RA Customers includes in the MTNLTRUSTLINE Subscriber Agreement and the Relying Party Agreement warranties, disclaimers of warranty, limitations of liability, and force majeure clauses set forth in CPS §§ [2.2.1.1](#), [2.2.1.2](#), [2.2.1.3](#), [2.2.1.4](#).

2.2.3 SUBSCRIBER LIABILITY

2.2.3.1 SUBSCRIBER WARRANTIES

MTNLTRUSTLINE Subscriber Agreement requires the 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 this 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

CPS § 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 states 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 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 CPS § 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 requires 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 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 (as detailed in CPS § 1.3.4) 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 disclaim any fiduciary relationship between MTNLTRUSTLINE on one hand and a Subscriber or Relying Party on the other hand.

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

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



2.3.3 ADMINISTRATIVE PROCESSES

MTNLTRUSTLINE has sufficient financial resources to maintain the integrity of its PKI, and is reasonably able to bear the risk of liability to Subscribers and Relying Parties. MTNLTRUSTLINE's audited books of accounts are set forth in disclosures appearing at <http://www.mtnltrustline.com/corporate/boa.html>.

MTNLTRUSTLINE maintains a reasonable level of risk coverage for errors and omissions, either through errors and omissions insurance or self-insured retention (provision).

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 GOVERNING LAW

The Laws of the India govern the use of this CPS, 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 contain severability, survival, merger, and notice clauses.

A severability clause in an agreement prevents any determination of the invalidity or unenforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that continue in effect despite the termination or expiration of the agreement. A merger clause states that all understandings concerning the subject matter of an agreement are incorporated in the agreement. A notice clause in an agreement sets forth how the parties are to provide notices to each other.

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.

MTNLTRUSTLINE Subscriber Agreement and Relying Party Agreement contain a dispute resolution clause.



2.4.3.1 ROLE OF THE CCA

Under the IT-Act 2000, the Controller of Certifying Authorities (CCA) is authorized to resolve disputes arising out of CA services.

2.5 FEES

2.5.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

MTNLTRUSTLINE and MTNLTRUSTLINE Enterprise Sub-CA/RA Customers are entitled to charge End User Subscribers for the Issuance, Renewal, and Replacement of Digital Certificates.

The fees charged by MTNLTRUSTLINE for the Retail (CPS § 1.1.5) Digital Certificates are published within MTNLTRUSTLINE Repository at <https://www.mtnltrustline.com/repository/fees/retail.html>.

The fees charged by MTNLTRUSTLINE for the Enterprise (CPS § 1.1.5) Digital Certificates are published within MTNLTRUSTLINE Repository at <https://www.mtnltrustline.com/repository/fees/enterprise.html>.

2.5.2 CERTIFICATE ACCESS FEES

MTNLTRUSTLINE does not charge a fee as a condition of making a Certificate available in its Repository or otherwise making Certificates available to Relying Parties.

2.5.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

MTNLTRUSTLINE does 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.

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



2.5.4 FEES FOR OTHER SERVICES SUCH AS POLICY INFORMATION

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

2.5.5 REFUND POLICY

MTNLTRUSTLINE does not refund any fees paid towards the issuance of a Digital Certificate after the issuance of the Certificate.

MTNLTRUSTLINE may refuse to issue a Certificate to any person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Upon a refusal to issue a Certificate, MTNLTRUSTLINE will refund to the Certificate Applicant any paid Certificate fees, unless the Certificate Applicant submitted fraudulent or falsified information to the RA or failed to submit documentary evidence in support of the Certificate Application within one month of the application. In such a case the fee will not be refunded.

This refund policy is published within the MTNLTRUSTLINE Repository at <https://www.mtnltrustline.com/repository/refund.html>.

2.6 PUBLICATION AND REPOSITORIES

2.6.1 PUBLICATION OF CA INFORMATION

MTNLTRUSTLINE Repository published within MTNLTRUSTLINE's web-site at <https://www.mtnltrustline.com/repository/> includes the following:

MTNLTRUSTLINE CPS: <https://www.mtnltrustline.com/repository/cps>

MTNLTRUSTLINE CP: <https://www.mtnltrustline.com/repository/cp>

Subscriber Agreement: <https://www.mtnltrustline.com/repository/subscriber.html>

Relying Party Agreement: <https://www.mtnltrustline.com/repository/rpa.html>

MTNLTRUSTLINE CAs: <https://www.mtnltrustline.com/repository/ca-list.html>

MTNLTRUSTLINE CRL List: <https://www.mtnltrustline.com/repository/crl.html>

MTNLTRUSTLINE RA List: <https://www.mtnltrustline.com/repository/ra-list.html>

Refund Policy: <https://www.mtnltrustline.com/repository/refund.html>



Fees: <https://www.mtnltrustline.com/repository/fees/>

FAQ: <https://www.mtnltrustline.com/repository/faq/>

MTNLTRUSTLINE End Entity Certificates, CA and Sub-CA Certificates, and CRLs are published in the MTNLTRUSTLINE X.500 directory (directory.mtnltrustline.com). This directory can be assessed using an LDAP client (LDAP protocol) or a web browser (<https://directory.mtnltrustline.com> and <http://directory.mtnltrustline.com>). More information about using this directory is available at <https://www.mtnltrustline.com/repository/directory.html>.

All MTNLTRUSTLINE End Entity Certificates contain a pointer to this CPS and/or the Relying Party Agreement in accordance with CPS §§ [3.1.1](#), [7.1.6](#), [7.1.8](#).

2.6.2 FREQUENCY OF PUBLICATION

Updates to this CPS are published in accordance with CPS § [8](#).

Updates to the Subscriber Agreement, Relying Party Agreement, and other information are published as necessary.

Certificates are published upon issuance. CRLs are published in accordance with CPS § [4.4.9](#).

2.6.3 ACCESS CONTROLS

Information published in the MTNLTRUSTLINE Repository is publicly accessible information. MTNLTRUSTLINE provides unrestricted read-only access to all information in its Repository. MTNLTRUSTLINE requires persons to agree to the Relying Party Agreement as a condition to accessing Certificates or CRLs.

MTNLTRUSTLINE has implemented logical and physical security 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. See CPS § 2.1.5.

2.7 COMPLIANCE AUDIT

MTNLTRUSTLINE performs regular audits as required for compliance with the IT-Act 2000, and its associated rules and regulations. These audits are performed by an auditor appointed by the Controller of Certifying Authorities (CCA) from a set of empanelled auditors.

In addition to third party audits MTNLTRUSTLINE performs half yearly self-audits.

2.7.1 FREQUENCY OF COMPLIANCE AUDIT

Statutory compliance audits are conducted annually.

2.7.2 IDENTITY/ QUALIFICATIONS OF AUDITOR

Only a third party certified public auditing firm, empanelled by the Controller of Certifying Authorities (CCA), performs the compliance audits of MTNLTRUSTLINE. Such firms are required to possess demonstrated expertise in computer security and in the performance of IT security and PKI compliance audits.

2.7.2.1 SELF-AUDITS

Half yearly internal audit of the security policy, physical security, planning of operation and the repository shall be conducted.

2.7.3 AUDITOR'S RELATIONSHIP TO AUDITED PARTY

Third-party audit firms performing compliance audits of MTNLTRUSTLINE are independent of MTNLTRUSTLINE and MTNL.

With respect to self-audits, see CP § 2.7.2.1.



2.7.4 TOPICS COVERED BY AUDIT

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

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

The quarterly audits focus on the Repository.

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

The annual compliance audits 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

Significant exceptions or deficiencies identified during an audit will result in a determination of actions to be taken. This determination is made by MTNLTRUSTLINE management with input from the auditor. MTNLTRUSTLINE management is responsible for developing and implementing a corrective action plan. If MTNLTRUSTLINE determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the MTNLTRUSTLINE PKI, a corrective action plan will be developed on a best effort basis in as short a time frame as possible and implemented within a reasonable period of time. For less serious exceptions or deficiencies, MTNLTRUSTLINE Management will evaluate the significance of such issues and determine the appropriate course of action.

In any case, MTNLTRUSTLINE Management will endeavor to rectify all deficiencies found during a statutory compliance audit.

2.7.6 COMMUNICATIONS OF RESULTS

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

2.8 CONFIDENTIALITY POLICY

In compliance with CP § 2.8 MTNLTRUSTLINE has implemented a privacy policy (<https://www.mtnltrustline.com/privacy.html>). This privacy policy requires MTNLTRUSTLINE and its RAs not to disclose or sell the names of Certificate Applicants or other identifying information about them, subject to CPS § 2.8.2 and the right of a terminating CA to transfer such information to a successor CA under CPS § 4.9.

2.8.1 TYPES OF INFORMATION TO BE KEPT CONFIDENTIAL

The following information, subject to CPS § 2.8.2, are kept confidential ("Confidential Information"):

- . • CA application records, whether approved or disapproved,
- . • Certificate Application records (subject to CPS § 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.

2.8.3 DISCLOSURE OF CERTIFICATE REVOCATION/SUSPENSION INFORMATION

Certificate Revocation/Suspension information, including reasons for Revocation/Suspension is Public Information as per CPS § [2.8.2](#)

2.8.4 RELEASE TO LAW ENFORCEMENT OFFICIALS

MTNLTRUSTLINE PKI Participants 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 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

MTNLTRUSTLINE privacy policy has provisions relating to the disclosure of confidential information to the person disclosing it to MTNLTRUSTLINE.

MTNLTRUSTLINE shall disclose the information provided by the Subscriber to whom MTNLTRUSTLINE is obliged to keep such information confidential upon the request from the same Subscriber to do so.

2.8.7 OTHER INFORMATION RELEASE CIRCUMSTANCES

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

2.9.1 RIGHTS IN CERTIFICATES

MTNLTRUSTLINE PKI Participants acknowledge that MTNLTRUSTLINE retains all Intellectual Property Rights in and to the Certificates and Revocation information that it issues. MTNLTRUSTLINE grants 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 PKI Participants acknowledge that MTNLTRUSTLINE retains all Intellectual Property Rights in and to this CPS and the MTNLTRUSTLINE CP.



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 and End User Subscribers are the property of the 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

MTNLTRUSTLINE End User Subscriber Digital Certificates contain an X.501 Distinguished Name (DN) in the subject name field.

MTNLTRUSTLINE Primary CA and Sub-CA DN format is as shown in table below:

TABLE 4: MTNLTRUSTLINE CA AND SUB-CA DN FORMAT

ATTRIBUTE	VALUE
COUNTRY (c)	INDIA (IN)
ORGANIZATION (O)	"MAHANAGAR TELEPHONE NIGAM LIMITED"
ORGANIZATIONAL UNIT (OU)	"MTNLTRUSTLINE"
STATE OR PROVINCE (S)	NOT USED
LOCALITY (L)	NOT USED
COMMON NAME (CN)	THIS ATTRIBUTE INDICATES THE CA / SUB-CA NAME

'MTNLTRUSTLINE Enterprise Sub-CA Customer' Sub-CA DN format is as shown in table below.

TABLE 5: 'MTNLTRUSTLINE ENTERPRISE SUB-CA CUSTOMER' SUB-CA DN FORMAT

ATTRIBUTE	VALUE
COUNTRY (c)	INDIA (IN) OR NOT USED
ORGANIZATION (O)	LEGAL NAME OF THE CUSTOMER ORGANIZATION
ORGANIZATIONAL UNIT (OU)	"MTNLTRUSTLINE"
STATE OR PROVINCE (S)	STATE OR PROVINCE OF THE ORGANIZATION OR NOT USED
LOCALITY (L)	LOCALITY OF THE ORGANIZATION OR NOT USED
COMMON NAME (CN)	THIS ATTRIBUTE INDICATES THE SUB-CA NAME



MTNLTRUSTLINE End User Subscriber DN format is as shown in table below:

TABLE 6: MTNLTRUSTLINE END USER SUBSCRIBER DN FORMAT

ATTRIBUTE	VALUE
COUNTRY (c)	INDIA (IN) OR NOT USED.
ORGANIZATION (O)	<p>"MTNLTRUSTLINE INDIVIDUAL SUBSCRIBER" FOR RETAIL INDIVIDUAL CERTIFICATES;</p> <p>"MTNLTRUSTLINE ENTERPRISE SUBSCRIBER" FOR MTNLTRUSTLINE ENTERPRISE RA CUSTOMER CERTIFICATES;</p> <p>"MTNLTRUSTLINE ADMINISTRATOR" FOR ADMINISTRATOR CERTIFICATES;</p> <p>SUBSCRIBER ORGANIZATIONAL NAME FOR RETAIL SERVER CERTIFICATES;</p> <p>THE LEGAL NAME OF THE CUSTOMER ORGANIZATION FOR MTNLTRUSTLINE ENTERPRISE SUB-CA CUSTOMER CERTIFICATES;</p> <p>OR NOT USED.</p>
ORGANIZATIONAL UNIT (OU)	"MTNLTRUSTLINE"
STATE OR PROVINCE (S)	STATE OR PROVINCE OF THE SUBSCRIBER OR NOT USED.
LOCALITY (L)	LOCALITY OF THE SUBSCRIBER OR NOT USED.
COMMON NAME (CN)	<p>NAME FOR INDIVIDUAL CERTIFICATES, EXCEPT FOR 'CLASS 1' CERTIFICATES WHICH HAVE THIS ATTRIBUTE VALUE SET TO "MTNLTRUSTLINE E-MAIL USER";</p> <p>DOMAIN NAME FOR SERVER CERTIFICATES;</p> <p>SUBSCRIBER ORGANIZATIONAL NAME FOR CODE/OBJECT SIGNING CERTIFICATES;</p>
E-MAIL ADDRESS (E)	E-MAIL ADDRESS (MUST FOR CLASS 1) OR NOT USED.
SERIAL NUMBER (SN)	MTNLTRUSTLINE ASSIGNED UNIQUE REFERENCE ID OF THE CERTIFICATE.
ANY OTHER NAME ATTRIBUTE (IF REQUIRED)	AUTHENTICATED VALUE OF THE NAME ATTRIBUTE REQUIRED FOR IDENTIFYING THE ENTITY OR NOT USED.



3.1.2 MEANING OF NAMES

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

For Certificates issued to Individuals (except Class 1 Certificates) the common name (CN) attribute represents the individual's generally accepted personal name.

For Certificates issued to Devices this common name is either 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, when present in the subject distinguished name, represents the legal name of the Subscriber organization. This is meant to be used to only determine the identity of the Subscriber and does not imply any power-of-attorney or other rights.

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 are 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 are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others.

However, MTNLTRUSTLINE does not determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application nor arbitrates, mediates, or otherwise resolves any dispute concerning the ownership of any domain name, trade name, trademark, or service mark.

MTNLTRUSTLINE is entitled, without liability to any Certificate Applicant, to reject or revoke any Certificate Application because of such dispute.



3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

See CPS § 3.1.5.

3.1.7 METHOD TO PROVE POSSESSION OF PRIVATE KEY

MTNLTRUSTLINE verifies Certificate Subscriber's possession of the private key corresponding to the public key to be published in the Digital Certificate through the use of a digitally signed certificate request pursuant to 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 RAs 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:

- » Verify 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 consists of authenticating the existence of the organization pursuant to CPS § 3.1.8.1. MTNLTRUSTLINE RAs 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 use the device names, confirm that the organization's use of such names does not conflict with generally accepted standards.

In addition, MTNLTRUSTLINE RAs 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 consists of authenticating the existence of the organization pursuant to CPS § 3.1.8.1. MTNLTRUSTLINE RAs during such authentication process, verify by querying the appropriate Domain Registry, 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 RAs 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 enter into an agreement with MTNLTRUSTLINE.

MTNLTRUSTLINE authenticates the identity of the prospective Sub-CA or RA Customer before final approval of its status as Sub-CA or RA. This is also 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 CPS § 3.1.8.1 are also performed, except that instead of a Certificate Application, the validation is of an application to become a Sub-CA or RA. Also, MTNLTRUSTLINE confirms that the person identified as an Administrator is authorized to act in the capacity.



3.1.9 AUTHENTICATION OF INDIVIDUAL IDENTITY

MTNLTRUSTLINE RAs confirm the identity of an individual, before issuing a Digital Certificate, in accordance with the procedures of authentication set forth in this CPS § 3.1.9 for each Class of Certificate.

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

- » Verify that the Certificate Applicant is the person identified in the Certificate Application (except for Certificate Applicants for Class 1 Certificates - CPS § 3.1.9.1),
- » Establish that the Certificate Applicant rightfully holds the private key corresponding to the Public Key to be listed in the Certificate in accordance with CPS § 3.1.7, and
- » Confirm 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 consists 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 does not authenticate the identity of the Class 1 Certificate Applicant. As a result, the Certificate Applicant's personal name does not appear in the subject name of the Certificate. Instead the Certificates Subscriber Distinguished Name is populated with "mtnlTrustLine E-Mail User" pursuant to CPS § 3.1.1.



3.1.9.2 CLASS 2 CERTIFICATES

Authentication of Individuals or Devices for Class 2 Certificates consists of matching identifying information in the Certificate Application with 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 RAs approve and issue the Certificate.

MTNLTRUSTLINE provides its RAs with an optional software module for automatic approval of users or Devices directly from pre-existing databases, rather than requiring manual authentication for each Certificate Application. RAs using software to automate the processing of Certificate requests authenticate the identity of potential Certificate Applications before placing their information in the Validating Database. When a Certificate Applicant submits a Certificate Application, then, the Software Module compares information in the Certificate Application with that in the database and, if the information matches, automatically approves the Certificate Application for immediate issuance.

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 at <https://www.mtnltrustline.com/repository/ra-list.html>. The agent, notary or other official checks 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 MTNLTRUSTLINE Enterprise RA Customer or MTNLTRUSTLINE Enterprise Sub-CA Customer RAs for Class 3 Administrator Certificates (RA Certificates) consists of authenticating the existence of the Administrator's employer and confirming the employment and authorization of the person named as Administrator. MTNLTRUSTLINE authenticates Certificate Applications first by authenticating the identity of the entity employing or retaining the Administrator pursuant to CPS § 3.1.8.1. Such entity is either a MTNLTRUSTLINE Enterprise RA Customer or a MTNLTRUSTLINE Enterprise Sub-CA Customer. MTNLTRUSTLINE during such authentication process also confirms 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 authentication procedures for the Renewal of an End User Certificate are the same as for original Certificate Application pursuant to CPS §§ [3.1.8](#), [3.1.9](#).

3.2.2 RENEWAL OF SUB-CA CERTIFICATES

MTNLTRUSTLINE authentication procedures for renewal of Sub-CA Certificates are the same as for original enrollment pursuant to CPS § [3.1.8.4](#).

3.3 REKEY AFTER REVOCATION -NO KEY COMPROMISE

MTNLTRUSTLINE does 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. Renewal procedures are the same as for original Certificate Application pursuant to CPS §§ [3.1.8](#), [3.1.9](#).



