Mango Teleservices Limited

MANGO CA – CPS

Document Version. 2.131114

Author:
Hasan T. Emdad Rumi, Head of CA & Managed Services, Mango Teleservices Limited

Mango Teleservices Limited Certifying Authority

Date:
14-November-2013

Mango Certifying Authority
CPS (Certification Practice Statement)

Table of Contents

Executive Summary

This document - "MANGO CA – CPS" (henceforth referred as 'this document' or 'this CPS' or 'MANGO CPS' or 'MANGO CA CPS' interchangeably) represents the manner in which MANGO Teleservices Limited will operate its licensed certification authority business ("MANGO CA" or 'MANGO') in the provision of digital certificates (the "MANGO CA Service").

The implementation of a Public Key Infrastructure (PKI) is a complex undertaking involving tight and stringent business process and IT controls, which this document details.

This document contains the ways in which MANGO CA will create a registration authority, accept registrations, verify details, issue digital certificates and manage digital certificates as part of providing PKI solutions to its customers. It also outlines the roles and responsibilities of all parties involved in generating and using digital certificates.

This document covers the following **operational aspects** of the MANGO CA Service:

- The operation of all Certificate Authority (CA) services.
- The operation of all Registration Authority (RA) services.
- The operation of all Registration Authority Operators (RAO) services.
- Customer agreements.
- MANGO CA certificate policies.
- MANGO CA certificate applications.

In addition, this CPS indicates the type of applications that the issued digital certificates may be used for. The types of applications include, but are not limited to, email; transmission of documents; signature of electronic forms; and authentication of network components such as Web servers and firewalls.

1. Introduction

This CPS is the Certification Practice Statement under which MANGO CA operates. This CPS covers the practices and procedures employed by **MANGO CA** to operate the **MANGO CA Service**. Information contained within this document is based on the various certificate policies and certification practices that have been adopted by MANGO CA and how digital certificates are to be issued to the end user following Information Technology Act 2006 and Information Technology (Certificate Authority) Rules 2010 and the licensing guidelines for Certifying Authorities issued under the Act. This document also sets out details of the security procedures that have been put into place for subscribers, relying parties and the system architecture. Please refer to the table of contents to view the precise contents of this document.

The **services** that are offered by the MANGO CA Services include;

- Handling Certificate Request
- Identification and authentication of individuals/organizations and servers
- Certificate holder key pair generation (if by MANGO)
- Certificate generation
- Certificate signing
- Certificate issuance and publication
- Certificate revocation LDAP directory service (Certificate Revocation List (CRL) Management)
- Certificate Suspension
- Certificate Activation - in case of suspended certificates
- Bespoke software development

1.1 Overview

This document is based on the structure as outlined in [RFC 3647]. The section numbering and titles follow the [RFC 3647] recommendations.

None of the sections stipulated by RFC 3647 have been omitted; however, some sections of this document may state "**no stipulation**" when the Certification Practice Statement (CPS) imposes no requirements or makes no disclosure. Additionally, some sections may state "**not applicable**" if the particular topic addressed by that section does not apply.

The entire content of RFC 3647 is available at the following sources (in different formats):

- Plain text: http://www.ietf.org/rfc/rfc3647.txt or
  http://www.faqs.org/rfcs/rfc3647.html
- HTML: http://www.faqs.org/rfcs/rfc3647.html

- Text PDF: http://www.faqs.org/ftp/rfc/pdf/rfc3647.txt.pdf

In some of the sections, this document provides instructions from RFC 3647. However, if the instructions are too long, they are not provided in this document and can be referenced at one of the links above.

MANGO CPS is applicable to digital certificates issued by MANGO binding the identity of individuals and organizations to a public key for digital signature and non-repudiation**.**

The purpose of this document is to describe the procedures employed by MANGO CA to undertake the MANGO CA Services and to provide evidence of the methods used to manage tasks associated with authentication and digital certificate generation.

Certificate holders can consult MANGO CPS to obtain details of precisely how the certificate policies are implemented by the MANGO CA for any particular digital certificate.

1.1.1 Certificate Policy

The term Certificate Policy (CP) is defined by the X.509 standard as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."

1.1.2 References

Table 1 provides a list of references for documents that are related to this document.

References for Related Documents	
Document ID	**Document Name and URL**
RFC 3647	Internet Engineering Task Force (IETF) Request for Comments 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," November 2003

Table 1: References for Related Documents

1.2 Document Name and Identification

Name of this document: "Mango Certificate Authority Certification Practice Statement."

CPS Version. 2.131114

Mango CA OID (Allocation made by Office of the Controller of Certifying Authority)– 2.16.50.1.8 (mango-certifying-authority) Ref: CCA- 56.03.0000.003.22.039.12-1126 Dated: 12/11/2013

CPS OID- 2.16.50.1.8.1

1.3 PKI Participants

The subsections below describe the types of entities that fill the roles of participants.

Within the MANGO CA hierarchy there is one Root CA entity that represents the source of all trust within the MANGO PKI. The parties involved in MANGO CA PKI are:

- MANGO CA that issue certificates.
- Entities that function as RAs.

- Entities that are certified as applicants or subscribers.
- Entities that rely on the certificates (relying party).

Digital certificates are issued on both an individual and an organizational basis.

The function of MANGO Certificate Practice Statement (CPS) is to present reliable information to subscribers and to the relying parties. MANGO CA will issue, administer and revoke Class 1, 2 and 3 digital certificates which are trustworthy and lawfully valid under Information and Communication Technology Act, 2006. The use of certificates will be confined with the usage scheme prescribed in consultation with the Controller of Certifying Authorities (CCA). Any other type of usage of certificates which are not mentioned is explicitly prohibited.

The suitable applications are as follows: secure electronic mail (s/mime), file and form signing, client authentication, retail transactions (banking applications), VPN & IPSEC applications, secure SSL/TLS applications, contracts signing applications, custom e-Commerce applications, code signing, time signing etc. MANGO digital certificates comply with the latest in Internet Standards (X509 V3) as set out in RFC 2459.

More generally, certificates shall be used only to the extent such use is consistent with all applicable laws, rules and regulations and in particular shall be used only to the extent permitted by applicable export or import laws.

1.3.1 Certification Authorities

Mango Teleservices Limited founded the Mango Certificate Authority (CA) and created the CA root certificate, certitied by the CCA's root certificate. It currently operates at the direction of the Board of Directors.

A single root CA – the Mango CA – is used for issuing Certificates to authenticated and authorised end-entities.

The Mango CA issues Certificates that MAY be compliant with one or more Trust Providers.

1.3.2 Registration Authorities

"Registration Authority (RA)" is an entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

Since Mango CA shall issue Digital Certificates to new entities or subscribers in demographically dispersed areas, multiple Registration Authorities (RAs) are set up to process and approve Certificate Applications and Certificate revocation requests. Initially a primary RA is installed which will be used to set up secondary RAs that will handle Applications and Requests of specific sub-groups or constituency.

1.3.3 Subscribers

Subscribers are all Requesters of a Certificate that have successfully obtained a Certificate issued by the Mango CA.

Different types of Certificates MUST be requested by different entities: MANGO CA provides identification and authentication services for certificate holders, servers, and PC or network devices. The registration procedures set out in this document and in **Appendix A** define the credentials necessary to establish the identity of an individual or entity. For Class 3 Certificates, all identification processes for individuals require applicants to present themselves for physical verification.

Table below shows Requester by Type of Certificate:

Type of Certificate	Requester
Network Entity Certificate (Organisational Certificate)	administrators and owners of the network entity named in the Certificate's Subject (Organisational Requester)
Personal User Certificate (Personal Certificate)	the person named in the Certificate's Subject (Personal Requester)
Group Certificate (Organisational Certificate)	responsible member of the group named in the Certificate's Subject or their superior staff (Organisational Requester)

1.3.4 Relying Parties

Relying Parties are individuals or organisations using the Certificates issued by the Mango CA to verify the identity of and/or secure electronic communication with Subscribers.

Relying Parties MAY or MAY not be Subscribers of the Mango CA.

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

The use of certificates is confined with the usage scheme prescribed in consultation with the Controller of Certifying Authorities (CCA). Any further update in the usage scheme will be consulted with CCA.

1.4.1 Appropriate Certificate Uses

The Controller of Certifying Authorities (CCA) has currently suggested four classes as the following:

Class 0 Certificate: This certificate shall be issued only for demonstration/ test purposes.

Class 1 Certificate: These certificates shall be issued to individual subscribers only. It will authenticate an email address to its associated name or alias within the CA database. Can be used only with digitally signed email application. The verification of the certificate request of this class represent a simple check of the certainty of the subject name within the MANGO CA repository, plus a limited verification of the address, other personal information and e-mail address. Class 1 certificates are appropriate for digital signatures and encryption where assurance level is low.

Class 2 Certificate: These certificates are issued to individual or enterprise subscribers (sub class) Usage It will authenticate an email address or other digitally signed files & forms to its signature provider's associated name within the CA database. Can be used for digitally signed email application, file or form signing, client and/or server authentication, secure email, transactions or other applications.MANGO CA has the right to reject the certificate request if it finds the application is not meeting the criteria. Physical presence Physical presence may or may not be required, Mango CA would decide on case to case. Class 2 certificates are appropriate for digital signatures and encryption where assurance level is medium.

Class 3 Certificate: These Certificates are issued to Individuals Enterprises and Servers (sub class) Usage Can be used for email, files, forms signing, VPN, Client Authentication, Server side signing or other application, SSL server authentication or similar services & applications or for Code Signing or Time Stamping for various applications. Physical presence Physical presence may or may not be required, Mango CA would decide on case to case basis. In case of server sub class, along with the application form the authorized person must give the domain name or the Server IP address on which it needs the Certificate. The domain name must be registered and the proof must also be accompanied

with the application. Class 3 certificates are appropriate for digital signatures and encryption requiring a high assurance about the subscriber's identity.

In particular, it is prohibited to generate subscriber certificates from the CA certificate.

1.5 Policy Administration

This section includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this document. It also includes the name, electronic mail address, telephone number, and fax number of a contact person.

1.5.1 Organization Administering the Document

The authority responsible for the registration, maintenance, and interpretation of this document is MANGO's CA Committee**.** In the event that individuals have any queries regarding any aspect of the MANGO CA Service, the following email address and telephone number is to be used to submit those:

Organization Name: Mango Teleservice Limited (Certificate Authority Administrator)

Email Address: contact@mango.com.bd

Telephone: +880 2 8814507, 9895712

Fax: +880 2 8814537

Address: 82, Mohakhali Commercial Area, (12th floor), Dhaka, 1212, Bangladesh

1.5.2 Contact Person

The persons responsible for this CPS are the members of the Mango CA task within Mango Teleservices Limited.

Point of Contact: Hasan T. Emdad, Head of Technical Solution

Email Address: hasan.emdad@mango.com.bd

Telephone: +880 2 8814507, 9895712

Fax: +880 2 8814537

Address: 82, Mohakhali Commercial Area, (12th floor), Dhaka, 1212, Bangladesh

1.5.3 Person Determining CPS Suitability for the Policy

The following bodies will verify MANGO CPS suitability for the policy and must sanction MANGO CPS for use within MANGO CA.

- MANGO CA Policy Approval Committee
- MANGO CA Legal Department

However, the final approval to the CPS will be made by the Controller of Certifying Authorities Bangladesh, Ministry of Information and Communication Technology, Government of the People's Republic of Bangladesh.

1.5.4 CPS Approval Procedures

Approval of the CPS is effected by the responsible persons named in section 1.5.2.

The review and approval process MUST assure that this CPS adheres to:

RFC 3647

1.6 Definitions and Acronyms

"**Act**" means the Information Technology and Communication Act, 2006

"**Access**" means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network

"**Affixing Digital Signature**" means adoption of any methodology or procedure by an individual for the purpose of authenticating an electronic record by means of Digital Signature

"**Auditor**" means any globally recognized computer security professional or agency appointed by the Certifying Authority and recognized by the Controller of Certifying Authorities for conducting technical audit of operation of Certifying Authority

"CA" refers to the Certifying Authority licensed by the Controller of Certifying Authorities

"Certification" The process of creating a public key certificate for an entity binding the entity's identity to its public key.