3.4 REVOCATION REQUESTS

Prior to Revocation of any Certificate, MTNLTRUSTLINE verifies that the Revocation has in fact been requested by the Certificate's Subscriber or the RA that approved the Certificate Application. MTNLTRUSTLINE acceptable procedures for authenticating Subscriber revocation requests include:

- . • Having the Subscriber submit the Subscriber's challenge phrase², if applicable, and revoking the Certificate 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
- . • Online request from Subscriber. The Subscriber submits an online revocation request, or the Subscriber sends a revocation request message that is not digitally signed with reference to the Certificate to be revoked. In these cases, MTNLTRUSTLINE confirms the revocation request by sending an e-mail to the certificate subscriber (to the e-mail address listed in the certificate to be revoked) and requests the subscriber to respond confirming the revocation. MTNLTRUSTLINE revokes the Certificate only after receiving the confirmation from the Subscriber.

MTNLTRUSTLINE RAs are entitled to request the revocation of End User Subscriber Certificates managed by them. The RAs are authenticated for such requests via access control based on their RA Certificates.

² As part of the certificate application process, subscribers optionally choose and submit a challenge phrase with their enrollment information.



4 OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 ENROLLMENT FOR END USER SUBSCRIBER CERTIFICATES

For all MTNLTRUSTLINE Certificates End User Subscribers 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 CPS § 6.1 and ensure reasonable precautions to protect the private key from compromise in accordance with CPS §§ 6.1, 6.2, 6.4.
- . • The Certificate Applicant delivering the Public Key to MTNLTRUSTLINE in accordance with CPS § 6.1.3,
- . • Demonstrating to MTNLTRUSTLINE pursuant to CPS § 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 are submitted either to a MTNLTRUSTLINE RA (<https://www.mtnltrustline.com/repository/ra-list.html>) or Web-RA (<https://www.mtnltrustline.com>).

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. Sub-CA and RA applicants provide their credentials as required by CPS § 3.1.8.4 to demonstrate their identity.



All Sub-CAs certificate requests are created and approved by authorized mtntlTrustLine personnel through a controlled process that requires the participation of multiple trusted individuals.

For all RAs, as subscribers to the relevant 'administrator Sub-CA', the requirement specified in CPS § 4.1.1 apply

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 (CPS § 4.1.1) validates or refutes the information in the Certificate Application pursuant to CPS §§ 3.1.8, 3.1.9. Upon successful performance of all required authentication procedures pursuant to CPS § 3.1, the RA receiving the Certificate Application approves the Certificate Application. If authentication is unsuccessful, the RA receiving the Certificate Application rejects the Certificate Application.

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

The procedures of this section are also 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 authenticates the identity of the entities wishing to become Sub-CA's or RA's as per CPS § 3.1.8.4 before entering into a contract with the Sub-CA or RA applicant under CPS § 4.1.2. The execution of such a contract indicates 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. If approved, MTNLTRUSTLINE issues the Certificates needed to perform the Sub-CA or RA functions in accordance with CPS § 6.1



4.3 CERTIFICATE ACCEPTANCE

MTNLTRUSTLINE notifies Subscribers about the decision to issue the Subscriber's Digital Certificates, and provides the Subscribers with instructions to download/install the Certificates.

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 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 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 not satisfied,
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 CPS § 3.4.

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

4.4.1.2 CIRCUMSTANCES FOR REVOKING SUB-CA OR RA CERTIFICATES

MTNLTRUSTLINE revokes a Sub-CA or RA Certificate 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 CPS and MTNLTRUSTLINE CP,
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 not satisfied, or
6. The Sub-CA or RA requests Revocation of the Certificate in accordance with CPS § 3.4.



4.4.2 WHO CAN REQUEST REVOCATION

4.4.2.1 WHO CAN REQUEST REVOCATION OF AN END USER SUBSCRIBER CERTIFICATE

The parties permitted to request Revocation of a Certificate are 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.

MTNLTRUSTLINE Enterprise Customers (Sub-CAs and RAs) are entitled, through their duly authorized representatives, to request the Revocation of their own Certificates.

MTNLTRUSTLINE is also entitled to request or initiate the Revocation of MTNLTRUSTLINE Enterprise Customer Sub-CA and RA Certificates.

4.4.3 PROCEDURE FOR REVOCATION REQUEST

4.4.3.1 PROCEDURE FOR REVOCATION REQUEST OF AN END USER SUBSCRIBER CERTIFICATE

An End User Subscriber or duly authorized representative, as applicable, requesting Revocation is required to communicate the request to the RA that approved the Subscriber's Certificate Application as described in CPS § 3.4. Upon receiving a valid Revocation request the RA will promptly revoke the Certificate and notify the Subscriber about the Certificate Revocation.

A MTNLTRUSTLINE RA revoking an End User Subscriber Certificate initiates Revocation pursuant to CPS § 3.4.



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

A Sub-CA or RA requesting Revocation is required to communicate the request to MTNLTRUSTLINE pursuant to CPS § 3.4. Upon receiving a valid Revocation request MTNLTRUSTLINE will promptly revoke that Certificate and notify the requester about the successful Revocation. In case of the Revocation of a Sub-CA, MTNLTRUSTLINE will also notify the concerned RAs about the Sub-CA Revocation.

MTNLTRUSTLINE revoking a Sub-CA or RA Certificate initiates Revocation pursuant to CPS § 3.4.

4.4.4 REVOCATION REQUEST GRACE PERIOD

Revocation requests must be submitted as promptly as possible within a reasonable time and in any case within 24 hours of the subscriber coming to know of a compromise requiring revocation.

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 updates and publishes 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 updates and publishes 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.

Expired Certificates are removed from later-issued CRLs starting thirty (30) days after the Certificate's expiration.

4.4.10 CERTIFICATE REVOCATION LIST CHECKING REQUIREMENTS

Relying Parties must 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 provides 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 (CPS § 2.6.1) which is available online and can be accessed using the LDAP, LDAPS, HTTP, and 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

In addition to the procedures described in CPS §§ 4.4.9 -4.4.14, MTNLTRUSTLINE uses reasonable efforts to notify potential Relying Parties if MTNLTRUSTLINE discovers, or has reason to believe, that there has been a compromise of the private key of a CA or Sub-CA within the MTNLTRUSTLINE PKI Hierarchy.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 TYPES OF EVENTS RECORDED

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

4.5.1.1 EVENTS RECORDED BY MTNLTRUSTLINE CA

MTNLTRUSTLINE records in audit log files significant events in the MTNLTRUSTLINE PKI, including:

1. System start-up and shutdown,
2. CA application start-up and shutdown,
1. 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 also collects and consolidates, both electronically as well as manually, security information not generated by the CA system, including:
 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.
 20. All agreements and correspondence relating to MTNLTRUSTLINE CA services.

4.5.1.2 EVENTS RECORDED BY MTNLTRUSTLINE RAS

MTNLTRUSTLINE PKI RAs record in audit log files events relating to the security of their systems, including:

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 routinely process the audit logs on a fortnightly basis.

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

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



4.5.3 PERIOD FOR WHICH AUDIT LOGS ARE KEPT

Audit logs are retained online for at least three (3) months after processing and thereafter archived in accordance with CPS § 4.6.2.

4.5.4 PROTECTION OF AUDIT LOG

Only authorized MTNLTRUSTLINE personnel have access to view and process audit log files. Electronic and manual audit log files are protected from unauthorized viewing, modification, deletion, or other tampering through the use of physical and logical access controls.

4.5.5 AUDIT LOG BACKUP PROCEDURES

Incremental backups of audit logs on physical removable media are created daily and full backups weekly. The backup media is stored in a safe storage. In addition, audit logs and audit summaries are backed up or copied if in manual form.

4.5.6 AUDIT LOG ACCUMULATION SYSTEM (INTERNAL OR EXTERNAL)

The audit log accumulation system is internal to MTNLTRUSTLINE.

4.5.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

4.5.8 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 retains 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 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 CPS § 2.7.

Records are kept in the form of either computer-based messages or paper-based documents. It is ensured that the indexing, storage, preservation, and reproduction of records 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 are archived for at least seven years after expiration.

Audit information detailed in CPS § 4.5.1, is archived pursuant to CPS § 4.5.3 and is also retained for a period of seven years.



4.6.3 PROTECTION OF ARCHIVE

MTNLTRUSTLINE protects its archived records compiled under CPS § 4.6.1 so that only authorized persons can access the archived data.

MTNLTRUSTLINE protects 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 are maintained to ensure that the archive data can be accessed for the time period set forth in CPS § 4.6.2.

4.6.4 ARCHIVE BACKUP PROCEDURES

MTNLTRUSTLINE creates back up copies of archives compiled under CPS § 4.6.1 as and when the archives are created.

Backup copies of the archive and copies of paper-based records under CPS § 4.6.1 are maintained in an off-site disaster recovery facility in accordance with CPS § 4.8.

4.6.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Certificates, CRLs, and other revocation database entries 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 is internal to MTNLTRUSTLINE.

4.6.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Only MTNLTRUSTLINE trusted personnel are permitted to access the archived data. Additionally, the archive information may be made available to the CCA upon request.



4.7 KEY CHANGEOVER

Before the usage period of the MTNLTRUSTLINE CA private key expires (CPS § 6.3.2), key changeover takes place. The old "CA" along with its private key is deactivated, and a new "CA" with a different private key and distinguished name put in use. The new MTNLTRUSTLINE CA Certificate issued by the RCAI is made available through the Repository (CPS § 6.1.4).

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

The distinguished name of the new CA or Sub-CA differentiates 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 remains the same.

4.8 COMPROMISE AND DISASTER RECOVERY

MTNLTRUSTLINE maintains off-site backups of the application logs, Certificate Application data, audit data (per CPS § 4.5.1), and records for all Certificates and CRLs issued. Backup of CA and Sub-CA private keys are generated and maintained in accordance with CPS § 6.2.4. These backups are 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, is promptly made by the affected CA or RA personnel in accordance with MTNLTRUSTLINE incident and compromise reporting and handling procedures. Such procedures 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 Certificate Revocation is reported in accordance with CPS § 4.4.9 in the MTNLTRUSTLINE Repository,
- . • Reasonable efforts are be used to provide additional notice of the Revocation to MTNLTRUSTLINE PKI participants, and
- . • MTNLTRUSTLINE performs a key changeover in accordance with CPS § 4.7, except following Revocation of a CA or Sub-CA Certificate in connection with the termination of a CA or Sub-CA under CPS § 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. CCA India would be notified incase MTNL primary CA key is compromised.

4.8.4 SECURE FACILITY AFTER A NATURAL OR OTHER TYPE OF DISASTER

MTNLTRUSTLINE has installed and tested redundant and fault tolerant equipment at its primary site in New Delhi to support CA/RA functions following all but a major disaster that would render the entire facility inoperable.

MTNLTRUSTLINE maintains a disaster recovery site (DR site) in Mumbai 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 has 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 site has the same equipment, security, and physical security protections as the primary site.

MTNLTRUSTLINE disaster recovery site is also used for testing patches and new releases before they are applied to the main site. The synchronization of the DR site with the main site is disabled during such testing, if required, and is re-enabled after such testing is over. MTNLTRUSTLINE ensures that the disaster recovery database is synchronized with the production database within a time limit of twelve hours.

4.9 CA TERMINATION

MTNLTRUSTLINE management at its discretion can terminate any Sub-CA. However, the termination of a MTNLTRUSTLINE Enterprise Customer Sub-CA is subject to the contract between the terminating Sub-CA and MTNLTRUSTLINE.

In case of termination of a CA or Sub-CA MTNLTRUSTLINE creates a termination plan that reasonably minimizes disruption to Customers, Subscribers, and Relying Parties. The termination plan covers issues including:

- . • Providing notice to parties affected by the termination, such as Subscribers, Relying Parties, Customers, and the CCA,
- . • In case of non-MTNL 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 CPS § 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) are required to draft, implement, and enforce a security policy compliant with the Schedules II and III of the Information Technology (Certifying Authorities) Rules, 2000.

MTNLTRUSTLINE has implemented the MTNLTRUSTLINE Security Policy, which supports the security requirements of this CPS and the MTNLTRUSTLINE CP.

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

All MTNLTRUSTLINE CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

The Primary Site for MTNLTRUSTLINE CA Operations is in New Delhi and the Disaster Recovery Site is in Mumbai.

MTNLTRUSTLINE Primary and Disaster Recovery Sites have clearly defined security perimeters (i.e. physical barriers) around the CA and RA systems. The physical security perimeter is constructed with materials that deter, prevent, and detect covert or overt penetration. The physical security perimeter permits 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 are 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) are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted to MTNLTRUSTLINE trusted



personnel. The opening and closing of cabinets or containers is logged for audit purposes.

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

5.1.2 PHYSICAL ACCESS

MTNLTRUSTLINE has implemented 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 is logged electronically as well as manually as applicable.

5.1.3 POWER AND AIR CONDITIONING

MTNLTRUSTLINE CA and RA locations are equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities are equipped with primary and backup air conditioning systems to control the temperature.

5.1.4 WATER EXPOSURES

MTNLTRUSTLINE CA and RA locations are reasonably protected against floods and other damaging exposure to water.

5.1.5 FIRE PREVENTION AND PROTECTION

MTNLTRUSTLINE CA and RA locations are constructed and equipped, and procedures implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures also meet all applicable fire safety regulations.



5.1.6 MEDIA STORAGE

MTNLTRUSTLINE protects the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards by storage in 'Media Rated Safes' located within MTNLTRUSTLINE Primary Site and MTNLTRUSTLINE Disaster Recovery Site.

5.1.7 WASTE DISPOSAL

Sensitive documents containing confidential information within the meaning of CPS § 2.8.1 are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic Devices are physically destroyed or zeroized in accordance with the manufacturers' guidelines prior to disposal.

5.1.8 OFF-SITE BACKUP

MTNLTRUSTLINE stores all offsite backup media in a physically secure manner at the Mumbai Disaster Recovery Site.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

MTNLTRUSTLINE employees that are designated to manage trustworthiness of the MTNLTRUSTLINE PKI are 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 are required to successfully meet the screening requirements of CPS § 5.3.

MTNLTRUSTLINE also requires contractors, consultants, and auditors who have access to sensitive systems to meet the screening requirements of CPS § 5.3 even though they cannot have any control.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

MTNLTRUSTLINE maintains a policy and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility. Sensitive tasks, such as access to and management of CA cryptographic hardware and associated key material, require multiple Trusted Persons.

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



5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

MTNLTRUSTLINE authenticates 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 is further confirmed through the background checking procedures in CPS §§ [5.3.1](#), [5.3.2](#).

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

- . • Issued access Devices and granted access to the required facilities;
- . • Issued electronic credentials to access and perform specific functions on MTNLTRUSTLINE CA, RA, or other IT systems.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND CLEARANCE

REQUIREMENTS

MTNLTRUSTLINE requires 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 conducts background checks for internal employees through the MTNL Vigilance Cell. For external employees the following is ensured:

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

5.3.3 TRAINING REQUIREMENTS AND TRAINING PROCEDURES

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

MTNLTRUSTLINE also periodically reviews its training programs. Training programs 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 provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

MTNLTRUSTLINE maintains and enforce employment policies for the discipline of personnel following unauthorized actions. Disciplinary actions include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 CONTRACTING PERSONNEL REQUIREMENTS

Independent contractors and consultants are 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 provides 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 ensures 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 is carried out within a FIPS 140-1 level 3 or higher device in a physically secured environment by multiple pre-selected personnel in trusted roles under, at least, dual control. The personnel authorized to carry out this function are limited to those required to do so under the MTNLTRUSTLINE's practices. The activities performed for each CA/Sub-CA key pair generation are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking in accordance with CPS § 4.5.1 and CPS § 4.6.

RA key pair generation is carried out in FIPS 140-1/2 level 2 device or above. Generation of End User Subscriber key pairs is performed by the Subscriber or at a MTNLTRUSTLINE RA office in the presence of the Subscriber.

6.1.2 PRIVATE KEY DELIVERY TO ENTITY

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

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The acceptable mechanism within the MTNLTRUSTLINE PKI for Public Key delivery to Certificate Issuer 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 makes its CA and Sub-CA Public Keys available to the Relying Parties via CA Certificates in a secure fashion.

These CA Certificates are published in the MTNLTRUSTLINE Certificate Repository (<https://www.mtnltrustline.com/repository/ca-list.html>). MTNLTRUSTLINE CA and Sub-CA Certificates are verifiable by users with respect to the RCAI root Certificate.

6.1.5 KEY SIZES

MTNLTRUSTLINE uses 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.³

6.1.7 PARAMETER QUALITY CHECKING

No stipulation.⁴

³ MTNLTRUSTLINE supports the RSA Public Key algorithm for which this requirement is not relevant.

⁴ See footnote above.



6.1.8 HARDWARE OR SOFTWARE KEY GENERATION

MTNLTRUSTLINE generates 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 are generated in hardware (smart cards).

MTNLTRUSTLINE Subscriber Agreement recommends that End User Subscribers generate their key pairs in hardware (Smart Cards or Tokens), although such key pairs may be generated by the Subscriber in hardware or software.

6.1.9 KEY USAGE PURPOSES

MTNLTRUSTLINE sets 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 is configured so as to set and clear bits and the criticality field in accordance with table below.

TABLE 7: KEYUSAGE EXTENSIONS FOR X.509 V3 CERTIFICATES:

		CA'S AND SUB-CAS	CLASS 1	CLASS 2	CLASS 3	ADMINISTRATOR (CLASS 3)
CRITICALITY		FALSE	FALSE	FALSE	FALSE	FALSE
0	DIGITALSIGNATURE	CLEAR	SET	SET	SET	SET
1	NONREPUDIATION	CLEAR	CLEAR	SET	SET	SET
2	KEYENCIPHERMENT	CLEAR	SET	SET	SET	SET
3	DATAENCIPHERMENT	CLEAR	CLEAR	CLEAR	CLEAR	CLEAR
4	KEYAGREEMENT	CLEAR	CLEAR	CLEAR	CLEAR	CLEAR
5	KEYCERTSIGN	SET	CLEAR	CLEAR	CLEAR	CLEAR
6	CRLSIGN	SET	CLEAR	CLEAR	CLEAR	CLEAR
7	ENCIPHERONLY	CLEAR	CLEAR	CLEAR	CLEAR	CLEAR
8	DECIPHERONLY	CLEAR	CLEAR	CLEAR	CLEAR	CLEAR



6.2 PRIVATE KEY PROTECTION

MTNLTRUSTLINE has implemented a combination of physical, logical, and procedural controls to ensure the security of MTNLTRUSTLINE PKI CA and Sub-CA private keys. Logical and procedural controls are described in CPS § 6.2. Physical access controls are described in CPS § 5.1.2.

6.2.1 STANDARDS FOR CRYPTOGRAPHIC MODULES

MTNLTRUSTLINE performs 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.

All MTNLTRUSTLINE RAs (MTNLTRUSTLINE as well as non-MTNLTRUSTLINE) perform all cryptographic operations with their own private keys on hardware cryptographic modules.

End User Subscribers have the option of protecting their private keys in a smart card or other hardware token. MTNLTRUSTLINE recommends that all End User Subscribers use hardware cryptographic modules.

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

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

MTNLTRUSTLINE uses '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' is held by a distinct MTNLTRUSTLINE trusted personnel referred to as the Custodian. A threshold number of secret shares (n) out of the total number of secret shares (m) are required to operate the private key.

MTNLTRUSTLINE also uses secret sharing to protect the activation data needed to activate private keys located at its disaster recovery site.

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

**TABLE 8: 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 NUMBERS OF SECRET SHARES CUSTODIANS	NEEDED	TOTAL
mtnlTrustLine PRIMARY CA	N/A	3	5	3	5
mtnlTrustLine OFFLINE SUB-CA	N/A	3	5	3	5
mtnlTrustLine ONLINE SUB-CA	3	3	5	3	5

6.2.3 PRIVATE KEY ESCROW

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

6.2.4 PRIVATE KEY BACKUP

[MTNLTRUSTLINE](#) creates backup copies of CA/Sub-CA private keys for routine recovery and disaster recovery purposes. Such keys are stored within hardware cryptographic modules meeting the requirements of CPS § 6.2.1. CA/Sub-CA private keys are copied to backup hardware cryptographic modules in accordance with CPS § 6.2.6. Modules containing backup copies of CA/Sub-CA private keys are subject to the requirements of CPS §§ 5.1, 6.2.1.

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

6.2.5 PRIVATE KEY ARCHIVAL

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

6.2.6 PRIVATE KEY ENTRY INTO CRYPTOGRAPHIC MODULE

[MTNLTRUSTLINE](#) generates CA/Sub-CA key pairs on the hardware cryptographic modules in which the keys will be used.

In addition, [MTNLTRUSTLINE](#) makes 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 are transported between modules in encrypted form.



6.2.7 METHOD OF ACTIVATING PRIVATE KEY

All MTNLTRUSTLINE PKI participants 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 are activated by a threshold number of Custodians supplying their activation data (tokens or pass-phrases) in accordance with CPS § 6.2.2.

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

For MTNLTRUSTLINE Online Sub-CAs, the CA private keys are activated for an indefinite period and the token remains online in the production data center until the Sub-CA is taken offline (e.g., for system maintenance). Individual signing activities are initiated by a digitally signed request from an RA.

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 CPS § 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 are deactivated upon removal from the token reader.

When an Online Sub-CA is taken offline MTNLTRUSTLINE personnel 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 remove the token containing such private keys from the reader in order to deactivate it. Once removed from the reader, tokens are 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 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 are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking in accordance with CPS § 4.5.1 and CPS § 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 are archived as part of routine archival procedures (CPS § 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 9: 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	5 YEARS
MTNLTRUSTLINE END USER SUBSCRIBER	2 YEAR



In addition, MTNLTRUSTLINE CAs/Sub-CAs 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 generates activation data for the CAs and Sub-CAs within the MTNLTRUSTLINE PKI in accordance with the secret sharing requirements of CPS § 6.2.2. The creation and distribution of Secret Shares to the Custodians is logged.

MTNLTRUSTLINE RAs are required to select strong passwords to protect their private keys. The passwords must:

- . • Be generated by the user;
- . • Have at least eight characters;
- . • Have at least one alphabetic, one numeric, and one upper-case character; and
- . • Not contain the user's profile name.

MTNLTRUSTLINE strongly recommends that End User Subscribers choose passwords that meet the same requirements. MTNLTRUSTLINE also recommends the use of two factor authentication mechanisms (e.g., token and passwords, biometric and token, or biometric and passwords) for private key activation.

6.4.2 ACTIVATION DATA PROTECTION

MTNLTRUSTLINE utilizes secret sharing in accordance with CPS § 6.2.2 and the Custodians are required to safeguard their Secret Shares and sign an agreement acknowledging their Custodian responsibilities.

MTNLTRUSTLINE RAs are required to generate and store their RA Private Keys in hardware (CPS § 6.2.1).

MTNLTRUSTLINE strongly recommends that End User Subscribers store their private keys in encrypted form and protect their private keys through the use of hardware token and/or strong passwords. The use of two factor authentication mechanisms (e.g., token and passwords, biometric and token, or biometric and passwords) is encouraged.



6.4.3 OTHER ASPECTS OF ACTIVATION DATA

See CPS §§ 6.4.1, 6.4.2.

6.5 COMPUTER SECURITY CONTROLS

MTNLTRUSTLINE performs all CA and RA functions 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 systems maintaining CA and RA software and data files are trustworthy systems secure from unauthorized access, which is demonstrated by compliance with audit criteria applicable under CPS § 2.7.4. In particular, MTNLTRUSTLINE deployed systems 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 implementations by MTNLTRUSTLINE are carried out in accordance with MTNLTRUSTLINE change management standards.

MTNLTRUSTLINE after loading new or updated Software on its CA/RA systems verifies before first use that the software on the system is as provided by the software vendor and is the correct version intended for use.

MTNLTRUSTLINE maintains separate production and development environments.

6.6.2 SECURITY MANAGEMENT CONTROLS

Software for CA and RA functions is subject to checks to verify integrity. MTNLTRUSTLINE requires the software vendors to provide a hash of all software packages or software updates that they provide to MTNLTRUSTLINE. This hash is used to verify the integrity of such software manually. MTNLTRUSTLINE also has mechanisms and/or policies in place to control and monitor the configuration of its CA and RA systems. Upon installation, and at regular intervals, MTNLTRUSTLINE validates the integrity of the CA and RA systems.

6.6.3 LIFE CYCLE SECURITY RATINGS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

MTNLTRUSTLINE performs 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 protects 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 meet the requirements specified in CPS § 6.2.1.



7 CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

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

TABLE 10: BASIC CERTIFICATE	
BASIC FIELD	VALUE OR VALUE CONSTRAINT
VERSION	VERSION 3 (VALUE 2) (CPS § 7.1.1)
SERIAL NUMBER	INTEGER VALUE, UNIQUE FOR EACH CERTIFICATE ISSUED BY THE ISSUER
SIGNATURE ALGORITHM	ALGORITHM IDENTIFIER FOR THE ALGORITHM USED BY THE ISSUER TO SIGN THE CERTIFICATE (CPS § 7.1.3)
ISSUER DN	THE X.500 DISTINGUISHED NAME OF THE ENTITY SIGNING THE CERTIFICATE (CPS § 7.1.4)
VALIDITY⁵	<p>THE CERTIFICATE VALIDITY PERIOD REPRESENTED BY TWO DATES:</p> <p>VALIDITY NOT BEFORE - THE DATE ON WHICH THE CERTIFICATE VALIDITY PERIOD BEGINS, AND</p> <p>VALIDITY NOT AFTER - THE DATE ON WHICH THE CERTIFICATE VALIDITY PERIOD ENDS.</p>

⁵ 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 (CPS § 7.1.4)
SUBJECT PUBLIC KEY	ENCODED IN ACCORDANCE WITH RFC 2459
SIGNATURE	GENERATED AND ENCODED IN ACCORDANCE WITH RFC 2459

7.1.1 VERSION NUMBER(S) SUPPORTED

All MTNLTRUSTLINE PKI Certificates are X.509 version 3 Certificates.

7.1.2 CERTIFICATE EXTENSIONS

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

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 CPS § 6.1.9	
CERTIFICATE POLICIES POLICY IDENTIFIER POLICY QUALIFIERS	AS PER CPS § 7.1.6 AS PER CPS § 7.1.8	FALSE
SUBJECT ALTERNATIVE NAME	AS PER RFC 2459	FALSE
ISSUER ALTERNATIVE NAMES	AS PER RFC 2459	FALSE
BASIC CONSTRAINTS	AS PER CPS § 7.1.2.1	
EXTENDED KEY USAGE FIELD	AS PER CPS § 7.1.2.2	
CRL DISTRIBUTION POINTS	URI OF THE CRL.	FALSE

**7.1.2.1 BASIC CONSTRAINTS**

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

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

X.509 Version 3 Online Sub-CA Certificates issuing End User Subscriber Certificates have a path length constraint field of the basic constraints extension set to a value of "none".

MTNLTRUSTLINE CA and Offline Sub-CA Certificates 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 is set to TRUE for CA and Sub-CA Certificates, but otherwise set to FALSE.

7.1.2.2 EXTENDED KEY USAGE

MTNLTRUSTLINE populates 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 12: 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



	CRITICALITY	SERVER AUTH	CLIENT AUTH	CODE SIGNING	EMAIL PROTECTION	TIME STAMPING
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 sign Certificates using sha-1With RSA Encryption algorithm (OID: = 1.2.840.113549.1.1.5).

The algorithm identifier of the subject Public Key is rsa Encryption (OID: = 1.2.840.113549.1.1.1).

7.1.4 NAME FORMS

MTNLTRUSTLINE PKI Certificates are populated with an issuer and subject distinguished name in accordance with CPS § 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 populates 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 populates all 'X.509 version 3 Certificates' with a CPS pointer policy qualifier having a value pointing to the URL of the MTNLTRUSTLINE CPS (<https://www.mtnltrustline.com/repository/cps>).

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

No stipulation.

7.2 CRL PROFILE

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

7.2.1 VERSION NUMBER(S) SUPPORTED

All MTNLTRUSTLINE PKI CRLs are 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 CPS shall be made by the MTNLTRUSTLINE Policy and Procedures 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 CPS 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 CPS.

8.1.1 ITEMS THAT CAN CHANGE WITHOUT NOTIFICATION

The MTNLTRUSTLINE Policy and Procedures 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.

8.1.2 ITEMS THAT CAN CHANGE WITH NOTIFICATION

8.1.2.1 LIST OF ITEMS

All updates, except those covered in CPS § 8.1.1, to the CPS shall require notification prior to becoming effective.

8.1.2.2 NOTIFICATION MECHANISM

Except as noted under CPS § 8.1.1, MTNLTRUSTLINE Policy and Procedures 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 CPS 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 CPS § 8.1.1, the comment period for any changes to the CPS 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 Committee up to the end of this comment period.

8.1.2.4 MECHANISM TO HANDLE COMMENTS

The MTNLTRUSTLINE Policy and Procedures 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 CPS § 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 CPS § 8.1.2.3.

8.1.3 CHANGES REQUIRING CHANGES IN THE CERTIFICATE POLICY OID

As per CP § 8.1.3, if the MTNLTRUSTLINE Policy and Procedures 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

8.2.1 ITEMS NOT PUBLISHED IN THE CPS

Security documents considered confidential by MTNLTRUSTLINE are not disclosed to the public.



8.2.2 DISTRIBUTION OF THE CPS

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

The CPS is also available for download in Adobe Acrobat (pdf) format. MTNLTRUSTLINE also makes the CPS available upon request sent to feedback@mtnlTrustLine.com

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

TABLE 13: CONTACT FOR OBTAINING PAPER COPY OF THIS CPS

SUBJECT: CPS REQUEST

MTNLTRUSTLINE POLICY AND PROCEDURES COORDINATOR

MAHANAGAR TELEPHONE NIGAM LIMITED

Sanchar Haat, Eastern Court, Janpath, NEW DELHI – 110 050

TEL: +91 11 23718636, FAX: +91 11 23718637

8.3 CPS APPROVAL PROCEDURES

Not applicable.



9 LIST OF TERMS

9.1 LIST OF ACRONYMS

TABLE 14: LIST OF ACRONYMS

ACRONYM	TERM
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
PKI	PUBLIC KEY INFRASTRUCTURE



ACRONYM	TERM
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

TERM	DEFINITION
ACCEPT (A DIGITAL SIGNATURE CERTIFICATE)	TO DEMONSTRATE APPROVAL OF A DIGITAL SIGNATURE CERTIFICATE BY A DIGITAL SIGNATURE CERTIFICATE APPLICANT WHILE KNOWING OR HAVING NOTICE OF ITS INFORMATIONAL CONTENTS.
ACCESS	GAINING ENTRY INTO, INSTRUCTING OR COMMUNICATING WITH THE LOGICAL, ARITHMETICAL, OR MEMORY FUNCTION RESOURCES OF A COMPUTER, COMPUTER SYSTEM OR COMPUTER NETWORK;
ACCESS CONTROL	THE PROCESS OF LIMITING ACCESS TO THE RESOURCES OF A COMPUTER SYSTEM ONLY TO AUTHORIZED USERS, PROGRAMS OR OTHER COMPUTER SYSTEMS.
ACCREDITATION	A FORMAL DECLARATION BY THE CONTROLLER THAT A PARTICULAR INFORMATION SYSTEM, PROFESSIONAL OR OTHER EMPLOYEE OR CONTRACTOR, OR ORGANIZATION IS APPROVED TO PERFORM CERTAIN DUTIES AND TO OPERATE IN A SPECIFIC SECURITY MODE, USING A PRESCRIBED SET OF SAFEGUARDS.
ADDRESSEE	A PERSON WHO IS INTENDED BY THE ORIGINATOR TO RECEIVE THE ELECTRONIC RECORD BUT DOES NOT INCLUDE ANY INTERMEDIARY.
ADMINISTRATOR	A TRUSTED PERSON THAT PERFORMS VALIDATION AND OTHER CA OR RA FUNCTIONS



TERM	DEFINITION
ADMINISTRATOR SUB-CA	A SUBORDINATE CA ISSUING CERTIFICATES SOLELY TO PKI ADMINISTRATORS
AFFILIATED CERTIFICATE	A CERTIFICATE ISSUED TO AN AFFILIATED INDIVIDUAL. (SEE ALSO AFFILIATED INDIVIDUAL)
AFFIRM / AFFIRMATION	TO STATE OR INDICATE BY CONDUCT THAT DATA IS CORRECT OR INFORMATION IS TRUE.
AFFIXING DIGITAL SIGNATURE	WITH ITS GRAMMATICAL VARIATIONS AND COGNATE EXPRESSIONS MEANS ADOPTION OF ANY METHODOLOGY OR PROCEDURE BY A PERSON FOR THE PURPOSE OF AUTHENTICATING AN ELECTRONIC RECORD BY MEANS OF DIGITAL SIGNATURE;
ALIAS	A PSEUDONYM.
APPLICANT	(SEE CA APPLICANT; CERTIFICATE APPLICANT)
APPLICATION SOFTWARE	A SOFTWARE THAT IS SPECIFIC TO THE SOLUTION OF AN APPLICATION PROBLEM. IT IS THE SOFTWARE CODED BY OR FOR AN END USER THAT PERFORMS A SERVICE OR RELATES TO THE USER'S WORK.
APPLICATION SYSTEM	A FAMILY OF PRODUCTS DESIGNED TO OFFER SOLUTIONS FOR COMMERCIAL DATA PROCESSING, OFFICE, AND COMMUNICATIONS ENVIRONMENTS, AS WELL AS TO PROVIDE SIMPLE, CONSISTENT PROGRAMMER AND END USER INTERFACES FOR BUSINESSES OF ALL SIZES.
ARCHIVE	TO STORE RECORDS AND ASSOCIATED JOURNALS FOR A GIVEN PERIOD OF TIME FOR SECURITY, BACKUP, OR AUDITING PURPOSES.
ASSURANCES	STATEMENTS OR CONDUCT INTENDED TO CONVEY A GENERAL INTENTION, SUPPORTED BY A GOOD-FAITH EFFORT, TO PROVIDE AND MAINTAIN A SPECIFIED SERVICE. "ASSURANCES" DOES NOT NECESSARILY IMPLY A GUARANTEE THAT THE SERVICES WILL BE PERFORMED FULLY AND SATISFACTORILY. ASSURANCES ARE DISTINCT FROM INSURANCE, PROMISES, GUARANTEES, AND WARRANTIES, UNLESS OTHERWISE EXPRESSLY INDICATED.
ASYMMETRIC CRYPTO SYSTEM	A SYSTEM OF A SECURE KEY PAIR CONSISTING OF A PRIVATE KEY FOR CREATING A DIGITAL SIGNATURE AND A PUBLIC KEY TO VERIFY THE DIGITAL SIGNATURE.
AUDIT	A PROCEDURE USED TO VALIDATE THAT CONTROLS ARE IN PLACE AND ADEQUATE FOR THEIR PURPOSES. INCLUDES RECORDING AND ANALYZING ACTIVITIES TO DETECT INTRUSIONS OR ABUSES INTO AN INFORMATION SYSTEM. INADEQUACIES FOUND BY AN AUDIT ARE



TERM	DEFINITION
AUDIT TRAIL	<p>REPORTED TO APPROPRIATE MANAGEMENT PERSONNEL.</p> <p>A CHRONOLOGICAL RECORD OF SYSTEM ACTIVITIES PROVIDING DOCUMENTARY EVIDENCE OF PROCESSING THAT ENABLES MANAGEMENT STAFF TO RECONSTRUCT, REVIEW, AND EXAMINE THE SEQUENCE OF STATES AND ACTIVITIES SURROUNDING OR LEADING TO EACH EVENT IN THE PATH OF A TRANSACTION FROM ITS INCEPTION TO OUTPUT OF FINAL RESULTS.</p>
AUTHENTICATED RECORD	<p>A SIGNED DOCUMENT WITH APPROPRIATE ASSURANCES OF AUTHENTICATION OR A MESSAGE WITH A DIGITAL SIGNATURE VERIFIED BY A RELYING PARTY. HOWEVER, FOR SUSPENSION AND REVOCATION NOTIFICATION PURPOSES, THE DIGITAL SIGNATURE CONTAINED IN SUCH NOTIFICATION MESSAGE MUST HAVE BEEN CREATED BY THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY CONTAINED IN THE DIGITAL SIGNATURE CERTIFICATE.</p>
AUTHENTICATION	<p>A PROCESS USED TO CONFIRM THE IDENTITY OF A PERSON OR TO PROVE THE INTEGRITY OF SPECIFIC INFORMATION. MESSAGE AUTHENTICATION INVOLVES DETERMINING ITS SOURCE AND VERIFYING THAT IT HAS NOT BEEN MODIFIED OR REPLACED IN TRANSIT. (SEE ALSO VERIFY (A DIGITAL SIGNATURE))</p>
AUTHORITY REVOCATION LIST (ARL)	<p>A LIST OF REVOKED CERTIFYING AUTHORITY CERTIFICATES. AN ARL IS A CRL FOR CERTIFYING AUTHORITY CROSS-CERTIFICATES.</p>
AUTHORIZATION	<p>THE GRANTING OF RIGHTS, INCLUDING THE ABILITY TO ACCESS SPECIFIC INFORMATION OR RESOURCES.</p>
AVAILABILITY	<p>THE EXTENT TO WHICH INFORMATION OR PROCESSES ARE REASONABLY ACCESSIBLE AND USABLE, UPON DEMAND, BY AN AUTHORIZED ENTITY, ALLOWING AUTHORIZED ACCESS TO RESOURCES AND TIMELY PERFORMANCE OF TIME-CRITICAL OPERATIONS.</p>
BACKUP	<p>THE PROCESS OF COPYING CRITICAL INFORMATION, DATA AND SOFTWARE FOR THE PURPOSE OF RECOVERING ESSENTIAL PROCESSING BACK TO THE TIME THE BACKUP WAS TAKEN.</p>
BINDING	<p>AN AFFIRMATION BY A CERTIFYING AUTHORITY OF THE RELATIONSHIP BETWEEN A NAMED ENTITY AND ITS PUBLIC KEY.</p>
CERTIFICATE	<p>A DIGITAL SIGNATURE CERTIFICATE ISSUED BY CERTIFYING AUTHORITY.</p> <p>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.</p>