"Certification Authority (CA)" An entity trusted by one or more entities to create, assign or revoke public key certificates.

"Certification Practice Statement (CPS)" A statement of the practices, which a certification authority employs in issuing certificates.

"**Controller**" means Controller of Certifying Authorities

"**Compromise**" means a infringement (or suspected infringement) of a security policy, in which an unauthorized revelation of or loss of control over sensitive information may have occurred

"**Computer**" means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network

"**Computer resource**" means computer, computer system, computer network, data, computer data base or software

"**CPS**" means the MANGO CA Certification Practice Statement

"**CSP**" means the MANGO CA Certification Status Provider, example: OCSP

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

"**Digital Signature**" means authentication of any electronic record by a Subscriber by means of an electronic method or procedure

"**Digital Certificate**" means Digital Certificate issued by MANGO Certifying Authority

"**End Entity**" or "Entity" refers to either applicant or subscriber of Digital Certificate issued by MANGO CA

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

"**Key Pair**" is 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

"**License**" means a license granted to Certifying Authorities for the issue of Digital Certificates under the Information and Communication Technology Act,2006

"**Licensed** CA" refers to a Certifying Authority who has been granted a license by Controller of Certifying Authorities to issue Digital Certificates

"**Private Key**" means the key of a key pair used to create a Digital Signature

"**Public Key**" means the key of a key pair used to verify a Digital Signature and listed in the Digital Certificate

"**Person**" shall include an individual or a company or association or body of individuals, whether incorporated or not

"Relying Party" A recipient who acts in reliance on a certificate and digital signature.

"Registration Authority (RA)" An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

"Subscriber" An applicant for and/or a holder of a MANGO digital certificate, including without limitation, organizations, individuals and/or hardware and/or software devices.

"**Subscriber identity verification method**" means the method used to verify and authenticate the identity of a Subscriber

"**Suspect of compromise**" means any compromise of the digital certificate or private key of a user reported explicitly to the MANGO CA within a reasonable period of time.

"**Trusted person**" means any person who has: direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the ICT Act 2006or IT(CA) Rules 2006 in respect of a Certifying Authority or duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificate (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of a Certifying Authority's computing facilities

"**Unverified information**" means any information in a digital certificate which is not expressly/explicitly verified by MANGO CA as per the MANGO CA CPS, CA's Master Agreement.

"**Verify**" in relation to a Digital Signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether: The initial electronic record was affixed with the Digital Signature by the use of private key corresponding to the public key of the Subscriber and/or the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the Digital Signature.

Note: Words and expressions used herein and not defined shall have the meaning respectively assigned to them in the context.

Acronym	Meaning
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Status Provider
CSR	Certificate Signing Request
DN	Distinguished Name
FIPS	Federal Information Processing Standard
LDAP	Lightweight Directory Access Protocol
PIN	Personal Identification Number
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
RAA	Registration Authority Administrator
RAO	Registration Authority Operator

2. Publication and Repository Responsibilities

The MANGO CA repository is a collection of databases for storing and retrieving certificates and other information related to certificates. The MANGO CA repository's content includes: certificates, CRL, current and prior versions of the MANGO CA CPS, and other information as prescribed by MANGO CA from time to time.

MANGO will host a repository in the form of an LDAP directory for the purpose of

- Storing and making available all X.509 v 3 certificates issued under the MANGO CA, facilitating public access to download these digital certificates for subscriber and relying party requirements.
- Receiving (from the MANGO CA), storing and making publicly available regularly updated CRL v.2 information, for the purpose of digital certificate validation.

2.1 Repositories

Mango CA publishes this CPS, certificate terms and conditions, the relying party agreement and the subscriber agreement in the official Mango CA repository at http://www.mangoca.com/repository/ Any revocation data on issued digital certificates is published at location of the CRL distribution point or OCSP responder specified in the certificate.

LDAP Directory: All digital certificate information shall be published to the dedicated MANGO LDAP directory server. Each time the MANGO CA issues a digital certificate a copy of this digital certificate will automatically be published to the directory server via the LDAP v3 protocol. The directory server is publicly available in the MANGO repository.

2.2 Publication of Certification Information

Any changes that shall be made to MANGO CPS such as practices for certificate registration process, the version of digital certificates that are issued shall be published within reasonable time frame possible.

Upon the subscriber's acceptance of the certificate, the MANGO CA shall publish a copy of the certificates in the MANGO CA repository and/or in one or more other repositories, as determined by the MANGO CA. It will also publish MANGO CA's Public Key Certificate and the Certification Practice Statement (CPS).

The Certificate Revocation List that comprises of the revoked certificates will also be published. Mango CA publishes CRLs to allow relying parties to determine the validity of a certificate issued by Mango CA. Each CRL contains entries for all revoked un-expired certificates issued and is valid for a period from 24 hours up to 7 days.

Mango CA certificate services and the repository are accessible through several means of communication:

- On the web: www.mangoca.com
- By email to contact@mangoca.com
- By mail addressed to: Mango Teleservices Limited (Certifying Authority), 82, Mohakhali C/A, 12th Floor, Dhaka, 1212, Bangladesh
- By telephone : **+880 2 8814507, 9895712**
- **By Fax: +880 2 8814537**

2.2.1 Time or Frequency of Publication

Publication of the MAN**GO Certificate Revocation List will** be configured to be issued once a day. In addition to this configuration, the CA will automatically publish a CRL to the dedicated directory every time a digital certificate has been revoked. This measure ensures that the directory makes available CRLs that include all revoked digital certificates under the MANGO CA at any given time.

2.3 Access Controls on Repositories

Information published in the MANGO CA repository is publicly-accessible information.

Public access to CA published information objects such as certificate policy definitions, MANGO CPS, issued digital certificates and digital certificate status shall be unrestricted. All information relating to issued digital certificates and digital certificate status will be published to the dedicated MANGO directory server.