TERM	DEFINITION
CERTIFICATE ACCEPTANCE	THE SUBSCRIBER'S ACT OF DEMONSTRATING APPROVAL OF THE CERTIFICATE. 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- (A) TO ONE OR MORE PERSONS; (B) IN A REPOSITORY, OR OTHERWISE DEMONSTRATES HIS APPROVAL OF THE DIGITAL SIGNATURE CERTIFICATE IN ANY MANNER."
CERTIFICATE APPLICANT	AN INDIVIDUAL OR ORGANIZATION THAT REQUESTS THE ISSUANCE OF A CERTIFICATE BY A MTNLTRUSTLINE CA OR SUB-CA.
CERTIFICATE APPLICATION	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.
CERTIFICATE CHAIN	AN ORDERED LIST OF CERTIFICATES CONTAINING AN END USER SUBSCRIBER CERTIFICATE AND CA CERTIFICATES.
CERTIFICATE CLASS	A DIGITAL SIGNATURE CERTIFICATE OF A SPECIFIED LEVEL OF TRUST.
CERTIFICATE EXPIRATION	THE TIME AND DATE SPECIFIED IN THE DIGITAL SIGNATURE CERTIFICATE WHEN THE OPERATIONAL PERIOD ENDS, WITHOUT REGARD TO ANY EARLIER SUSPENSION OR REVOCATION.
CERTIFICATE EXTENSION	AN EXTENSION FIELD TO A DIGITAL SIGNATURE CERTIFICATE WHICH MAY CONVEY ADDITIONAL INFORMATION ABOUT THE PUBLIC KEY BEING CERTIFIED, THE CERTIFIED SUBSCRIBER, THE DIGITAL SIGNATURE CERTIFICATE ISSUER, AND/OR THE CERTIFICATION PROCESS. STANDARD EXTENSIONS ARE DEFINED IN AMENDMENT 1 TO ISO/IEC 9594-8:1995 (X.509). CUSTOM EXTENSIONS CAN ALSO BE DEFINED BY COMMUNITIES OF INTEREST.
CERTIFICATE ISSUANCE	THE ACTIONS PERFORMED BY A CA OR SUB-CA IN CREATING A DIGITAL SIGNATURE CERTIFICATE AND NOTIFYING THE DIGITAL SIGNATURE CERTIFICATE APPLICANT (ANTICIPATED TO BECOME A SUBSCRIBER) LISTED IN THE DIGITAL SIGNATURE CERTIFICATE OF ITS CONTENTS.
CERTIFICATE MANAGEMENT [MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE]	CERTIFICATE MANAGEMENT INCLUDES, BUT IS NOT LIMITED TO, STORAGE, DISTRIBUTION, DISSEMINATION, ACCOUNTING, PUBLICATION, COMPROMISE, RECOVERY, REVOCATION, SUSPENSION AND ADMINISTRATION OF DIGITAL SIGNATURE CERTIFICATES. A CERTIFYING AUTHORITY UNDERTAKES DIGITAL SIGNATURE CERTIFICATE MANAGEMENT FUNCTIONS BY SERVING AS A REGISTRATION AUTHORITY FOR SUBSCRIBER DIGITAL SIGNATURE



TERM	DEFINITION
	CERTIFICATES. A CERTIFYING AUTHORITY DESIGNATES ISSUED AND ACCEPTED DIGITAL SIGNATURE CERTIFICATES AS VALID BY PUBLICATION.
CERTIFICATE POLICY (CP)	A SPECIALIZED FORM OF ADMINISTRATIVE POLICY TUNED TO ELECTRONIC TRANSACTIONS PERFORMED DURING DIGITAL SIGNATURE CERTIFICATE MANAGEMENT. A CERTIFICATE POLICY ADDRESSES ALL ASPECTS ASSOCIATED WITH THE GENERATION, PRODUCTION, DISTRIBUTION, ACCOUNTING, COMPROMISE RECOVERY AND ADMINISTRATION OF DIGITAL CERTIFICATES. INDIRECTLY, A CERTIFICATE POLICY CAN ALSO GOVERN THE TRANSACTIONS CONDUCTED USING A COMMUNICATIONS SYSTEM PROTECTED BY A CERTIFICATE-BASED SECURITY SYSTEM. BY CONTROLLING CRITICAL CERTIFICATE EXTENSIONS, SUCH POLICIES AND ASSOCIATED ENFORCEMENT TECHNOLOGY CAN SUPPORT PROVISION OF THE SECURITY SERVICES REQUIRED BY PARTICULAR APPLICATIONS.
CERTIFICATE RENEWAL	RENEWAL OF A CERTIFICATE WITHIN ITS VALIDITY PERIOD GENERALLY TO EXTEND THE VALIDITY.
CERTIFICATE REPLACEMENT	REPLACEMENT OF A CERTIFICATE WITHIN ITS VALIDITY PERIOD WITHOUT EXTENDING THE CERTIFICATE VALIDITY PERIOD.
CERTIFICATE REVOCATION	THE ACT OF INVALIDATING A CERTIFICATE AS A TRUSTED SECURITY CREDENTIAL PRIOR TO THE NATURAL EXPIRATION OF ITS VALIDITY PERIOD. (ALSO SEE REVOKE A CERTIFICATE)
CERTIFICATE REVOCATION LIST (CRL)	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.
CERTIFICATE SERIAL NUMBER	A VALUE THAT UNAMBIGUOUSLY IDENTIFIES A DIGITAL SIGNATURE CERTIFICATE GENERATED BY A CERTIFYING AUTHORITY.
CERTIFICATE SIGNING REQUEST (CSR)	A MACHINE-READABLE FORM OF A DIGITAL SIGNATURE CERTIFICATE APPLICATION.
CERTIFICATE SUBJECT	THE ENTITY IDENTIFIED AS THE OWNER OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY LISTED IN THE CERTIFICATE.
CERTIFICATE SUBSCRIBER	SEE CERTIFICATE SUBJECT.
CERTIFICATE SUSPENSION	(SEE SUSPEND A CERTIFICATE)



TERM	DEFINITION
CERTIFICATION / CERTIFY	THE PROCESS OF ISSUING A DIGITAL SIGNATURE CERTIFICATE BY A CERTIFYING AUTHORITY.
CERTIFICATION PRACTICE STATEMENT (CPS)	A STATEMENT ISSUED BY A CERTIFYING AUTHORITY TO SPECIFY THE PRACTICES THAT THE CERTIFYING AUTHORITY EMPLOYS IN ISSUING DIGITAL SIGNATURE CERTIFICATES.
CERTIFIER	(SEE ISSUING AUTHORITY)
CERTIFYING AUTHORITY (CA)	A PERSON WHO HAS BEEN GRANTED A LICENCE TO ISSUE A DIGITAL SIGNATURE CERTIFICATE UNDER SECTION 24 OF INFORMATION TECHNOLOGY ACT, 2000.
CERTIFYING AUTHORITY SOFTWARE	THE CRYPTOGRAPHIC SOFTWARE REQUIRED TO MANAGE THE KEYS OF END ENTITIES.
CERTIFYING AUTHORITY SYSTEM	ALL THE HARDWARE AND SOFTWARE SYSTEM (E.G. COMPUTER, PKI SERVERS, NETWORK DEVICES ETC.) USED BY THE CERTIFYING AUTHORITY FOR GENERATION, PRODUCTION, ISSUE AND MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE.
CHALLENGE PHRASE	A SET OF NUMBERS AND/OR LETTERS THAT ARE CHOSEN BY A DIGITAL SIGNATURE CERTIFICATE APPLICANT, COMMUNICATED TO THE CERTIFYING AUTHORITY WITH A DIGITAL SIGNATURE CERTIFICATE APPLICATION, AND USED BY THE CERTIFYING AUTHORITY TO AUTHENTICATE THE SUBSCRIBER FOR VARIOUS PURPOSES AS REQUIRED BY THE CERTIFICATION PRACTICE STATEMENT. A CHALLENGE PHRASE IS ALSO USED BY A SECRET SHARE HOLDER TO AUTHENTICATE HIMSELF, HERSELF, OR ITSELF TO A SECRET SHARE ISSUER.
CLASS	A SPECIFIED LEVEL OF ASSURANCES AS DEFINED WITHIN CP § 1.1.4.
CLIENT APPLICATION	AN APPLICATION THAT RUNS ON A PERSONAL COMPUTER OR WORKSTATION AND RELIES ON A SERVER TO PERFORM SOME OPERATION.
COMMON KEY	SOME SYSTEMS OF CRYPTOGRAPHIC HARDWARE REQUIRE ARMING THROUGH A SECRET-SHARING PROCESS AND REQUIRE THAT THE LAST OF THESE SHARES REMAIN PHYSICALLY ATTACHED TO THE HARDWARE IN ORDER FOR IT TO STAY ARMED. IN THIS CASE, "COMMON KEY" REFERS TO THIS LAST SHARE. IT IS NOT ASSUMED TO BE SECRET AS IT IS NOT CONTINUALLY IN AN INDIVIDUAL'S POSSESSION.
COMMUNICATION/NETWORK SYSTEM	A SET OF RELATED, REMOTELY CONNECTED DEVICES AND COMMUNICATIONS FACILITIES INCLUDING MORE THAN ONE COMPUTER SYSTEM WITH THE CAPABILITY TO TRANSMIT DATA AMONG THEM THROUGH THE COMMUNICATIONS FACILITIES



TERM	DEFINITION
	<p>(COVERING ISDN, LEASE LINES, DIAL-UP, LAN, WAN, ETC.).</p>
COMPLIANCE AUDIT	<p>A PERIODIC AUDIT THAT THE MTNLTRUSTLINE OR ITS CUSTOMER UNDERGOES TO DETERMINE ITS CONFORMANCE WITH MTNLTRUSTLINE PKI REQUIREMENTS THAT APPLY TO IT.</p>
COMPROMISE	<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>
COMPUTER	<p>ANY ELECTRONIC, MAGNETIC, OPTICAL OR OTHER HIGH-SPEED DATA PROCESSING DEVICE OR SYSTEM WHICH PERFORMS LOGICAL, ARITHMETIC, AND MEMORY FUNCTIONS BY MANIPULATIONS OF ELECTRONIC, MAGNETIC OR OPTICAL IMPULSES, AND INCLUDES ALL INPUT, OUTPUT, PROCESSING, STORAGE, COMPUTER SOFTWARE, OR COMMUNICATION FACILITIES WHICH ARE CONNECTED OR RELATED TO THE COMPUTER IN A COMPUTER SYSTEM OR COMPUTER NETWORK.</p>
COMPUTER CENTRE	<p>(SEE DATA CENTRE)</p>
COMPUTER DATA BASE	<p>MEANS A REPRESENTATION OF INFORMATION, KNOWLEDGE, FACTS, CONCEPTS OR INSTRUCTIONS IN TEXT, IMAGE, AUDIO, VIDEO THAT ARE BEING PREPARED OR HAVE BEEN PREPARED IN A FORMALISED MANNER OR HAVE BEEN PRODUCED BY A COMPUTER, COMPUTER SYSTEM OR COMPUTER NETWORK AND ARE INTENDED FOR USE IN A COMPUTER, COMPUTER SYSTEM OR COMPUTER NETWORK.</p>
COMPUTER NETWORK	<p>INTERCONNECTION OF ONE OR MORE COMPUTERS THROUGH—</p> <p>(I) THE USE OF SATELLITE, MICROWAVE, TERRESTRIAL LINE OR OTHER COMMUNICATION MEDIA; AND</p> <p>(II) TERMINALS OR A COMPLEX CONSISTING OF TWO OR MORE INTERCONNECTED COMPUTERS WHETHER OR NOT THE INTERCONNECTION IS CONTINUOUSLY MAINTAINED.</p>
COMPUTER PERIPHERAL	<p>MEANS EQUIPMENT THAT WORKS IN CONJUNCTION WITH A COMPUTER BUT IS NOT A PART OF THE MAIN COMPUTER ITSELF, SUCH AS PRINTER, MAGNETIC TAPE READER, ETC.</p>
COMPUTER RESOURCE	<p>MEANS COMPUTER, COMPUTER SYSTEM, COMPUTER NETWORK, DATA, COMPUTER DATABASE OR SOFTWARE.</p>
COMPUTER SYSTEM	<p>A DEVICE OR COLLECTION OF DEVICES, INCLUDING INPUT AND OUTPUT SUPPORT DEVICES AND EXCLUDING CALCULATORS WHICH ARE NOT PROGRAMMABLE AND CAPABLE OF BEING USED IN CONJUNCTION WITH EXTERNAL FILES, WHICH CONTAIN COMPUTER</p>



TERM	DEFINITION
	PROGRAMMES, ELECTRONIC INSTRUCTIONS, INPUT DATA AND OUTPUT DATA, THAT PERFORMS LOGIC, ARITHMETIC, DATA STORAGE AND RETRIEVAL, COMMUNICATION CONTROL AND OTHER FUNCTIONS.
COMPUTER VIRUS	(SEE VIRUS)
CONFIDENTIAL INFORMATION	INFORMATION REQUIRED TO BE KEPT CONFIDENTIAL PURSUANT TO CP § 2.8.1.
CONFIDENTIALITY	THE CONDITION IN WHICH SENSITIVE DATA IS KEPT SECRET AND DISCLOSED ONLY TO AUTHORIZED PARTIES.
CONFIRM	TO ASCERTAIN THROUGH APPROPRIATE INQUIRY AND INVESTIGATION. (SEE ALSO AUTHENTICATION; VERIFY A DIGITAL SIGNATURE)
CONFIRMATION OF DIGITAL SIGNATURE CERTIFICATE CHAIN	THE PROCESS OF VALIDATING A DIGITAL SIGNATURE CERTIFICATE CHAIN AND SUBSEQUENTLY VALIDATING AN END-USER SUBSCRIBER DIGITAL SIGNATURE CERTIFICATE.
CONTINGENCY PLANS	THE ESTABLISHMENT OF EMERGENCY RESPONSE, BACK UP OPERATION, AND POST-DISASTER RECOVERY PROCESSES MAINTAINED BY AN INFORMATION PROCESSING FACILITY OR FOR AN INFORMATION SYSTEM. ESTABLISH THE STRATEGY FOR RECOVERING FROM UNPLANNED DISRUPTION OF INFORMATION PROCESSING OPERATIONS. THE STRATEGY INCLUDES THE IDENTIFICATION AND PRIORITY OF WHAT MUST BE DONE, WHO PERFORMS THE REQUIRED ACTION, AND WHAT TOOLS MUST BE USED. A DOCUMENT, DEVELOPED IN CONJUNCTION WITH APPLICATION OWNERS AND MAINTAINED AT THE PRIMARY AND BACKUP COMPUTER INSTALLATION, WHICH DESCRIBES PROCEDURES AND IDENTIFIES THE PERSONNEL NECESSARY TO RESPOND TO ABNORMAL SITUATIONS SUCH AS DISASTERS. CONTINGENCY PLANS HELP MANAGERS ENSURE THAT COMPUTER APPLICATION OWNERS CONTINUE TO PROCESS (WITH OR WITHOUT COMPUTERS) MISSION-CRITICAL APPLICATIONS IN THE EVENT THAT COMPUTER SUPPORT IS INTERRUPTED.
CONTROLS	MEASURES TAKEN TO ENSURE THE INTEGRITY AND QUALITY OF A PROCESS.
CORRESPOND	TO BELONG TO THE SAME KEY PAIR. (SEE ALSO PUBLIC KEY; PRIVATE KEY)
CRITICAL INFORMATION	DATA DETERMINED BY THE DATA OWNER AS MISSION CRITICAL OR ESSENTIAL TO BUSINESS PURPOSES.
CROSS-CERTIFICATE	A CERTIFICATE USED TO ESTABLISH A TRUST RELATIONSHIP BETWEEN TWO CERTIFYING AUTHORITIES.