The right to make modification in MANGO CPS rests with MANGO CA.

Parties (including Subscribers and Relying Parties) accessing the Mango CA Repository and other Mango CA publication resources (CRLs and OCSP) are deemed to have agreed with the provisions of this CPS and any other conditions of usage that Mango CA may make available.

3. Identification and Authentication

This section serves as an overview of the requirements to be followed in identifying and authenticating individuals and organizations requesting certification under the MANGO CA. As the MANGO CA will be involved in certifying a variety of certificate types, the identification and authentication process may vary in each particular case. Therefore refer to Appendix A for a detailed description of the identification and authentication procedure for each certificate type.

3.1 Naming

3.1.1 Types of Names

The naming convention used by MANGO to identify certificate holders uniquely is ISO/IEC 9594 (X.500) Distinguished Name (DN).

The MANGO X500 Distinguished Name will comprise of a number of the following components:

Dname Attributes	Example
Common Name (CN=)	• **Individual Digital Certificate:** The digital certificate holders given name • **Role based Digital Certificate:** The digital certificate holders organizational role (e.g. general manager) • **Server Digital Certificate:** The DNS server name () • **Company Digital Certificate:** The organization name
Organization (O=)	Registered business name of organization instead Common Name will be used
Country (C=)	BD (Bangladesh)
Organization Unit (OU=)	• Internal organization department (e.g. Sales and Marketing) • Job description • Certificate description
Locality (L=)	Town/ City of certificate holder or organization
State or Province (SP=)	Not Applicable.
Email(E=)	Email address of the certificate holder
Phone Number(Phone=)	Contact number of the certificate holder

Non-wildcard SSL Certificates and Unified Communications Certificates are issued using the Fully Qualified Domain Name (FQDN) name or IP address of the servers, services or applications that have been confirmed with the Subscriber.

On the listed table CN, O, OU, C, L, are mandatory Dname parameters.

3.1.2 Need for Names to Be Meaningful

All subject names must be meaningful. The names provided on the digital certificate must be as accurate as possible when describing the person or organization or role within the organization. Digital certificates will not be issued for names that are not to be deemed meaningful by MANGO.

The Subject and Issuer names contained in a certificate MUST be meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.

- For personal certificates, the CN DN attribute contains the legal name as presented in a government issued photo-identification.

- For server certificates, the CN DN attribute contains the fully qualified domain name of the server.

Mango CA ensures that the Organization (O) and Organizational Unit (OU) attributes in the Subject field accurately identify the legal entity that is the subject of the certificate. Similarly, Mango CA uses nonambiguous designations in the Issuer field to identify itself as the Issuer of a certificate (e.g., Mango Certificate Authority).

3.1.3 Anonymity or Pseudonymity of Subscribers

Mango CA does not issue anonymous or pseudonymous or intermediate or temporary certificates.

3.1.4 Rules for Interpreting Various Name Forms

The names shall be interpreted as specified in the CPS. Other terms, numbers, characters and letters may be appended to existing names to ensure the uniqueness of each name.

3.1.5 Uniqueness of Names

The Distinguished names form the basis for the uniqueness of each assigned name but the same Applicant/Subscriber can have multiple Digital Signature Certificates with the same DNs for different Digital Signature Certificate purposes as specified in the CPS.

The distinguished names should be able to uniquely identify the Subscriber in public Repository in which it is published. Additionally all the Digital Signature Certificates shall be assigned a unique serial number, which will enable identification, suspension, activation and revocation of the Digital Signature Certificates when required.

All names must be unique within the MANGO domain. Each digital certificate request must contain a unique set of Dname attributes. These attributes include a collection of the persons/companies name, organization unit, common name, and postal address. Any digital certificate requests which are not unique will be automatically rejected by the MANGO CA. Subscribers who have been rejected by the CA on the grounds that their name is not unique will be notified as promptly as is operationally possible.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers represent and warrant that all information supplied in the digital certificate application process is accurate and does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other Intellectual Property Rights of any third party. Subscribers also warrant that any material they supply or transmit is not libelous and does not constitute malicious falsehood or disparagement of goods or services, is not otherwise defamatory, is not immoral, obscene, pornographic, is not illegal and does not advocate illegal activity, does not constitute a violation of privacy and does not infringe any Intellectual Property Rights of MANGO or a third party.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The applicant must submit a digitally signed PKCS#10 CSR while the certificate is generated to establish that it holds the private key corresponding to the public key to be included in a certificate. Mango CA parses the PKCS#10 CSR submitted by the Applicant in a secure manner and verifies that the Applicant's digital signature on the PKCS#10 was created by the private key corresponding to the public key in the PKCS#10 CSR.

This is not applicable for applicant requested personal information exchange format certificate.

3.2.2 Authentication of Organization Identity

MANGO CA needs to verify that an entity belongs to the set of entities that the MANGO CA recognizes as qualified to become an end user. A representative of an organization should come with a letter authorizing him/her to represent the organization for the given purpose.

As the authentication process is dependent on the class of digital certificate being issued, this procedure will differ accordingly. Please refer to **Appendix A** for a detailed account of the various authentication processes MANGO will carry out.

3.2.3 Authentication of Individual Identity

The authentication process may include a face to face identity verification process, prior to key material or digital certificate distribution.

Acceptable documentation for face-to-face identity verification shall at least include the following pieces of information:

- Individual's name,
- Individual's photograph,
- Individual's signature,
- Individual's postal address supporting document such as copies of phone bill or utility bill,
- Individual's National Identity (NID) or passport.
- Additional supporting document as may required by Mango CA cerifying officer.

3.2.4 Nonverified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organizational affiliation shall be issued only after ascertaining the applicant has the authorization to act on behalf of the organization in the asserted capacity.

For certificates issued at the request of a Subscriber's agent, both the agent and the Subscriber shall jointly and severally indemnify and hold harmless Mango CA, and its parent companies, subsidiaries, directors, officers, employees, agents, and contractors. The Subscriber shall control and be responsible for the data that an agent of the Subscriber supplies to Mango CA. The Subscriber must promptly notify Mango CA of any misrepresentations and omissions made by an agent of the Subscriber. The duty of this article is continuous.