TERM	DEFINITION
CRYPTOGRAPHIC ALGORITHM	A CLEARLY SPECIFIED MATHEMATICAL PROCESS FOR COMPUTATION; A SET OF RULES THAT PRODUCE A PRESCRIBED RESULT.
CRYPTOGRAPHY (SEE ALSO PUBLIC KEY CRYPTOGRAPHY)	(I) THE MATHEMATICAL SCIENCE USED TO SECURE THE CONFIDENTIALITY AND AUTHENTICATION OF DATA BY REPLACING IT WITH A TRANSFORMED VERSION THAT CAN BE RECOVERED TO REVEAL THE ORIGINAL DATA ONLY BY SOMEONE HOLDING THE PROPER CRYPTOGRAPHIC ALGORITHM AND KEY. (II) A DISCIPLINE THAT EMBODIES THE PRINCIPLES, MEANS, AND METHODS FOR TRANSFORMING DATA IN ORDER TO HIDE ITS INFORMATION CONTENT, PREVENT ITS UNDETECTED MODIFICATION, AND/OR PREVENT ITS UNAUTHORIZED USES.
CUSTODIAN	A MTNLTRUSTLINE TRUSTED PERSON WHO HOLDS A SECRET SHARE.
CUSTOMER	AN INDIVIDUAL OR ORGANIZATION THAT HAS PURCHASED A PRODUCT OR SERVICE FROM MTNLTRUSTLINE AND/OR ITS REPRESENTATIVES. ORGANIZATIONAL CUSTOMERS INCLUDE ORGANIZATIONS THAT ARE SUB-CAS AND/ OR RAS WITHIN THE MTNLTRUSTLINE PKI.
DAMAGE	MEANS TO DESTROY, ALTER, DELETE, ADD, MODIFY OR REARRANGE ANY COMPUTER RESOURCE BY ANY MEANS.
DATA	MEANS A REPRESENTATION OF INFORMATION, KNOWLEDGE, FACTS, CONCEPTS OR INSTRUCTIONS WHICH ARE BEING PREPARED OR HAVE BEEN PREPARED IN A FORMALISED MANNER, AND IS INTENDED TO BE PROCESSED, IS BEING PROCESSED OR HAS BEEN PROCESSED IN A COMPUTER SYSTEM OR COMPUTER NETWORK, AND MAY BE IN ANY FORM (INCLUDING COMPUTER PRINTOUTS MAGNETIC OR OPTICAL STORAGE MEDIA, PUNCHED CARDS, PUNCHED TAPES) OR STORED INTERNALLY IN THE MEMORY OF THE COMPUTER.
DATA BASE	(SEE COMPUTER DATABASE)
DATA CENTRE (AS ALSO COMPUTER CENTRE)	THE FACILITY COVERING THE COMPUTER ROOM, MEDIA LIBRARY, NETWORK AREA, SERVER AREA, PROGRAMMING AND ADMINISTRATION AREAS, OTHER STORAGE AND SUPPORT AREAS USED TO CARRY OUT THE COMPUTER PROCESSING FUNCTIONS. USUALLY REFERS TO THE COMPUTER ROOM AND MEDIA LIBRARY.
DATA CONFIDENTIALITY	(SEE CONFIDENTIALITY)
DATA INTEGRITY	A CONDITION IN WHICH DATA HAS NOT BEEN ALTERED OR DESTROYED IN AN UNAUTHORIZED MANNER. (SEE ALSO THREAT; COMPROMISE)



TERM	DEFINITION
DATA SECURITY	THE PRACTICE OF PROTECTING DATA FROM ACCIDENTAL OR MALICIOUS MODIFICATION, DESTRUCTION, OR DISCLOSURE.
DEMO CERTIFICATE	A DIGITAL SIGNATURE CERTIFICATE ISSUED BY A CERTIFYING AUTHORITY TO BE USED EXCLUSIVELY FOR DEMONSTRATION AND PRESENTATION PURPOSES AND NOT FOR ANY SECURE OR CONFIDENTIAL COMMUNICATIONS. DEMO DIGITAL SIGNATURE CERTIFICATES MAY BE USED BY AUTHORIZED PERSONS ONLY.
DIGITAL CERTIFICATE	SEE CERTIFICATE.
DIGITAL CERTIFICATE APPLICANT	A PERSON THAT REQUESTS THE ISSUANCE OF A PUBLIC KEY DIGITAL SIGNATURE CERTIFICATE BY A CERTIFYING AUTHORITY. (SEE ALSO CA APPLICANT; SUBSCRIBER)
DIGITAL CERTIFICATE APPLICATION	A REQUEST FROM A DIGITAL SIGNATURE CERTIFICATE APPLICANT (OR AUTHORIZED AGENT) TO A CERTIFYING AUTHORITY FOR THE ISSUANCE OF A DIGITAL SIGNATURE CERTIFICATE. (SEE ALSO CERTIFICATE APPLICANT; CERTIFICATE SIGNING REQUEST)
DIGITAL SIGNATURE	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.
DIGITAL SIGNATURE CERTIFICATE	MEANS A DIGITAL SIGNATURE CERTIFICATE ISSUED UNDER SUB SECTION (4) OF SECTION 35 OF THE INFORMATION TECHNOLOGY ACT, 2000.
DISTINGUISHED NAME	A SET OF DATA THAT IDENTIFIES A REAL-WORLD ENTITY, SUCH AS A PERSON IN A COMPUTER-BASED CONTEXT.
DOCUMENT	A RECORD CONSISTING OF INFORMATION INSCRIBED ON A TANGIBLE MEDIUM SUCH AS PAPER RATHER THAN COMPUTER-BASED INFORMATION. (SEE ALSO MESSAGE; RECORD)
ELECTRONIC FORM	WITH REFERENCE TO INFORMATION MEANS ANY INFORMATION GENERATED, SENT, RECEIVED OR STORED IN MEDIA, MAGNETIC, OPTICAL, COMPUTER MEMORY, MICRO-FILM, COMPUTER GENERATED MICRO FICHE OR SIMILAR DEVICE.
ELECTRONIC MAIL ("E MAIL")	MESSAGES SENT, RECEIVED OR FORWARDED IN DIGITAL FORM VIA A COMPUTER-BASED COMMUNICATION MECHANISM.
ELECTRONIC RECORD	MEANS DATA, RECORD OR DATA GENERATED, IMAGE OR SOUND STORED, RECEIVED OR SENT IN AN ELECTRONIC FORM OR MICROFILM OR COMPUTER GENERATED MICRO-FICHE.



TERM	DEFINITION
ENCRYPTION	<p>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.</p> <p>THERE ARE TWO MAIN TYPES OF ENCRYPTION: ASYMMETRIC ENCRYPTION (ALSO CALLED PUBLIC-KEY ENCRYPTION) AND SYMMETRIC ENCRYPTION.</p>
EXTENSIONS	<p>EXTENSION FIELDS IN X.509 v3 CERTIFICATES. (SEE X.509)</p>
FILE TRANSFER PROTOCOL (FTP)	<p>THE APPLICATION PROTOCOL THAT OFFERS FILE SYSTEM ACCESS FROM THE INTERNET SUITE OF PROTOCOLS.</p>
FIREWALL/DOUBLE FIREWALL	<p>ONE OF SEVERAL TYPES OF INTELLIGENT DEVICES (SUCH AS ROUTERS OR GATEWAYS) USED TO ISOLATE NETWORKS. FIREWALLS MAKE IT DIFFICULT FOR ATTACKERS TO JUMP FROM NETWORK TO NETWORK. A DOUBLE FIREWALL IS TWO FIREWALLS CONNECTED TOGETHER. DOUBLE FIREWALLS ARE USED TO MINIMISE RISK IF ONE FIREWALL GETS COMPROMISED OR PROVIDE ADDRESS TRANSLATION FUNCTIONS.</p>
FUNCTION	<p>IN RELATION TO A COMPUTER, INCLUDES LOGIC, CONTROL, ARITHMETICAL PROCESS, DELETION, STORAGE AND RETRIEVAL AND COMMUNICATION OR TELECOMMUNICATION FROM OR WITHIN A COMPUTER.</p>
GATEWAY	<p>HARDWARE OR SOFTWARE THAT IS USED TO TRANSLATE PROTOCOLS BETWEEN TWO OR MORE SYSTEMS.</p>
GENERATE A KEY PAIR	<p>A TRUSTWORTHY PROCESS OF CREATING PRIVATE KEYS DURING DIGITAL SIGNATURE CERTIFICATE APPLICATION WHOSE CORRESPONDING PUBLIC KEYS ARE SUBMITTED TO THE APPLICABLE CERTIFYING AUTHORITY DURING DIGITAL SIGNATURE CERTIFICATE APPLICATION IN A MANNER THAT DEMONSTRATES THE APPLICANT'S CAPACITY TO USE THE PRIVATE KEY.</p>
HARD COPY	<p>A COPY OF COMPUTER OUTPUT THAT IS PRINTED ON PAPER IN A VISUALLY READABLE FORM; E.G. PRINTED REPORTS, LISTING, AND DOCUMENTS.</p>
HASH (HASH FUNCTION)	<p>AN ALGORITHM THAT MAPS OR TRANSLATES ONE SET OF BITS INTO ANOTHER (GENERALLY SMALLER) SET IN SUCH A WAY THAT :</p> <p>I) A MESSAGE YIELDS THE SAME RESULT EVERY TIME THE ALGORITHM IS EXECUTED USING THE SAME MESSAGE AS INPUT.</p> <p>II) IT IS COMPUTATIONALLY INFEASIBLE FOR A MESSAGE TO BE DERIVED OR RECONSTITUTED FROM THE RESULT PRODUCED BY THE</p>



TERM	DEFINITION
HIGH-SECURITY ZONE	<p>ALGORITHM. II) IT IS COMPUTATIONALLY INFEASIBLE TO FIND TWO DIFFERENT MESSAGES THAT PRODUCE THE SAME HASH RESULT USING THE SAME ALGORITHM.</p> <p>AN AREA TO WHICH ACCESS IS CONTROLLED THROUGH AN ENTRY POINT AND LIMITED TO AUTHORIZED, APPROPRIATELY SCREENED PERSONNEL AND PROPERLY ESCORTED VISITORS. HIGH-SECURITY ZONES SHOULD BE ACCESSIBLE ONLY FROM SECURITY ZONES, AND ARE SEPARATED FROM SECURITY ZONES AND OPERATIONS ZONES BY A PERIMETER. HIGH-SECURITY ZONES ARE MONITORED 24 HOURS A DAY A WEEK BY SECURITY STAFF, OTHER PERSONNEL OR ELECTRONIC MEANS.</p>
IDENTIFICATION / IDENTIFY	<p>THE PROCESS OF CONFIRMING THE IDENTITY OF A PERSON. IDENTIFICATION IS FACILITATED IN PUBLIC KEY CRYPTOGRAPHY BY MEANS OF CERTIFICATES.</p>
IDENTITY	<p>A UNIQUE PIECE OF INFORMATION THAT MARKS OR SIGNIFIES A PARTICULAR ENTITY WITHIN A DOMAIN. SUCH INFORMATION IS ONLY UNIQUE WITHIN A PARTICULAR DOMAIN.</p>
INDIAN IT-ACT 2000	<p>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.</p>
INFORMATION	<p>INCLUDES DATA, TEXT, IMAGES, SOUND, VOICE, CODES, COMPUTER PROGRAMMES, SOFTWARE AND DATABASES OR MICRO-FILM OR COMPUTER GENERATED MICRO FICHE.</p>
INFORMATION ASSETS	<p>MEANS ALL INFORMATION RESOURCES UTILIZED IN THE COURSE OF ANY ORGANIZATION'S BUSINESS AND INCLUDES ALL INFORMATION, APPLICATION SOFTWARE (DEVELOPED OR PURCHASED), AND TECHNOLOGY (HARDWARE, SYSTEM SOFTWARE AND NETWORKS).</p>
INFORMATION TECHNOLOGY SECURITY	<p>ALL ASPECTS RELATED TO DEFINING, ACHIEVING, AND MAINTAINING CONFIDENTIALITY, INTEGRITY, AVAILABILITY, ACCOUNTABILITY, AUTHENTICITY, AND RELIABILITY.</p>
INFORMATION TECHNOLOGY SECURITY POLICY	<p>RULES, DIRECTIVES AND PRACTICES THAT GOVERN HOW INFORMATION ASSETS, INCLUDING SENSITIVE INFORMATION, ARE MANAGED, PROTECTED AND DISTRIBUTED WITHIN AN ORGANIZATION AND ITS INFORMATION TECHNOLOGY SYSTEMS.</p>
INTERMEDIARY	<p>WITH RESPECT TO ANY PARTICULAR ELECTRONIC MESSAGE MEANS ANY PERSON WHO ON BEHALF OF ANOTHER PERSON RECEIVES, STORES OR TRANSMITS THAT MESSAGE OR PROVIDES ANY SERVICE</p>



TERM	DEFINITION
	WITH RESPECT TO THAT MESSAGE.
KEY	A SEQUENCE OF SYMBOLS THAT CONTROLS THE OPERATION OF A CRYPTOGRAPHIC TRANSFORMATION (E.G. ENCIPHERMENT, DECIPHERMENT, CRYPTOGRAPHIC CHECK FUNCTION COMPUTATION, SIGNATURE GENERATION, OR SIGNATURE VERIFICATION).
KEY GENERATION	THE TRUSTWORTHY PROCESS OF CREATING A PRIVATE KEY / PUBLIC KEY PAIR.
KEY MANAGEMENT	THE ADMINISTRATION AND USE OF THE GENERATION, REGISTRATION, CERTIFICATION, DEREGISTRATION, DISTRIBUTION, INSTALLATION, STORAGE, ARCHIVING, REVOCATION, DERIVATION AND DESTRUCTION OF KEYING MATERIAL IN ACCORDANCE WITH A SECURITY POLICY.
KEY PAIR	IN AN ASYMMETRIC CRYPTO SYSTEM, MEANS A PRIVATE KEY AND ITS MATHEMATICALLY RELATED PUBLIC KEY, WHICH ARE SO RELATED THAT THE PUBLIC KEY CAN VERIFY A DIGITAL SIGNATURE CREATED BY THE PRIVATE KEY.
LICENCE	MEANS A LICENCE GRANTED TO A CERTIFYING AUTHORITY.
LOCAL AREA NETWORK (LAN)	A GEOGRAPHICALLY SMALL NETWORK OF COMPUTERS AND SUPPORTING COMPONENTS USED BY A GROUP OR DEPARTMENT TO SHARE RELATED SOFTWARE AND HARDWARE RESOURCES.
LOW-SENSITIVE	APPLIES TO INFORMATION THAT, IF COMPROMISED, COULD REASONABLY BE EXPECTED TO CAUSE INJURY OUTSIDE THE NATIONAL INTEREST, FOR EXAMPLE, DISCLOSURE OF AN EXACT SALARY FIGURE.
MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE	[SEE CERTIFICATE MANAGEMENT]
MEDIA	THE MATERIAL OR CONFIGURATION ON WHICH DATA IS RECORDED. EXAMPLES INCLUDE MAGNETIC TAPS AND DISKS.
MESSAGE	A DIGITAL REPRESENTATION OF INFORMATION; A COMPUTER-BASED RECORD. A SUBSET OF RECORD. (SEE ALSO RECORD)
MTNLTRUSTLINE	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'.
MTNLTRUSTLINE PKI PARTICIPANTS	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.
MTNLTRUSTLINE SECURITY	THE HIGHEST-LEVEL DOCUMENT DESCRIBING MTNLTRUSTLINE'S



TERM	DEFINITION
POLICY	SECURITY POLICIES.
MTNLTRUSTLINE REPOSITORY	MTNLTRUSTLINE'S DATABASE OF RELEVANT MTNLTRUSTLINE PKI INFORMATION ACCESSIBLE ONLINE.
NAME	A SET OF IDENTIFYING ATTRIBUTES PURPORTED TO DESCRIBE AN ENTITY OF A CERTAIN TYPE.
NETWORK	A SET OF RELATED, REMOTELY CONNECTED DEVICES AND COMMUNICATIONS FACILITIES INCLUDING MORE THAN ONE COMPUTER SYSTEM WITH THE CAPABILITY TO TRANSMIT DATA AMONG THEM THROUGH THE
NETWORK ADMINISTRATOR	THE PERSON AT A COMPUTER NETWORK INSTALLATION WHO DESIGNS, CONTROLS, AND MANAGES THE USE OF THE COMPUTER NETWORK.
NODE	IN A NETWORK, A POINT AT WHICH ONE OR MORE FUNCTIONAL UNITS CONNECT CHANNELS OR DATA CIRCUITS.
NOMINATED WEBSITE	A WEBSITE DESIGNATED BY THE CERTIFYING AUTHORITY FOR DISPLAY OF INFORMATION SUCH AS FEE SCHEDULE, CERTIFICATION PRACTICE STATEMENT, CERTIFICATE POLICY ETC.
NON-REPUDIATION	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. NOTE: ONLY ADJUDICATION BY A COURT, ARBITRATION PANEL, CCA, OR OTHER TRIBUNAL CAN ULTIMATELY PREVENT REPUDIATION. 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.
NOTARY	A NATURAL PERSON AUTHORIZED BY AN EXECUTIVE GOVERNMENTAL AGENCY TO PERFORM NOTARIAL SERVICES SUCH AS TAKING ACKNOWLEDGMENTS, ADMINISTERING OATHS OR AFFIRMATIONS, WITNESSING OR ATTESTING SIGNATURES, AND NOTING PROTESTS OF NEGOTIABLE INSTRUMENTS.
OFFLINE SUBORDINATE CERTIFYING AUTHORITY (OFFLINE SUB-CA)	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



TERM	DEFINITION
	USER SUBSCRIBER'S CERTIFICATE.
ON-LINE	COMMUNICATIONS THAT PROVIDE A REAL-TIME CONNECTION.
ONLINE SUBORDINATE CERTIFYING AUTHORITY (ONLINE SUB-CA)	A CERTIFYING AUTHORITY THAT ISSUES THE END USER SUBSCRIBER CERTIFICATES.
OPERATIONAL CERTIFICATE	A DIGITAL SIGNATURE CERTIFICATE WHICH IS WITHIN ITS OPERATIONAL PERIOD AT THE PRESENT DATE AND TIME OR AT A DIFFERENT SPECIFIED DATE AND TIME, DEPENDING ON THE CONTEXT.
OPERATIONAL MANAGEMENT	REFERS TO ALL BUSINESS/SERVICE UNIT MANAGEMENT (I.E. THE USER MANAGEMENT) AS WELL AS INFORMATION TECHNOLOGY MANAGEMENT.
OPERATIONAL PERIOD	THE PERIOD STARTING WITH THE DATE AND TIME A DIGITAL SIGNATURE CERTIFICATE IS ISSUED (OR ON A LATER DATE AND TIME CERTAIN IF STATED IN THE DIGITAL SIGNATURE CERTIFICATE) AND ENDING WITH THE DATE AND TIME ON WHICH THE DIGITAL SIGNATURE CERTIFICATE EXPIRES OR IS EARLIER SUSPENDED OR REVOKED.
OPERATIONS ZONE	AN AREA WHERE ACCESS IS LIMITED TO PERSONNEL WHO WORK THERE AND TO PROPERLY ESCORTED VISITORS. OPERATIONS ZONES SHOULD BE MONITORED AT LEAST PERIODICALLY, BASED ON A THREAT RISK ASSESSMENT (TRA), AND SHOULD PREFERABLY BE ACCESSIBLE FROM A RECEPTION ZONE.
ORGANIZATION	AN ENTITY WITH WHICH A USER IS AFFILIATED. AN ORGANIZATION MAY ALSO BE A USER.
ORIGINATOR	A PERSON WHO SENDS, GENERATES, STORES OR TRANSMITS ANY ELECTRONIC MESSAGE OR CAUSES ANY ELECTRONIC MESSAGE TO BE SENT, GENERATED, STORED OR TRANSMITTED TO ANY OTHER PERSON BUT DOES NOT INCLUDE AN INTERMEDIARY.
PARTICULARLY SENSITIVE	APPLIES TO INFORMATION THAT, IF COMPROMISED, COULD REASONABLY BE EXPECTED TO CAUSE SERIOUS INJURY OUTSIDE THE NATIONAL INTEREST, FOR EXAMPLE LOSS OF REPUTATION OR COMPETITIVE ADVANTAGE.
PASSWORD (PASS PHRASE; PIN NUMBER)	CONFIDENTIAL AUTHENTICATION INFORMATION USUALLY COMPOSED OF A STRING OF CHARACTERS USED TO PROVIDE ACCESS TO A COMPUTER RESOURCE.
PC CARD (SEE ALSO SMART CARD)	A HARDWARE TOKEN COMPLIANT WITH STANDARDS PROMULGATED BY THE PERSONAL COMPUTER MEMORY CARD INTERNATIONAL ASSOCIATION (PCMCIA) PROVIDING EXPANSION CAPABILITIES TO