3.2.6 Criteria for Interoperation

Certificates shall be issued in accordance with CCA interoperability guidelines.

3.3 Identification and Authentication for Rekey Requests

The validity period associated with a digital certificate will be dependent on the digital certificate class in question. The MANGO CA will provide a facility to reissue digital certificates that are just about to expire. The frequency at which digital certificates are reissued/rolled over is dependent on the class of digital certificates in question.

MANGO CA Certification Services support Certificate renewal in the mode of rekey. Subscribers may request Certificate renewal provided that:

- Content of Certificate information as contained in the registration records has not been changed.
- The request is made before the expiry of their current certificates.
- Their current certificates have not been revoked.
- They are not listed in the compromised user.
- Their keys are not included as the compromised keys.

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. MANGO CA requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

3.3.1 Identification and Authentication for Routine Rekey

At any time prior to certificate expiration, a Subscriber may perform routine re-key by logging into the Subscriber's customer account using his or her username and password. Through routine re-key, a new certificate is created with the same certificate contents except for a new Public Key and, optionally, a new, extended validity period. Re-keying is allowed in accordance with Section 4.7.

3.3.2 Identification and Authentication for Rekey After Revocation

Once a digital certificate has been revoked, for whatever reason, the subscriber will be required to begin the request process afresh if they require a new digital certificate. All previous certificate information will be deemed unusable.

A subscriber may re-key following revocation by submitting a new application. Identification and authentication is performed by using the subscriber's existing account username and password. The person with access to the account must be the subscriber or someone authorized to act on behalf of the subscriber. Otherwise, a new subscriber account must be established in accordance with the identification and authentication requirements for obtaining an original certificate.

3.4 Identification and Authentication for Revocation Request

See Section 4.9.3 (Procedure for Revocation Request)

4. Certificate Life-Cycle Operational Requirements

This Part of the CPS describes the certificate application process.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate applications must be submitted by the individual who is the subject of the certificate or by persons who are duly authorized to request a certificate on behalf of the applicant. The WHOIS record maintained by the domain registrar presumptively indicates who the persons are with authority over the domain.

4.1.2 Enrollment Process and Responsibilities

All online/offline certificate applicants/subscribers needing a certificate shall complete the following general procedures for each certificate application:

- Generate a key pair
- Protect the private key of this key pair from compromise
- Submit a certificate request, along with the public key of this pair, to MANGO CA

The detailed procedure for digital certificate application/registration is dependent on the class of digital certificate being applied for. Please see **Appendix A** for a detailed description of the application/registration procedure for each class of digital certificate.

A subscriber is solely responsible for the protection of their private keys. Subscribers shall notify MANGO immediately if they believe that a private key has or may have been compromised in any way. A Subscriber shall be liable to MANGO and third parties for any misrepresentations they make to MANGO, as well as for direct and indirect consequences of those misrepresentations. Subscribers to MANGO CA Services acknowledge that they have been advised to obtain proper training in the use of a public key infrastructure prior to requesting or relying upon a digital certificate. MANGO offers different classes of digital certificate. MANGO makes no endorsement or recommendation in relation to these of any particular class of digital certificate for any particular application or purpose.

Subscribers must independently assess and determine the appropriateness of each class of digital certificate for any particular application or purpose.

Subscribers discharge their obligations under MANGO CPS by:

- Requesting the issue, renewal and if, necessary revocation of their certificates.
- Generating the key pair (except in the case of Encryption Certificate) on a secure medium as specified in MANGO CPS.
- Providing MANGO CA true and correct information at all times and providing sufficient proof of material certificate information to meet user registration or certificate renewal requirements.
- Acknowledging that in making a certificate application, they are consenting to certificate issue in the event the application is issued.
- Ensuring the safety and integrity of their private keys, including: controlling access to the computer containing their private keys and protecting the access control mechanism used to access their private keys.
- Agreeing to publish the public keys and certificates in the MANGO CA directory services by accepting the certificate.
- Using certificates in accordance with the purpose for which they are issued.
- Proving possession of private keys and establishing their right to use.

- Reporting MANGO CA of any error or defect in their certificates immediately or of any subsequent changes in the certificate information.
- Studying MANGO CPS before using their Certificates.
- Informing MANGO CA immediately, if a key pair is compromised, by a paper document and seeking urgent acknowledgement for the same.
- Exercising due diligence and sensible judgment before deciding to rely on a digital signature, including whether to check on the status of the relevant certificate.

To provide all required information to CA as and when required.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

During the certificate approval process, Mango CA employs controls to validate the identity of the Subscriber and other information featured in the certificate application.

After the receipt of the online/offline certificate request, MANGO CA shall perform all required validations as the precondition to certificate issuance.

MANGO CA shall validate that:

- The certificate applicant rightfully holds the private key corresponding to the public key listed in the certificate
- The certificate applicant/subscriber has agreed to the terms and conditions as stated in MANGO CA CPS
- The certificate applicant is the person identified in the request (for Class 2 and Class 3 Certificates)
- The information listed in the certificate request is accurate
- Subscriber does not own a revoked certificate, and incase subscriber's certificate is revoked he should conduct investigation to determine whether it is necessary to suspend or revoke other Digital Certificates owned by that particular subscriber.

Please see **Appendix A** for a detailed account of the issuance/distribution procedure for each class of digital certificate.

4.2.2 Approval or Rejection of Certificate Applications

From time to time, Mango CA may modify the requirements related to application information requested, based on Mango CA requirements, business context of the usage of certificates, or as it may be required by law with prior approval of CCA.

Following successful completion of all required validations of a certificate application, Mango CA will approve an application for a digital certificate.

If the information in the certificate application cannot be confirmed, then Mango CA will reject the certificate application. Mango CA reserves the right to reject an application for a certificate if, in its own assessment, the good and trusted name of Mango CA might be tarnished or diminished and may do so without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Mango CA reserves the right not to disclose reasons for such a refusal.

Applicants whose applications have been rejected may subsequently re-apply.