TERM	DEFINITION
	COMPUTERS, INCLUDING THE FACILITATION OF INFORMATION SECURITY.
PERSON	MEANS ANY COMPANY OR ASSOCIATION OR INDIVIDUAL OR BODY OF INDIVIDUALS, WHETHER INCORPORATED OR NOT.
PERSONAL PRESENCE	THE ACT OF APPEARING (PHYSICALLY RATHER THAN VIRTUALLY OR FIGURATIVELY) BEFORE A CERTIFYING AUTHORITY OR ITS DESIGNEE AND PROVING ONE'S IDENTITY AS A PREREQUISITE TO DIGITAL SIGNATURE CERTIFICATE ISSUANCE UNDER CERTAIN CIRCUMSTANCES.
PKCS #10	PUBLIC-KEY CRYPTOGRAPHY STANDARD #10, DEVELOPED BY RSA SECURITY INC., WHICH DEFINES A STRUCTURE FOR A CERTIFICATE SIGNING REQUEST.
PKCS #12	PUBLIC-KEY CRYPTOGRAPHY STANDARD #12, DEVELOPED BY RSA SECURITY INC., WHICH DEFINES A SECURE MEANS FOR THE TRANSFER OF PRIVATE KEYS.
PKI (PUBLIC KEY INFRASTRUCTURE) / PKI SERVER	A SET OF POLICIES, PROCESSES, SERVER PLATFORMS, SOFTWARE AND WORKSTATIONS USED FOR THE PURPOSE OF ADMINISTERING DIGITAL SIGNATURE CERTIFICATES AND PUBLIC-PRIVATE KEY PAIRS, INCLUDING THE ABILITY TO GENERATE, ISSUE, MAINTAIN, AND REVOKE PUBLIC KEY CERTIFICATES.
PKI HIERARCHY	A SET OF CERTIFYING AUTHORITIES WHOSE FUNCTIONS ARE ORGANIZED ACCORDING TO THE PRINCIPLE OF DELEGATION OF AUTHORITY AND RELATED TO EACH OTHER AS SUBORDINATE AND SUPERIOR CERTIFYING AUTHORITY.
PLEDGE	(SEE SOFTWARE PUBLISHER'S PLEDGE)
POLICY	<p>A BRIEF DOCUMENT THAT STATES THE HIGH-LEVEL ORGANIZATION POSITION, STATES THE SCOPE, AND ESTABLISHES WHO IS RESPONSIBLE FOR COMPLIANCE WITH THE POLICY AND THE CORRESPONDING STANDARDS.</p> <p>FOLLOWING IS AN ABBREVIATED EXAMPLE OF WHAT A POLICY MAY CONTAIN</p> <ul style="list-style-type: none">● INTRODUCTION● DEFINITIONS● POLICY STATEMENT IDENTIFYING THE NEED FOR "SOMETHING" (E.G. DATA SECURITY)● SCOPE● PEOPLE PLAYING A ROLE AND THEIR RESPONSIBILITIES● STATEMENT OF ENFORCEMENT, INCLUDING RESPONSIBILITY



TERM	DEFINITION
PRIMARY CERTIFYING AUTHORITY	A MTNLTRUSTLINE PKI CERTIFYING AUTHORITY WHOSE CERTIFICATE IS SIGNED BY THE RCAI.
PRIVATE KEY	THE KEY OF A KEY PAIR USED TO CREATE A DIGITAL SIGNATURE.
PROCEDURE	A SET OF STEPS PERFORMED TO ENSURE THAT A GUIDELINE IS MET.
PROGRAM	A DETAILED AND EXPLICIT SET OF INSTRUCTIONS FOR ACCOMPLISHING SOME PURPOSE, THE SET BEING EXPRESSED IN SOME LANGUAGE SUITABLE FOR INPUT TO A COMPUTER, OR IN MACHINE LANGUAGE.
PROXY SERVER	A SERVER THAT SITS BETWEEN A CLIENT APPLICATION SUCH AS A WEB BROWSER AND A REAL SERVER. IT INTERCEPTS ALL REQUESTS TO THE REAL SERVER TO SEE IF IT CAN FULFILL THE REQUEST ITSELF. IF NOT, IT FORWARDS THE REQUEST TO THE REAL SERVER.
PUBLIC ACCESS ZONE	GENERALLY SURROUNDS OR FORMS PART OF A GOVERNMENT FACILITY. EXAMPLES INCLUDE THE GROUNDS SURROUNDING A BUILDING, AND PUBLIC CORRIDORS AND ELEVATOR LOBBIES IN MULTIPLE-OCCUPANCY BUILDINGS. BOUNDARY DESIGNATORS SUCH AS SIGNS AND DIRECT OR REMOTE SURVEILLANCE MAY BE USED TO DISCOURAGE UNAUTHORIZED ACTIVITY.
PUBLIC KEY	THE KEY OF A KEY PAIR USED TO VERIFY A DIGITAL SIGNATURE AND LISTED IN THE DIGITAL SIGNATURE CERTIFICATE.
PUBLIC KEY CERTIFICATE	(SEE CERTIFICATE)
PUBLIC KEY CRYPTOGRAPHY	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.
PUBLIC KEY INFRASTRUCTURE (PKI)	THE ARCHITECTURE, ORGANIZATION, TECHNIQUES, PRACTICES, AND PROCEDURES THAT COLLECTIVELY SUPPORT THE IMPLEMENTATION AND OPERATION OF A CERTIFICATE-BASED PUBLIC KEY CRYPTOGRAPHIC SYSTEM. IT INCLUDES A SET OF POLICIES, PROCESSES, SERVER PLATFORMS, SOFTWARE AND WORKSTATIONS, USED FOR THE PURPOSE OF ADMINISTERING DIGITAL SIGNATURE CERTIFICATES AND KEYS.
PUBLIC/PRIVATE KEY PAIR	(SEE PUBLIC KEY; PRIVATE KEY; KEY PAIR)



TERM	DEFINITION
RECIPIENT (OF A DIGITAL SIGNATURE)	A PERSON WHO RECEIVES A DIGITAL SIGNATURE AND WHO IS IN A POSITION TO RELY ON IT, WHETHER OR NOT SUCH RELIANCE OCCURS. (SEE ALSO RELYING PARTY)
RECORD	INFORMATION THAT IS INSCRIBED ON A TANGIBLE MEDIUM (A DOCUMENT) OR STORED IN AN ELECTRONIC OR OTHER MEDIUM AND RETRIEVABLE IN PERCEIVABLE FORM. THE TERM "RECORD" IS A SUPERSET OF THE TWO TERMS "DOCUMENT" AND "MESSAGE". (SEE ALSO DOCUMENT; MESSAGE)
RE-ENROLLMENT	(SEE ALSO RENEWAL)
REGISTRATION AUTHORITY (RA)	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.
RELY / RELIANCE (ON A CERTIFICATE AND DIGITAL SIGNATURE)	TO ACCEPT A DIGITAL SIGNATURE AND ACT IN A MANNER THAT COULD BE DETRIMENTAL TO ONESELF WERE THE DIGITAL SIGNATURE TO BE INEFFECTIVE. (SEE ALSO RELYING PARTY; RECIPIENT)
RELYING PARTY	AN INDIVIDUAL OR ORGANIZATION THAT ACTS IN RELIANCE ON A CERTIFICATE AND/OR A DIGITAL SIGNATURE.
RELYING PARTY AGREEMENT	AN AGREEMENT USED BY MTNLTRUSTLINE SETTING FORTH THE TERMS AND CONDITIONS UNDER WHICH AN INDIVIDUAL OR ORGANIZATION ACTS AS A RELYING PARTY.
RENEWAL	THE PROCESS OF OBTAINING A NEW DIGITAL SIGNATURE CERTIFICATE OF THE SAME CLASS AND TYPE FOR THE SAME SUBJECT ONCE AN EXISTING DIGITAL SIGNATURE CERTIFICATE HAS EXPIRED.
REPOSITORY	A DATABASE OF DIGITAL SIGNATURE CERTIFICATES AND OTHER RELEVANT INFORMATION ACCESSIBLE ON-LINE.
REPUDIATION	(SEE ALSO NONREPUDIATION) THE DENIAL OR ATTEMPTED DENIAL BY AN ENTITY INVOLVED IN A COMMUNICATION OF HAVING PARTICIPATED IN ALL OR PART OF THE COMMUNICATION.
REVOKE A CERTIFICATE	THE PROCESS OF PERMANENTLY ENDING THE OPERATIONAL PERIOD OF A DIGITAL SIGNATURE CERTIFICATE FROM A SPECIFIED TIME FORWARD.
RISK	THE POTENTIAL OF DAMAGE TO A SYSTEM OR ASSOCIATED ASSETS THAT EXISTS AS A RESULT OF THE COMBINATION OF SECURITY THREAT AND VULNERABILITY.



TERM	DEFINITION
RISK ANALYSIS	THE PROCESS OF IDENTIFYING SECURITY RISKS, DETERMINING THEIR MAGNITUDE, AND IDENTIFYING AREAS NEEDING SAFEGUARDS.
RISK ASSESSMENT	AN ANALYSIS OF SYSTEM ASSETS AND VULNERABILITIES TO ESTABLISH AN EXPECTED LOSS FROM CERTAIN EVENTS BASED ON ESTIMATED PROBABILITIES OF THE OCCURRENCE OF THOSE EVENTS.
RISK MANAGEMENT	THE TOTAL PROCESS OF IDENTIFYING, CONTROLLING, AND ELIMINATING OR MINIMIZING UNCERTAIN EVENTS THAT MAY AFFECT INFORMATION TECHNOLOGY SYSTEM RESOURCES.
RSA	A PUBLIC KEY CRYPTOGRAPHIC SYSTEM INVENTED BY RIVEST, SHAMIR & ADELMAN.
S/MIME	A SPECIFICATION FOR E-MAIL SECURITY EXPLOITING A CRYPTOGRAPHIC MESSAGE SYNTAX IN AN INTERNET MIME ENVIRONMENT.
SECRET SHARE	A PORTION OF A CRYPTOGRAPHIC SECRET SPLIT AMONG A NUMBER OF PHYSICAL TOKENS.
SECRET SHARE HOLDER	AN AUTHORIZED HOLDER OF A PHYSICAL TOKEN CONTAINING A SECRET SHARE.
SECRET SHARING	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 § 6.2.2.
SECURE CHANNEL	A CRYPTOGRAPHICALLY ENHANCED COMMUNICATIONS PATH THAT PROTECTS MESSAGES AGAINST PERCEIVED SECURITY THREATS.
SECURE SYSTEM	MEANS COMPUTER HARDWARE, SOFTWARE, AND PROCEDURE THAT— (A) ARE REASONABLY SECURE FROM UNAUTHORIZED ACCESS AND MISUSE; (B) PROVIDE A REASONABLE LEVEL OF RELIABILITY AND CORRECT OPERATION; (C) ARE REASONABLY SUITED TO PERFORMING THE INTENDED FUNCTIONS; AND (D) ADHERE TO GENERALLY ACCEPTED SECURITY PROCEDURES.
SECURITY	THE QUALITY OR STATE OF BEING PROTECTED FROM UNAUTHORIZED ACCESS OR UNCONTROLLED LOSSES OR EFFECTS. ABSOLUTE SECURITY IS IMPOSSIBLE TO ACHIEVE IN PRACTICE AND THE QUALITY OF A GIVEN SECURITY SYSTEM IS RELATIVE. WITHIN A STATE-MODEL SECURITY SYSTEM, SECURITY IS A SPECIFIC "STATE" TO BE



TERM	DEFINITION
	PRESERVED UNDER VARIOUS OPERATIONS.
SECURITY POLICY	A DOCUMENT WHICH ARTICULATES REQUIREMENTS AND GOOD PRACTICES REGARDING THE PROTECTIONS MAINTAINED BY A TRUSTWORTHY SYSTEM.
SECURITY PROCEDURE	MEANS THE SECURITY PROCEDURE PRESCRIBED UNDER SECTION 16 OF THE INFORMATION TECHNOLOGY ACT, 2000.
SECURITY SERVICES	SERVICES PROVIDED BY A SET OF SECURITY FRAMEWORKS AND PERFORMED BY MEANS OF CERTAIN SECURITY MECHANISMS. SUCH SERVICES INCLUDE, BUT ARE NOT LIMITED TO, ACCESS CONTROL, DATA CONFIDENTIALITY, AND DATA INTEGRITY.
SECURITY ZONE	AN AREA TO WHICH ACCESS IS LIMITED TO AUTHORISED PERSONNEL AND TO AUTHORISED AND PROPERLY ESCORTED VISITORS. SECURITY ZONES SHOULD PREFERABLY BE ACCESSIBLE FROM AN OPERATIONS ZONE, AND THROUGH A SPECIFIC ENTRY POINT. A SECURITY ZONE NEED NOT BE SEPARATED FROM AN OPERATIONS ZONE BY A SECURE PERIMETER. A SECURITY ZONE SHOULD BE MONITORED 24 HOURS A DAY AND 7 WEEK BY SECURITY STAFF, OTHER PERSONNEL OR ELECTRONIC MEANS.
SELF-SIGNED PUBLIC KEY	A DATA STRUCTURE THAT IS CONSTRUCTED THE SAME AS A DIGITAL SIGNATURE CERTIFICATE BUT THAT IS SIGNED BY ITS SUBJECT. UNLIKE A DIGITAL SIGNATURE CERTIFICATE, A SELF-SIGNED PUBLIC KEY CANNOT BE USED IN A TRUSTWORTHY MANNER TO AUTHENTICATE A PUBLIC KEY TO OTHER PARTIES.
SERIAL NUMBER	(SEE CERTIFICATE SERIAL NUMBER)
SERVER	A COMPUTER SYSTEM THAT RESPONDS TO REQUESTS FROM CLIENT SYSTEMS.
SIGN	TO CREATE A DIGITAL SIGNATURE FOR A MESSAGE, OR TO AFFIX A SIGNATURE TO A DOCUMENT, DEPENDING UPON THE CONTEXT.
SIGNATURE	(SEE DIGITAL SIGNATURE)
SIGNER	A PERSON WHO CREATES A DIGITAL SIGNATURE FOR A MESSAGE, OR A SIGNATURE FOR A DOCUMENT.
SMART CARD	A HARDWARE TOKEN THAT INCORPORATES ONE OR MORE INTEGRATED CIRCUIT (IC) CHIPS TO IMPLEMENT CRYPTOGRAPHIC FUNCTIONS AND THAT POSSESSES SOME INHERENT RESISTANCE TO TAMPERING.
SUBJECT (OF A	THE HOLDER OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY. THE TERM "SUBJECT" CAN REFER TO BOTH THE EQUIPMENT OR



TERM	DEFINITION
CERTIFICATE)	DEVICE THAT HOLDS A PRIVATE KEY AND TO THE INDIVIDUAL PERSON, IF ANY, WHO CONTROLS THAT EQUIPMENT OR DEVICE. A SUBJECT IS ASSIGNED AN UNAMBIGUOUS NAME, WHICH IS BOUND TO THE PUBLIC KEY CONTAINED IN THE SUBJECT'S DIGITAL SIGNATURE CERTIFICATE.
SUBJECT NAME	THE UNAMBIGUOUS VALUE IN THE SUBJECT NAME FIELD OF A DIGITAL SIGNATURE CERTIFICATE, WHICH IS BOUND TO THE PUBLIC KEY.
SUBSCRIBER	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.
SUBSCRIBER AGREEMENT	THE AGREEMENT EXECUTED BETWEEN A SUBSCRIBER AND A CERTIFYING AUTHORITY FOR THE PROVISION OF DESIGNATED PUBLIC CERTIFICATION SERVICES IN ACCORDANCE WITH THIS CERTIFICATION PRACTICE STATEMENT.
SUBSCRIBER INFORMATION	INFORMATION SUPPLIED TO A CERTIFICATION AUTHORITY AS PART OF A DIGITAL SIGNATURE CERTIFICATE APPLICATION. (SEE ALSO CERTIFICATE APPLICATION)
SUPERIOR ENTITY	AN ENTITY ABOVE A CERTAIN ENTITY WITHIN THE MTNLTRUSTLINE PKI.
SUSPEND A CERTIFICATE	A TEMPORARY "HOLD" PLACED ON THE EFFECTIVENESS OF THE OPERATIONAL PERIOD OF A DIGITAL SIGNATURE CERTIFICATE WITHOUT PERMANENTLY REVOKING THE DIGITAL SIGNATURE CERTIFICATE. A DIGITAL SIGNATURE CERTIFICATE SUSPENSION IS INVOKED BY, E.G., A CRL ENTRY WITH A REASON CODE. (SEE ALSO REVOKE A CERTIFICATE)
SYSTEM ADMINISTRATOR	THE PERSON AT A COMPUTER INSTALLATION WHO DESIGNS, CONTROLS, AND MANAGES THE USE OF THE COMPUTER SYSTEM.
SYSTEM SECURITY	A SYSTEM FUNCTION THAT RESTRICTS THE USE OF OBJECTS TO CERTAIN USERS.
SYSTEM SOFTWARE	APPLICATION-INDEPENDENT SOFTWARE THAT SUPPORTS THE RUNNING OF APPLICATION SOFTWARE. IT IS A SOFTWARE THAT IS PART OF OR MADE AVAILABLE WITH A COMPUTER SYSTEM AND THAT DETERMINES HOW APPLICATION PROGRAMS ARE RUN; FOR EXAMPLE, AN OPERATING SYSTEM.
TEST CERTIFICATE	A DIGITAL SIGNATURE CERTIFICATE ISSUED BY A CERTIFYING