4.2.3 Time to Process Certificate Applications

Mango CA makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. The time frame is greatly dependent on the applicant providing the necessary details and documentation in a timely manner. Upon the receipt of the necessary details and documentation, Mango CA aims to confirm submitted application data and to complete the validation process and issue or reject a certificate application within ten (10) working days.

Occasionally, events outside of the control of Mango CA may delay the issuance process. However, Mango CA will make every reasonable effort to meet its issuance times and to make applicants aware of any factors that may affect issuance times.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The procedure for digital certificate issuance/distribution is dependent on the class of digital certificate being applied for. Please see **Appendix A** for a detailed account of the issuance/distribution procedure for each class of digital certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The procedure for digital certificate issuance/distribution is dependent on the class of digital certificate being applied for. Please see **Appendix A** for a detailed account of the issuance/distribution procedure for each class of digital certificate.

4.4 Certificate Acceptance

The procedure for digital certificate acceptance is dependent on the class of digital certificate being applied for. Please see **Appendix A** for a detailed account of the procedure for each class of digital certificate.

In the event that a subscriber requires both a private and public key from the MANGO CA service, the subscriber will be supplied with a secure encrypted container file, which contains both the public and private key components. This file may be formatted according to the PKCS#12 standard or using any other proprietary encrypted format.

A PKCS#12 file is encrypted using a 12 to 16 digit Personal Authentication Code (PAC) generated during the registration process.

In the event that a subscriber requires only a digital certificate (as the private and public keys have been generated outside the MANGO CA Service) the subscriber will be supplied with a digital certificate in various formats. For a detailed description of the digital certificate process refer to **Appendix A**.

By accepting a digital certificate issued by the MANGO CA from the MANGO Web site, the subscriber expressly agrees with MANGO and to all who reasonably rely on the information contained in the digital certificate that at the time of acceptance and throughout the operational period of the digital certificate, until notified otherwise by the subscriber that,

- no unauthorized person has ever had access to the subscriber's private key;
- all representations made by the subscriber to MANGO regarding the information contained in the digital certificate are true;
- all information contained in the digital certificate is true to the extent that the subscriber had knowledge or notice of such information, and does not promptly notify MANGO of any material inaccuracies in such information;

- the digital certificate is being used exclusively for authorized and legal purposes, consistent with MANGO CPS, and

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT IT AGREES TO THE TERMS AND CONDITIONS CONTAINED IN MANGO CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT –

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER ASSUMES A DUTY TO RETAIN CONTROL OF THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS EXCLUSION MODIFICATION OR UNAUTHORISED USE.

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD MANGO AND ITS AGENTS AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS, PROCEEDINGS OR CLAIMS, AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS FEES, THAT MANGO, ITS AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A DIGITAL CERTIFICATE AND THAT ARISE FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE SUBSCRIBER); (II) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE MANGO OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; (III) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE LOSS, DISCLOSURE, MODIFICATION OR UNAUTHORISED USE OF THE SUBSCRIBER'S PRIVATE KEY; (IV) USE OF THE DIGITAL CERTIFICATE FOR A PURPOSE WHICH IS LIBELLOUS OR CONSTITUTES MALICIOUS FALSEHOOD OR DISPARAGEMENT OF GOODS OR SERVICES, OR IS OTHERWISE DEFAMATORY, IS IMMORAL, OBSCENE, PORNOGRAPHIC, IS ILLEGAL OR ADVOCATES ILLEGAL ACTIVITY, OR CONSTITUTES A VIOLATION OF PRIVACY OR INFRINGES THE INTELLECTUAL PROPERTY RIGHTS OF MANGO OR A THIRD PARTY.

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber is responsible for installing the issued certificate on the subscriber's computer or hardware security module according to the subscriber's system specifications. A subscriber is deemed to have accepted a certificate when:

- The subscriber uses the certificate; or
- 15 days pass since issuance of the certificate.

4.4.2 Publication of the Certificate by the CA

Mango CA publishes the certificate by delivering it to the subscriber.

All the certificates issued by the Mango CA will be published in the on-line repository operated by the Mango CA.

See Section 2 for detailed description of certificate repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

If the RA has handled the communication with the subscriber, then it will be notified of the certificate issuance.

The RA will be informed about any certificate signatures and re-keys before expiration that were submitted through it.

All the certificates issued by the Mango CA will be published in the on-line repository operated by the Mango CA.

See Section 2 for detailed description of certificate repositories.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers shall protect their private keys from access by unauthorized personnel or other third parties. Subscribers shall use private keys only in accordance with the usages specified in the key usage extension.

Digital certificates are issued on both an individual and an organizational basis.

The suitable applications are as follows: secure electronic mail (s/mime), file and form signing, client authentication, retail transactions (banking applications), VPN & IPSEC applications, secure SSL/TLS applications, contracts signing applications, custom e-Commerce applications, code signing, time signing etc. MANGO digital certificates comply with the latest in Internet Standards (X509 V3) as set out in RFC 2459.

More generally, certificates shall be used only to the extent such use is consistent with all applicable laws, rules and regulations and in particular shall be used only to the extent permitted by applicable export or import laws.

4.5.2 Relying Party Public Key and Certificate Usage

Relying party – A Relying Party is an individual, or organization that relies on or uses a Digital Certificate issued by MANGO CA and/or any other information provided in a MANGO CA Repository to substantiate the identity and Public Key of a Subscriber and/or use such Public Key to send or receive digitally signed/encrypted communications to or from a Subscriber.

Relying parties shall be responsible for reviewing MANGO CPS to ensure the use of digital certificates for an appropriate purpose. Relying parties shall also be responsible for verifying certificate validity, including revocation checking before using the digital certificate. A relying party acknowledges and agrees to all applicable liability caps and warranties in a digital certificate before relying on that digital certificate. MANGO offers different classes of digital certificate. MANGO makes no endorsement or recommendation in relation to these of any particular class of digital certificate for any particular application or purpose. Relying parties must independently assess and determine the appropriateness of each class of digital certificate for any particular application or purpose.