TERM	DEFINITION
	AUTHORITY FOR THE LIMITED PURPOSE OF INTERNAL TECHNICAL TESTING. TEST CERTIFICATES MAY BE USED BY AUTHORIZED PERSONS ONLY.
THREAT	A CIRCUMSTANCE OR EVENT WITH THE POTENTIAL TO CAUSE HARM TO A SYSTEM, INCLUDING THE DESTRUCTION, UNAUTHORIZED DISCLOSURE, OR MODIFICATION OF DATA AND/OR DENIAL OF SERVICE.
TIME STAMP	A NOTATION THAT INDICATES (AT LEAST) THE CORRECT DATE AND TIME OF AN ACTION, AND IDENTITY OF THE PERSON OR DEVICE THAT SENT OR RECEIVED THE TIME STAMP.
TIME-OUT	A SECURITY FEATURE THAT LOGS OFF A USER IF ANY ENTRY IS NOT MADE AT THE TERMINAL WITHIN A SPECIFIED PERIOD OF TIME.
TOKEN	A HARDWARE SECURITY TOKEN CONTAINING A USER'S PRIVATE KEY(S), PUBLIC KEY CERTIFICATE, AND, OPTIONALLY, A CACHE OF OTHER CERTIFICATES, INCLUDING ALL CERTIFICATES IN THE USER'S CERTIFICATION CHAIN.
TRANSACTION	A COMPUTER-BASED TRANSFER OF BUSINESS INFORMATION, WHICH CONSISTS OF SPECIFIC PROCESSES TO FACILITATE COMMUNICATION OVER GLOBAL NETWORKS.
TRUST	GENERALLY, THE ASSUMPTION THAT AN ENTITY WILL BEHAVE SUBSTANTIALLY AS EXPECTED. TRUST MAY APPLY ONLY FOR A SPECIFIC FUNCTION. THE KEY ROLE OF THIS TERM IN AN AUTHENTICATION FRAMEWORK IS TO DESCRIBE THE RELATIONSHIP BETWEEN AN AUTHENTICATING ENTITY AND A CERTIFYING AUTHORITY. AN AUTHENTICATING ENTITY MUST BE CERTAIN THAT IT CAN TRUST THE CERTIFYING AUTHORITY TO CREATE ONLY VALID AND RELIABLE DIGITAL SIGNATURE CERTIFICATES, AND USERS OF THOSE DIGITAL SIGNATURE CERTIFICATES RELY UPON THE AUTHENTICATING ENTITY'S DETERMINATION OF TRUST.
TRUSTED PERSON	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 § 5.2.1.
TRUSTED POSITION	A ROLE THAT INCLUDES ACCESS TO OR CONTROL OVER CRYPTOGRAPHIC OPERATIONS THAT MAY MATERIALLY AFFECT THE ISSUANCE, USE, SUSPENSION, OR REVOCATION OF DIGITAL SIGNATURE CERTIFICATES, INCLUDING OPERATIONS THAT RESTRICT ACCESS TO A REPOSITORY.
TRUSTED THIRD PARTY	IN GENERAL, AN INDEPENDENT, UNBIASED THIRD PARTY THAT



TERM	DEFINITION
	CONTRIBUTES TO THE ULTIMATE SECURITY AND TRUSTWORTHINESS OF COMPUTER-BASED INFORMATION TRANSFERS. A TRUSTED THIRD PARTY DOES NOT CONNOTE THE EXISTENCE OF A TRUSTOR-TRUSTEE OR OTHER FIDUCIARY RELATIONSHIP. (Cf., TRUST)
TRUSTWORTHY SYSTEM	COMPUTER HARDWARE, SOFTWARE, AND PROCEDURES THAT ARE REASONABLY SECURE FROM INTRUSION AND MISUSE; PROVIDE A REASONABLE LEVEL OF AVAILABILITY, RELIABILITY, AND CORRECT OPERATION; ARE REASONABLY SUITED TO PERFORMING THEIR INTENDED FUNCTIONS; AND ENFORCE THE APPLICABLE SECURITY POLICY. A TRUSTWORTHY SYSTEM IS NOT NECESSARILY A "TRUSTED SYSTEM" AS RECOGNIZED IN CLASSIFIED GOVERNMENT NOMENCLATURE.
TYPE (OF CERTIFICATE)	THE DEFINING PROPERTIES OF A DIGITAL SIGNATURE CERTIFICATE, WHICH LIMIT ITS INTENDED PURPOSE TO A CLASS OF APPLICATIONS UNIQUELY, ASSOCIATED WITH THAT TYPE.
UNAMBIGUOUS NAME	(SEE DISTINGUISHED NAME)
UNIFORM RESOURCE LOCATOR (URL)	A STANDARDIZED DEVICE FOR IDENTIFYING AND LOCATING CERTAIN RECORDS AND OTHER RESOURCES LOCATED ON THE WORLD WIDE WEB.
USER	AN AUTHORIZED ENTITY THAT USES A CERTIFICATE AS APPLICANT, SUBSCRIBER, RECIPIENT OR RELYING PARTY, BUT NOT INCLUDING THE CERTIFYING AUTHORITY ISSUING THE DIGITAL SIGNATURE CERTIFICATE. (SEE ALSO CERTIFICATE APPLICANT; ENTITY; PERSON; SUBSCRIBER)
VALID CERTIFICATE	A DIGITAL SIGNATURE CERTIFICATE ISSUED BY A CERTIFYING AUTHORITY AND ACCEPTED BY THE SUBSCRIBER LISTED IN IT.
VALIDATE A CERTIFICATE (I.E. OF AN END-USER SUBSCRIBER CERTIFICATE)	THE PROCESS PERFORMED BY A RECIPIENT OR RELYING PARTY TO CONFIRM THAT AN END-USER SUBSCRIBER DIGITAL SIGNATURE CERTIFICATE IS VALID AND WAS OPERATIONAL AT THE DATE AND TIME A PERTINENT DIGITAL SIGNATURE WAS CREATED.
VALIDATION (OF CERTIFICATE APPLICATION)	THE PROCESS PERFORMED BY THE CERTIFYING AUTHORITY OR ITS AGENT FOLLOWING SUBMISSION OF A DIGITAL SIGNATURE CERTIFICATE APPLICATION AS A PREREQUISITE TO APPROVAL OF THE APPLICATION AND THE ISSUANCE OF A DIGITAL SIGNATURE CERTIFICATE. (SEE ALSO AUTHENTICATION; SOFTWARE VALIDATION)
VALIDATION (OF SOFTWARE)	(SEE SOFTWARE VALIDATION)
VALIDITY PERIOD	THE PERIOD STARTING WITH THE DATE AND TIME A CERTIFICATE IS



TERM	DEFINITION
VERIFY (A DIGITAL SIGNATURE)	<p>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.</p> <p>IN RELATION TO A DIGITAL SIGNATURE, ELECTRONIC RECORD OR PUBLIC KEY, WITH ITS GRAMMATICAL VARIATIONS AND COGNATE EXPRESSIONS MEANS TO DETERMINE WHETHER — (A) THE INITIAL ELECTRONIC RECORD WAS AFFIXED WITH THE DIGITAL SIGNATURE BY THE USE OF PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY OF THE SUBSCRIBER; (B) THE INITIAL ELECTRONIC RECORD IS RETAINED INTACT OR HAS BEEN ALTERED SINCE SUCH ELECTRONIC RECORD WAS SO AFFIXED WITH THE DIGITAL SIGNATURE.</p>
VIRUS	<p>MEANS ANY COMPUTER INSTRUCTION, INFORMATION, DATA OR PROGRAMME THAT DESTROYS, DAMAGES, DEGRADES OR ADVERSELY AFFECTS THE PERFORMANCE OF A COMPUTER RESOURCE OR ATTACHES ITSELF TO ANOTHER COMPUTER RESOURCE AND OPERATES WHEN A PROGRAMME, DATA OR INSTRUCTION IS EXECUTED OR SOME OTHER EVENT TAKES PLACE IN THAT COMPUTER RESOURCE.</p>
VULNERABILITY	<p>A WEAKNESS THAT COULD BE EXPLOITED TO CAUSE DAMAGE TO THE SYSTEM OR THE ASSETS IT CONTAINS.</p>
WEB BROWSER	<p>A SOFTWARE APPLICATION USED TO LOCATE AND DISPLAY WEB PAGES.</p>
WIRELESS APPLICATION PROTOCOL (WAP)	<p>A STANDARD FOR THE PRESENTATION AND DELIVERY OF WIRELESS INFORMATION AND TELEPHONY SERVICES ON MOBILE PHONES AND OTHER WIRELESS TERMINALS.</p>
WIRELESS TRANSPORT LAYER SECURITY (WTLS)	<p>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.</p>
WIRELESS TRANSPORT LAYER SECURITY CERTIFICATE (WTLS CERTIFICATE)	<p>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.</p>
WORLD WIDE WEB (WWW)	<p>A HYPERTEXT-BASED, DISTRIBUTED INFORMATION SYSTEM IN WHICH USERS MAY CREATE, EDIT, OR BROWSE HYPERTEXT DOCUMENTS. A GRAPHICAL DOCUMENT PUBLISHING AND RETRIEVAL MEDIUM; A COLLECTION OF LINKED DOCUMENTS THAT RESIDE ON THE INTERNET.</p>



TERM	DEFINITION
WRITING	INFORMATION IN A RECORD THAT IS ACCESSIBLE AND USABLE FOR SUBSEQUENT REFERENCE.
X.509	THE ITU-T (INTERNATIONAL TELECOMMUNICATIONS UNION-T) STANDARD FOR DIGITAL SIGNATURE CERTIFICATES. X.509 v3 REFERS TO CERTIFICATES CONTAINING OR CAPABLE OF CONTAINING EXTENSIONS.



ANNEXURE 1 - MTNLTRUSTLINE SUBSCRIBER AGREEMENT

YOU MUST READ THIS SUBSCRIBER AGREEMENT BEFORE APPLYING FOR, ACCEPTING, OR USING A CERTIFICATE FROM MTNLTRUSTLINE. IF YOU DO NOT AGREE TO THE TERMS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE CERTIFICATE.

This Subscriber Agreement details the terms and conditions regarding your application ("Certificate Application") for a Certificate and, if MTNLTRUSTLINE accepts your Certificate Application, the terms and conditions regarding your use of the Certificate to be issued by MTNLTRUSTLINE to you as "Subscriber" of that Certificate.

This Subscriber Agreement will become effective upon your submission of the Certificate Application to MTNLTRUSTLINE or an MTNLTRUSTLINE RA. By submitting your Certificate Application you are requesting MTNLTRUSTLINE to issue a Certificate to you and are expressing your agreement to the terms of this Subscriber Agreement. MTNLTRUSTLINE certification services are governed by the MTNLTRUSTLINE Certification Practice Statement ([MTNLTRUSTLINE CPS](#)) as amended from time to time, which is incorporated by reference into this Subscriber Agreement. You agree to use the Certificate and any related CA services only in accordance with the [MTNLTRUSTLINE CPS](#). By applying for a Certificate you confirm that you have read the [MTNLTRUSTLINE Certification Practice Statement](#) and agree to all its terms.

1. DESCRIPTION OF CERTIFICATES.

A Certificate is a digitally signed message that contains a Subscriber's Public Key and associates it with information authenticated by MTNLTRUSTLINE or an MTNLTRUSTLINE RA. MTNLTRUSTLINE under this Agreement offers three distinct classes ("Classes") of Certificates, Classes 1, 2, and 3. Each class, of Certificates provides specific functionality and security features and corresponds to a specific level of trust. You are responsible for choosing which Class of Certificate you need. The following subsections state the appropriate uses and authentication procedures for each Class of Certificate. For more detailed information about MTNLTRUSTLINE's digital certificates, please see the [MTNLTRUSTLINE Certification Practice Statement](#).

1.1. CLASS 1 CERTIFICATES.

Class 1 Certificates are issued to Individuals with valid e-mail addresses.



Class 1 validation procedures are based on the assurance 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.

1.2. CLASS 2 CERTIFICATES.

Class 2 Certificates are issued to Individuals and Devices.

Class 2 validation procedures are based on the assurance that subscriber's Distinguished Name (DN) is unique and unambiguous within MTNLTRUSTLINE Repository and 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.

1.3. CLASS 3 CERTIFICATES.

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

The validation procedures for Class 3 Certificates issued to Individuals are 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.

The validation procedures for Class 3 Certificates issued to Organizations are 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.

2. CERTIFICATE APPLICATION PROCESSING.

Upon MTNLTRUSTLINE's receipt of the necessary payment and upon completion of



authentication procedures required for the Certificate you have applied for, MTNLTRUSTLINE will process your Certificate Application. MTNLTRUSTLINE will notify you whether your Certificate Application is approved or rejected. If your Certificate Application is approved, MTNLTRUSTLINE will issue you a Certificate for your use in accordance with this Subscriber Agreement. Your act of receiving a certificate from MTNLTRUSTLINE or an MTNLTRUSTLINE RA, or downloading a certificate, or installing a certificate from a message attaching it is considered your acceptance of the Certificate. After you pick up or otherwise install your Certificate, you must review the information in it before using it and promptly notify MTNLTRUSTLINE of any errors. Upon receipt of such notice, MTNLTRUSTLINE may revoke your Certificate and issue a corrected Certificate.

3. OBLIGATIONS.

3.1. MTNLTRUSTLINE OBLIGATIONS.

MTNLTRUSTLINE agrees to:

- i. Perform the specific obligations described throughout the [MTNLTRUSTLINE CPS](#).
- ii. Maintain your Certificate and associated CRL in a 'X.500' compliant directory with LDAP access.
- iii. Regularly update the 'National Repository of Digital Certificates' (NRDC) about the Issuance, Revocation, or suspension of Digital Certificates.
- iv. Not disclose information provided by you to any third party unless the disclosure is with your prior approval or is forced by a court order or other legal requirement.

3.2 YOUR OBLIGATIONS.

You, as the Subscriber of a Certificate from MTNLTRUSTLINE, agree to:

- i. Provide complete and accurate information in your Certificate Application;
- ii. Assent to this [MTNLTRUSTLINE Subscriber Agreement](#) as a necessary precondition for obtaining a Certificate from MTNLTRUSTLINE.
- iii. Perform Subscriber functions in accordance with the specific obligations appearing throughout the [MTNLTRUSTLINE CPS](#).
- iv. Use your Certificate(s) in accordance with [MTNLTRUSTLINE CPS § 1.3.4](#).
- v. Protect your Private Key(s) in accordance with [MTNLTRUSTLINE CPS §§ 6.1, 6.2, 6.4](#).
- vi. If you discover or have reasons to believe that there has been a compromise of your Private Key or the activation data protecting such Private Key, or the information within the Certificate is incorrect or has changed, then you will promptly notify the entity that approved your Certificate Application in accordance with [MTNLTRUSTLINE CPS § 4.4.1.1](#) and request Revocation of the Certificate in accordance with [MTNLTRUSTLINE CPS §§ 3.4, 4.4.3.1](#), and notify any person that may reasonably be expected by you to rely on a digital signature verifiable with reference to your Certificate.



- vii. Cease use of your Private Key(s) at the end of the key usage periods in accordance with [MTNLTRUSTLINE CPS § 6.3.2](#).

You also agree not to intentionally monitor, interfere with, or reverse engineer the technical implementation of MTNLTRUSTLINE or otherwise intentionally compromise the security of the MTNLTRUSTLINE PKI.

4. WARRANTIES.

4.1. MTNLTRUSTLINE WARRANTIES. MTNLTRUSTLINE warrants to you that:

- i. There are no material misrepresentations of fact in the Digital Certificate known to or originating from MTNLTRUSTLINE or its Sub-CAs or RAs,
- ii. 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,
- iii. Your Digital Certificate(s) meet all material requirements of the [MTNLTRUSTLINE CPS](#), and
- iv. Revocation services and use of the Repository conform to the [MTNLTRUSTLINE CPS](#) in all material aspects.

4.2. YOUR WARRANTIES. You warrant to MTNLTRUSTLINE and anyone who relies on your Certificate that:

- i. Each digital signature created using the Private Key corresponding to the Public Key listed in the Digital Certificate is your digital signature and the Digital Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- ii. You have been (since the time of its creation) and will remain the only person possessing your Private Key and no unauthorized person has had or will have access to your Private Key,
- iii. You have been (since the time of its creation) and will remain the only person possessing any challenge phrase, PIN, software, or hardware mechanism protecting your Private Key and no unauthorized person has had or will have access to the same,
- iv. All representations made by you in the Certificate Application are true,
- v. All information supplied by you and contained in the Digital Certificate is true,
- vi. The Digital Certificate is being used exclusively for authorized and legal purposes, consistent with the [MTNLTRUSTLINE CPS](#), and
- vii. You are an End User Subscriber and not a CA, and will not use the Private Key corresponding to the Public Key listed in your Digital Certificate(s) for purposes of digitally signing any Digital Certificate (or any other format of certified Public Key) or CRL, as a CA or otherwise.



5. DISCLAIMERS OF WARRANTIES.

You agree that your use of MTNLTRUSTLINE's service(s) is solely at your own risk. You agree that all such services are provided on an "as is" and as available basis, except as otherwise noted in this subscriber agreement. MTNLTRUSTLINE expressly disclaims all warranties of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and non-infringement. Other than the warranties as set forth in section 4 above, MTNLTRUSTLINE does not make any warranty that the service will meet your requirements, or that the service will be uninterrupted, timely, secure or error free; nor does MTNLTRUSTLINE make any warranty as to the results that may be obtained from the use of the service or to the accuracy or reliability of any information obtained through MTNLTRUSTLINE's service. You understand and agree that any material and/or data downloaded or otherwise obtained through the use of MTNLTRUSTLINE's services is done at your own discretion and risk. No advice or information, whether oral or written, obtained by you from MTNLTRUSTLINE or through MTNLTRUSTLINE's services shall create any warranty not expressly made herein, you may not rely on any such information or advice. MTNLTRUSTLINE is not responsible for and shall have no liability with respect to any products and/or services purchased by you from a third party.

6. INDEMNITY.

You agree to release, indemnify, defend and hold harmless MTNLTRUSTLINE and any of its contractors, agents, employees, officers, directors, shareholders, and assigns from all liabilities, claims, damages, costs and expenses, including reasonable legal fees and expenses, of third parties relating to or arising out of (i) This Subscriber Agreement or the breach of your warranties, representations and obligations under this Subscriber Agreement, (ii) Falsehood or misrepresentation of fact by you on the Certificate Application, (iii) Failure to disclose a material fact on the Certificate Application if the misrepresentation or omission was made negligently or with intent to deceive any party, (iv) Any intellectual property or other proprietary right of any person or entity, (v) your failure to protect the Private Key, or use a trustworthy system, or to take the precautions necessary to prevent the compromise, loss, disclosure, modification or unauthorized use of the Private Key under the terms of this Subscriber Agreement. When MTNLTRUSTLINE is threatened with suit or sued by a third party, MTNLTRUSTLINE may seek written assurances from you concerning your promise to indemnify MTNLTRUSTLINE, your failure to provide those assurances may be considered by MTNLTRUSTLINE to be a material breach of this Subscriber Agreement. The terms of this section will survive any termination or cancellation of this Subscriber Agreement.

7. LIMITATIONS OF LIABILITY.

This section applies to liability under contract (including breach of warranty), tort (including negligence and/or strict liability), and any other legal or equitable form of claim. If you initiate any claim, action, suit, arbitration, or other proceeding relating to services provided under this agreement, and to the extent permitted by applicable law, MTNLTRUSTLINE's total liability for damages sustained by you and any third party for any use or reliance on a specific certificate shall be limited, in the aggregate, to the amounts set forth below:



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

The liability limitations provided in this section shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. MTNLTRUSTLINE shall not be obligated to pay more than the total liability limitation for each certificate.