- It is the sole duty of relying party to verify the purpose for which a certificate is used and these purposes should be in line with the purpose for which certificate is issued.
- Relying party has to verify the digital signature of a particular entity and has to satisfy itself with the validity.
- Check the CRL available at the MANGO CA repository every time relying on a digital signature created by the private key whose public key is certified and presented in the certificate issued by MANGO CA.

4.6 Certificate Renewal

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.1 Circumstance for Certificate Renewal

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.2 Who May Request Renewal

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.3 Processing Certificate Renewal Requests

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.4 Notification of New Certificate Issuance to Subscriber

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.6 Publication of the Renewal Certificate by the CA

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Mango CA will not renew subscribers' certificates. Subscribers must follow the re-key procedure as defined in section 4.7.

4.7 Certificate Rekey

The validity period associated with a digital certificate will be dependent on the digital certificate class in question. The MANGO CA will provide a facility to renew digital certificates that are just about to expire. The frequency at which digital certificates are reissued/rolled over is dependent on the class of digital certificates in question.

4.7.1 Circumstance for Certificate Rekey

Subscribers must regenerate their key pair in the following circumstances:

1. expiration of their certificate signed by the Mango CA;
2. revocation of their certificate by the Mango CA;

4.7.2 Who May Request Certification of a New Public Key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. MANGO CA requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

MANGO CA Certification Services support Certificate renewal in the mode of rekey. Subscribers may request Certificate renewal provided that:

- Content of Certificate information as contained in the registration records has not been changed.
- The request is made before the expiry of their current certificates.
- Their current certificates have not been revoked.
- They are not listed in the compromised user.
- Their keys are not included as the compromised keys.

4.7.3 Processing Certificate Rekeying Requests

Expiration warnings will be sent to subscribers before it is re-key time.

a) Re-key before expiration can be executed by stating a re-key request signed with the private key corresponding to the public one in the valid personal certificate of the subscriber. The requester is not required to pass the authentication procedure described in section 3.2.3, if this does not contrast with c) or d).
b) Re-key after certificate expiration uses completely the same authentication procedure as that for the new certificate.
c) At least once every 3 years the subscriber must go through the same authentication procedure as the one described for a new certificate.
d) In case the request for a new certificate is due to revocation of certificate the subscriber must follow the same procedure as the one described in for a new one.

4.7.4 Notification of New Certificate Issuance to Subscriber

Same as in section 4.3.2

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

Same as in section 4.4.1

4.7.6 Publication of the Rekeyed Certificate by the CA

Same as in section 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Same as in section 4.4.3

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Suspension is the process of making a certificate to make it invalid temporarily. Revocation is the process of making a certificate to be invalid permanently. MANGO CA can activate the suspended certificates. The revoked certificates cannot be reused and are listed in the CRL.

The MANGO CA reserves the right to revoke any of its issued digital certificates as per IT (CA) Rules 2010 or as instructed by the CCA. As per , the revoked Electronic Signature Certificate shall be added to the Certificate Revocation List (CRL).All revocation information is published and held in LDAP directory server where it is made publicly available when required for certificate verification processes.

4.9.1 Circumstances for Revocation

Digital certificates shall be revoked when any of the information on a digital certificate is known to be, or suspected be, inaccurate, or changes, or becomes obsolete or when the private key associated with the digital certificate is compromised or suspected to be compromised.

A digital certificate will be revoked in the following instances on notification:

1. Key Compromise (includes unauthorized access or suspect unauthorized access to private keys lost or suspected lost keys, stolen or suspected stolen keys, or destroyed keys).
2. Misuse of the Electronic Signature Certificate
3. Incorrect information contained in digital certificate
4. Electronic Signature Certificate is no longer required
5. Affiliation change
6. Subscriber loses relevant privileges
7. Subscriber’s name change
8. Superseded
9. Cessation of operation
10. Non-payment of invoice
11. Subscriber’s bankruptcy
12. Subscriber’s liquidation
13. Subscriber’s death
14. Breach of subscriber agreement with MANGO
15. Subscriber profile creation error
16. An end entity makes the request for the revocation
17. Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of MANGO CA Digital Certificate
18. Subscriber has breached or failed to meet their obligations under this CPS or any other agreement, regulation or law which may be in force

19. MANGO CA key compromise.

4.9.2 Who Can Request Revocation

The following entities may request revocation of a subscriber digital certificate:

- The MANGO CA.
- The subscriber/end entity user.
- The MANGO RA, on behalf of the individual subscriber.
- Any other entity holding evidence of a revocation circumstance about that certificate

4.9.3 Procedure for Revocation Request

Revocations shall be requested following the detection of a compromise or any other event necessitating revocation. MANGO will revoke the digital certificate upon such valid requests. Each time a digital certificate is revoked the MANGO CA issues and publishes a new CRL to the LDAP directory where it is available for public use in certificate verification. The subscriber is required to submit the revocation request via the MANGO Customer Management Portal (http://portal.mangoca.com) directly over an Internet connection. The subscriber may be required to provide a pass phrase that will be used to activate the revocation process. The subscriber need to download Revocation form from CA Repository (http://www.mangoca.com/repository/) and send it by hand delivery or fax by filling appropriate information as directed. From there on, the revocation process takes place automatically assuming the pass phrase has been verified. Digital certificate revocation requests may also be issued by contacting the administrators of the MANGO CA or RA administrators directly.

To process a revocation request initiated by an End Entity, MANGO CA:

- receives the End Entity revocation request
- revokes the certificate
- adds the certificate to its CRL
- publishes it in the repository
- informs subscriber about revocation of certificate by email

4.9.4 Revocation Request Grace Period

Revocation requests are to be verified on receipt and action should be taken as rapidly as possible.

4.9.5 Time Within Which CA Must Process the Revocation Request

Mango CA will process all revocation requests within 1 working day.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parts must download the CRL from the online-repository at least once a day and implement its restrictions while validating certificates.

4.9.7 CRL Issuance Frequency (If Applicable)

After the revocation request is received by MANGO CA, the concerned certificate will be revoked as per the procedure of certificate revocation, at the earliest. The revoked certificate will be added to the CRL immediately as part of this revocation procedure. The latest CRL will be available round the clock for downloading. In unforeseen circumstances the certificate will be revoked in not more than three working days after receiving the certificate revocation request. On detection of serious key

compromise, the corresponding digital certificate is revoked, CRL generated and published immediately.