8. FIDUCIARY RELATIONSHIPS (NOPARTNERSHIP).

MTNLTRUSTLINE expressly disclaims any intention to create a partnership, employer/ employee relationship, joint venture, joint enterprise, or fiduciary relationship with MTNLTRUSTLINE or MTNLTRUSTLINE Enterprise RA Customer or MTNLTRUSTLINE Enterprise Sub-CA Customer on one hand and you (Subscriber) on the other hand. It is understood, acknowledged, and agreed that nothing contained in this agreement nor any acts of MTNLTRUSTLINE or any subscriber shall constitute or be deemed to constitute MTNLTRUSTLINE or MTNLTRUSTLINE Enterprise RA Customer or MTNLTRUSTLINE Enterprise Sub-CA Customer on one hand and you (Subscriber) on the other hand as partners, employer and employee, joint venturer, principal and agent, trustee and beneficiary, or as in a fiduciary relationship of any kind, in any way, or for any purpose.

9. FORCE MAJEURE.

Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the Party relying upon this Section 7 shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event a force majeure event described in this Section 7 extends for a period in excess of thirty

(30) days in aggregate, the other party may immediately terminate this Subscriber Agreement.

10. SEVERABILITY.

You agree that the terms of this Subscriber Agreement are severable. If any term or provision is declared invalid or unenforceable, in whole or in part, that term or provision will not affect the remainder of this Subscriber Agreement; this Subscriber Agreement will be deemed amended to the extent necessary to make this Subscriber Agreement enforceable, valid and, to the maximum extent possible consistent with applicable law, consistent with the original intentions of the parties; and the remaining terms and provisions will remain in full force and effect.



11. GOVERNING LAW.

The laws of India shall govern the validity of this Subscriber Agreement, the construction of its terms, and the interpretation and enforcement of the rights and duties of the parties hereto.

12. DISPUTE RESOLUTION.

To the extent permitted by law, any and all disputes, claims or controversies arising out of or in any way connected with this agreement, its negotiation, performance, breach, existence, termination or validity shall be resolved by a meeting between the parties attended by individuals with decision making authority regarding the dispute, to attempt in good faith to negotiate a resolution of the dispute. If the parties are not successful in negotiating a resolution of the dispute within 30 days after such meeting, they must submit the dispute to the controller of certifying authorities (cca). Under the IT Act 2000, the controller of certifying authorities (cca) is authorized to resolve disputes arising out of CA services.

13. NON-ASSIGNMENT.

Except as otherwise set forth herein, your rights under this Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Subscriber Agreement, whether by attachment, levy, garnishment or otherwise, renders this Subscriber Agreement voidable at MTNLTRUSTLINE's option.

14. SURVIVAL.

This Subscriber Agreement shall be applicable for as long as the Certificate remains valid and you have not breached any provision of this Subscriber Agreement. All payment obligations shall survive any termination or expiration of this agreement.

15. PRIVACY.

You agree that MTNLTRUSTLINE may place in your Certificate certain information that you provide for inclusion in your Certificate. You also agree that MTNLTRUSTLINE may publish your Certificate and information about its status in MTNLTRUSTLINE's repository of Certificate information and make this information available to other repositories.

16. MODIFICATIONS TO AGREEMENT.

Except as otherwise provided in this Subscriber Agreement, you agree, during the term of this Subscriber Agreement, that MTNLTRUSTLINE Management may (i) Revise the terms and conditions of this Subscriber Agreement; and/or (ii) Change part of the services provided under this Subscriber Agreement at any time. Any such revision or change will be binding and effective seven (07) days after posting of the revised Subscriber Agreement or change to the service(s) on MTNLTRUSTLINE's [web site](#), or upon notification to you by e-mail or postal mail. You agree to



periodically review MTNLTRUSTLINE's [web site](#), including the current version of this [Subscriber Agreement](#) available on MTNLTRUSTLINE's web site, to be aware of any such revisions. If you do not agree with any revision to the Subscriber Agreement, you may terminate this Subscriber Agreement at any time by providing notice to MTNLTRUSTLINE. Notice of your termination will be effective on receipt and processing by MTNLTRUSTLINE. Any fees paid by you if you terminate this Subscriber Agreement are nonrefundable. By continuing to use MTNLTRUSTLINE services after any revision to this Subscriber Agreement or change in service(s), you agree to abide by and be bound by any such revisions or changes.

17. NOTICES.

You will make all notices, demands or requests to MTNLTRUSTLINE with respect to this Subscriber Agreement in writing to:

MTNLTRUSTLINE Subscriber Notice
Mahanagar Telephone Nigam Limited
7th Floor, T.E. Building, 8 Bikaji Cama Place, New Delhi – 110 066
Tel: +91 11 2617 5050, Fax: +91 11 2617 8102
E-mail: notice@mtnltrustline.com



ANNEXURE 2 -MTNLTRUSTLINE RELYING PARTY AGREEMENT

YOU MUST READ THIS RELYING PARTY AGREEMENT BEFORE VALIDATING A MTNLTRUSTLINE CERTIFICATE OR ACCESSING OR USING MTNLTRUSTLINE'S DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION ("REPOSITORY") OR ANY CERTIFICATE REVOCATION LIST ISSUED BY MTNLTRUSTLINE ("MTNLTRUSTLINE CRL"). IF YOU DO NOT AGREE TO THE TERMS OF THIS RELYING PARTY AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR USE ANY MTNLTRUSTLINE CRL BECAUSE YOU ARE NOT AUTHORIZED TO USE MTNLTRUSTLINE'S REPOSITORY OR ANY MTNLTRUSTLINE CRL.

This Relying Party Agreement details the terms and conditions regarding your (Relying Party) reliance on a MTNLTRUSTLINE Certificate.

This Relying Party Agreement will become effective when you submit a query to search for a Certificate or CRL, or to verify a digital signature created with a Private Key corresponding to a Public Key contained in a MTNLTRUSTLINE Certificate, by downloading a MTNLTRUSTLINE Certificate or CRL, or when you otherwise use or rely upon any information or services provided by MTNLTRUSTLINE's Repository, MTNLTRUSTLINE's website, or any MTNLTRUSTLINE CRL. By submitting your query to search for a Certificate or CRL, or by verifying a digital signature created with a Private Key corresponding to a Public Key contained in a MTNLTRUSTLINE Certificate, or by downloading a MTNLTRUSTLINE Certificate or CRL, or when you otherwise use or rely upon any information or services provided by MTNLTRUSTLINE's Repository, MTNLTRUSTLINE's website, or any MTNLTRUSTLINE CRL, you and are expressing your agreement to the terms of this Relying Party Agreement. Reliance on MTNLTRUSTLINE certification services is governed by the MTNLTRUSTLINE Certification Practice Statement ([MTNLTRUSTLINE CPS](#)) as amended from time to time, which is incorporated by reference into this Relying Party Agreement.

You acknowledge and agree that you have access to sufficient information to ensure that you can make an informed decision as to the extent to which you will choose to rely on the information in a Certificate. You acknowledge and agree that your use of the Repository and your use of any



MTNLTRUSTLINE CRL is governed by this Agreement and the [MTNLTRUSTLINE CPS](#). (For more educational material, see the tutorial contained in MTNLTRUSTLINE's Repository at [MTNLTRUSTLINE https://www.mtnltrustline.com/repository/](https://www.mtnltrustline.com/repository/)). YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON THE INFORMATION IN A CERTIFICATE. You also acknowledge and agree that you shall bear the legal consequences of your failure to comply with the Relying Party obligations set forth in this Agreement.

1. DESCRIPTION OF CERTIFICATES.

A Certificate is a digitally signed message that contains a Subscriber's Public Key and associates it with information authenticated by MTNLTRUSTLINE or an MTNLTRUSTLINE RA. MTNLTRUSTLINE under this Agreement offers three distinct classes ("Classes") of Certificates, Classes 1, 2, and 3. Each class, of Certificates provides specific functionality and security features and corresponds to a specific level of trust. You are responsible for choosing which Class of Certificate you need. The following subsections state the appropriate uses and authentication procedures for each Class of Certificate. For more detailed information about MTNLTRUSTLINE's digital certificates, please see the [MTNLTRUSTLINE Certification Practice Statement](#).

1.1. CLASS 1 CERTIFICATES.

Class 1 Certificates are issued to Individuals with valid e-mail addresses.

Class 1 validation procedures are based on the assurance 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.

1.2. CLASS 2 CERTIFICATES.

Class 2 Certificates are issued to Individuals and Devices.

Class 2 validation procedures are based on the assurance that subscriber's Distinguished Name (DN) is unique and unambiguous within MTNLTRUSTLINE Repository and 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.



1.3. CLASS 3 CERTIFICATES.

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

The validation procedures for Class 3 Certificates issued to Individuals are 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.

The validation procedures for Class 3 Certificates issued to Organizations are 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.

2. YOUR OBLIGATIONS. As a Relying Party, you are obligated to:

- i. 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, its Sub-CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate.
- ii. Not to use Certificates beyond the limitations in [MTNLTRUSTLINE CPS § 1.3.4.2](#) and for purposes prohibited in [MTNLTRUSTLINE CPS § 1.3.4.3](#).
- iii. Utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations you 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. You agree that you will not rely on a Certificate unless these verification procedures are successful.
- iv. Check the status of a Certificate on which you wish to rely, as well as all the Certificates in its Certificate Chain in accordance with [MTNLTRUSTLINE CPS §§ 4.4.10, 4.4.12](#). If any of the Certificates in the Certificate Chain have been revoked, then you agree that you will not rely on the Subscriber Certificate or other revoked Certificate in the Certificate Chain.
- v. Rely on the Certificate only if all of the checks described above are successful, provided that reliance upon the Certificate is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, you agree that it is your responsibility to obtain such assurances for such reliance to be deemed reasonable.

You also agree not to intentionally monitor, interfere with, or reverse engineer the technical implementation of MTNLTRUSTLINE or otherwise intentionally compromise the security of the MTNLTRUSTLINE PKI.



3. LIMITATIONS ON USE.

MTNLTRUSTLINE 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 [MTNLTRUSTLINE CPS § 1.3.4.1.1](#), Class 1 Certificates shall not be used as proof of identity or for non repudiation.

4. MTNLTRUSTLINE WARRANTIES.

MTNLTRUSTLINE warrants to Relying Parties who reasonably rely on a MTNLTRUSTLINE Certificate that:

- i. There are no material misrepresentations of fact in the Digital Certificate known to or originating from MTNLTRUSTLINE or its Sub-CAs or RAs,
- ii. 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,
- iii. The Digital Certificate meets all material requirements of the [MTNLTRUSTLINE CPS](#),
- iv. Revocation services and use of the Repository conform to the [MTNLTRUSTLINE CPS](#) in all material aspects.
- v. All information in or incorporated by reference in such Certificate is accurate,
- vi. Certificates appearing in the MTNLTRUSTLINE Repository, have been issued to the individual or organization named in the Certificate as the Subscriber, and the Subscriber has accepted the Certificate in accordance With [MTNLTRUSTLINE CPS § 4.3](#), and
- vii. MTNLTRUSTLINE has complied with this CPS when issuing the Certificate.

5. DISCLAIMERS OF WARRANTIES.

You agree that your use of MTNLTRUSTLINE's service(s) is solely at your own risk. You agree that all such services are provided on an "as is" and as available basis, except as otherwise noted in this Relying Party Agreement. MTNLTRUSTLINE expressly disclaims all warranties of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose and non-infringement. Other than the warranties as set forth in section 4 above, MTNLTRUSTLINE does not make any warranty that the service will meet your requirements, or that the service will be uninterrupted, timely, secure or error free; nor does MTNLTRUSTLINE make any warranty as to the results that may be obtained from the use of the service or to the accuracy or reliability of any information obtained through MTNLTRUSTLINE's service. You understand and agree that any material and/or data downloaded or otherwise obtained through the use of MTNLTRUSTLINE's services is done at your own discretion and risk. No advice or information, whether oral or written, obtained by you from MTNLTRUSTLINE or through MTNLTRUSTLINE's services shall create any warranty not expressly made herein, you may not rely on any such information or advice. MTNLTRUSTLINE



is not responsible for and shall have no liability with respect to any products and/or services purchased by you from a third party.

YOU ARE HEREBY NOTIFIED OF THE POSSIBILITY OF THEFT OR OTHER FORM OF COMPROMISE OF A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A CERTIFICATE, WHICH MAY OR MAY NOT BE DETECTED, AND OF THE POSSIBILITY OF USE OF A STOLEN OR COMPROMISED KEY TO FORGE A DIGITAL SIGNATURE TO A DOCUMENT.

6. INDEMNITY.

You agree to release, indemnify, defend and hold harmless MTNLTRUSTLINE and any of its contractors, agents, employees, officers, directors, shareholders, and assigns from all liabilities, claims, damages, costs and expenses, including reasonable legal fees and expenses, of third parties relating to or arising out of (i) your failure to perform the obligations of a Relying Party, (ii) your reliance on a Certificate that is not reasonable under the circumstances, or (iii) your failure to check the status of such Certificate to determine if the Certificate is expired or revoked. When MTNLTRUSTLINE is threatened with suit or sued by a third party, MTNLTRUSTLINE may seek written assurances from you concerning your promise to indemnify MTNLTRUSTLINE, your failure to provide those assurances may be considered by MTNLTRUSTLINE to be a material breach of this Relying Party Agreement. The terms of this section will survive any termination or cancellation of this Relying Party Agreement.

7. LIMITATIONS OF LIABILITY.

This section applies to liability under contract (including breach of warranty), tort (including negligence and/or strict liability), and any other legal or equitable form of claim. If you initiate any claim, action, suit, arbitration, or other proceeding relating to services provided under this agreement, and to the extent permitted by applicable law, MTNLTRUSTLINE's total liability for damages sustained by you and any third party for any use or reliance on a specific certificate shall be limited, in the aggregate, to the amounts set forth below:

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

The liability limitations provided in this section shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. MTNLTRUSTLINE shall not be obligated to pay more than the total liability limitation for each certificate.



8. FIDUCIARY RELATIONSHIPS (NOPARTNERSHIP).

MTNLTRUSTLINE expressly disclaims any intention to create a partnership, employer/ employee relationship, joint venture, joint enterprise, or fiduciary relationship with MTNLTRUSTLINE or MTNLTRUSTLINE Enterprise RA Customer or MTNLTRUSTLINE Enterprise Sub-CA Customer on one hand and you (Subscriber) on the other hand. It is understood, acknowledged, and agreed that nothing contained in this agreement nor any acts of MTNLTRUSTLINE or any subscriber shall constitute or be deemed to constitute MTNLTRUSTLINE or MTNLTRUSTLINE Enterprise RA Customer or MTNLTRUSTLINE Enterprise Sub-CA Customer on one hand and you (Subscriber) on the other hand as partners, employer and employee, joint venturer, principal and agent, trustee and beneficiary, or as in a fiduciary relationship of any kind, in any way, or for any purpose.

9. FORCE MAJEURE.

Except for payment and indemnity obligations hereunder, neither party shall be deemed in default hereunder, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligations hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the Party relying upon this Section 7 shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and (ii) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event a force majeure event described in this Section 7 extends for a period in excess of thirty (30) days in aggregate, the other party may immediately terminate this Relying Party Agreement.

10. SEVERABILITY.

You agree that the terms of this Relying Party Agreement are severable. If any term or provision is declared invalid or unenforceable, in whole or in part, that term or provision will not affect the remainder of this Relying Party Agreement; this Relying Party Agreement will be deemed amended to the extent necessary to make this Relying Party Agreement enforceable, valid and, to the maximum extent possible consistent with applicable law, consistent with the original intentions of the parties; and the remaining terms and provisions will remain in full force and effect.

11. GOVERNING LAW.

You and MTNLTRUSTLINE agree that the information technology act 2000, information technology (certifying authorities) rules 2000 and information technology (certifying authority) regulations 2001, and any subsequent updates shall govern all services provided under this agreement.

12. DISPUTE RESOLUTION.

To the extent permitted by law, any and all disputes, claims or controversies arising out of or in



any way connected with this agreement, its negotiation, performance, breach, existence, termination or validity shall be resolved by a meeting between the parties attended by individuals with decision making authority regarding the dispute, to attempt in good faith to negotiate a resolution of the dispute. If the parties are not successful in negotiating a resolution of the dispute within 30 days after such meeting, they must submit the dispute to the controller of certifying authorities (cca). Under the IT Act 2000, the controller of certifying authorities (cca) is authorized to resolve disputes arising out of CA services.

13. NON-ASSIGNMENT.

Except as otherwise set forth herein, your rights under this Agreement are not assignable or transferable. Any attempt by your creditors to obtain an interest in your rights under this Relying Party Agreement, whether by attachment, levy, garnishment or otherwise, renders this Relying Party Agreement voidable at MTNLTRUSTLINE's option.

14. SURVIVAL.

This Relying Party Agreement shall be applicable for as long as the Certificate remains valid and you have not breached any provision of this Relying Party Agreement. All payment obligations shall survive any termination or expiration of this agreement.

15. PRIVACY.

You agree that MTNLTRUSTLINE may place in your Certificate certain information that you provide for inclusion in your Certificate. You also agree that MTNLTRUSTLINE may publish your Certificate and information about its status in MTNLTRUSTLINE's repository of Certificate information and make this information available to other repositories.

16. MODIFICATIONS TO AGREEMENT.

Except as otherwise provided in this Relying Party Agreement, you agree, during the term of this Relying Party Agreement, that MTNLTRUSTLINE Management may (i) Revise the terms and conditions of this Relying Party Agreement; and/or (ii) Change part of the services provided under this Relying Party Agreement at any time. Any such revision or change will be binding and effective seven (07) days after posting of the revised Relying Party Agreement or change to the service(s) on MTNLTRUSTLINE's [web site](#), or upon notification to you by e-mail or postal mail. You agree to periodically review MTNLTRUSTLINE's [web site](#), including the current version of this [Relying Party Agreement](#) available on MTNLTRUSTLINE's web site, to be aware of any such revisions. If you do not agree with any revision to the Relying Party Agreement, you may terminate this Relying Party Agreement at any time by providing notice to MTNLTRUSTLINE. Notice of your termination will be effective on receipt and processing by MTNLTRUSTLINE. Any fees paid by you if you terminate this Relying Party Agreement are nonrefundable. By continuing to use MTNLTRUSTLINE services after any revision to this Relying Party Agreement or change in service(s), you agree to abide by and be bound by any such revisions or changes.



17. NOTICES.

You will make all notices, demands or requests to MTNLTRUSTLINE with respect to this Relying Party Agreement in writing to:

MTNLTRUSTLINE Relying Party Notice

Mahanagar Telephone Nigam Limited

7th Floor, T.E. Building, 8 Bikaji Cama Place, New Delhi – 110 066

Tel: +91 11 2617 5050, Fax: +91 11 2617 8102

E-mail: notice@mtnltrustline.com