The MANGO CA shall update and issue the CRL whenever certificates are revoked or suspended or or on each working day or on the first working day of each month or 30 days after the last update or as and when necessary, whichever occurs first. But MANGO CA will make every effort to publish new CRL in every last working day of the week.

MANGO CA includes the CRL distribution point extension, in the form of a URL, in the issued certificates indicating where the CRL, can be found.

4.9.8 Maximum Latency for CRLs (If Applicable)

No stipulation.

4.9.9 Online Revocation/Status Checking Availability

MANGO hosts a dedicated LDAP directory server for verifying the status of Certificates issued within the MANGO CA PKI. Details of the directory path will be provided in the MANGO CA certificate. The public will have unlimited access to the information contained within this directory.

MANGO CA has implemented the Online Certificate Status Protocol (OCSP) for the online status checking of the certificates.

4.9.10 Online Revocation Checking Requirements

CRL checking is the responsibility of the relying party whenever a transaction takes place. An entity that downloads a CRL from a repository shall verify the authenticity of the CRL by checking its digital signature and the associated certification path.

MANGO CA recommends that relying parties should check at least weekly, however where the value, the importance or sensitivity of a message, transaction or other file is high, it is recommended that the relying party checks on the transaction basis.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Rekey Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Suspension can be described as placing a certificate on hold for a brief period. This is useful for investigation to be carried out as to the validity of the certificate when required. A Certificate is suspended when:

- Verification as to whether the certificate has been issued containing wrong or falsified information is in progress
- Subscriber requests for suspension

4.9.14 Who Can Request Suspension

The subscriber shall request for the suspension of the certificate. The process of suspension can be initiated by MANGO CA also.

4.9.15 Procedure for Suspension Request

To process an online suspension request MANGO CA via Mango CA Customer Managerment Portal (http://portal.mangoca.com):

- receives and authenticates the digitally signed request
- suspends the certificate
- adds the certificate to its CRL
- publishes it in the repository

In case of offline certificate application:

- The suspension request is to be made by the subscriber in the application form available on www.mangoca.com
- Subscriber sends the duly signed application form to MANGO CA by fax/courier for suspension of certificate.
- MANGO CA suspends the certificate and publishes Certificate Revocation List (CRL).
- MANGO CA will inform about suspension of certificate to subscriber by email.

4.9.16 Limits on Suspension Period

A certificate may only be suspended for up to 15 days. If the subscriber has not removed their certificate from hold (suspension) within that period, the certificate shall be revoked for the reason of "Key Compromise".

In order to mitigate the threat of unauthorized person removing the certificate from hold, the subscriber identity shall be authenticated in person using initial identity proofing process described in Section 3.2.3.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Mango CA operates an on-line repository that contains all the certificates have been issued. The repository also contains CRL list. Promptly following revocation, the certificates and CRL status database in the repository, as applicable, shall be updated.

4.10.2 Service Availability

The on-line repository is maintained on best effort basis with intended availability of 24x7.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

MANGO CA will not escrow the private keys of subscribers.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. Facility, Management, and Operational Controls

This section describes the physical, procedural, and personnel security controls of the MANGO CA environment.

5.1 Physical Controls

The host site has been designed and built to ensure that the best possible protection is maintained at the MANGO CA site.

This facility is securely protected from unauthorized access by proactive access control alarm systems and surveillance equipment, and employees are only allowed access after being security clearance. A minimum of two people is required to be present to gain access into the secure CA rack itself.

5.1.1 Site Location and Construction

The CA site has been constructed with the highest possible security standards in mind. The location can only be accessed by correctly authenticated MANGO staff. In addition to this, there are certain areas of the location that require two specific individuals to be authenticated before access is granted.

Site is in a secure premise located in Dhaka.

- Remote surveillance system equipped with camera
- 24x7 trained professional guard to secure the datacenter

5.1.2 Physical Access

Only MANGO employees who possess the expert knowledge, experience and qualifications necessary to perform the allocated duties will operate all services.

- Single door standalone proximity time attendance controller
- Keep record of all visitor in enter and exit log
- Access control server which can generate report

5.1.3 Power and Air Conditioning

Alternative power sources have been put into place at the MANGO CA site. The secure location is also supplied with an air conditioning source.

- Online UPS
- Primary power supply from PDB
- Secondary power supply from Generator
- Adequate cooling system
- Dehumidifier system

5.1.4 Water Exposures

MANGO CA has taken adequate precautions to minimize the impact of water exposure to MANGO CA systems.

5.1.5 Fire Prevention and Protection

There has been sufficient fire prevention mechanisms put into place at the MANGO CA site.

- 67 L HFC 227 Agent cylinder c/w primary completer kit
- FM 200 (HFC 227) gas
- Smoke detector
- Extinguishing control panel with 2 detection zone and 2 releasing area with battery backup
- Rotating light, 6” fire alarm bell, strobe horn and warning sign

5.1.6 Media Storage

All backup magnetic media would be stored within the premises of the Mango CA securely with a copy at offsite.

5.1.7 Waste Disposal

MANGO has got adequate and environmentally safe waste disposal arrangements. The paper waste and other material would be disposed in such a manner that no confidential information could be known, from the waste disposed.

5.1.8 Off-Site Backup

All the backups of software, databases and records will be stored with all the security measures. There will be a backup in an offsite location based on the Disaster Recovery Policy.

5.2 Procedural Controls

Procedures are established, documented and implemented for all trusted and administrative roles required to operate the MANGO CA Service. Where possible and appropriate duties associated with MANGO specific operations are kept separate from general operations. This is accomplished through the assignment of different staff if possible, and with the use of separate physical and logical access controls.

There are a number of trusted roles assigned to different personnel involved in the operation of MANGO operations. These roles have been defined and assigned by senior management and are periodically reviewed as part of the Information Security Management System operated by MANGO. These reviews seek to reassign roles if necessary following staff changes or following company reorganization, to ensure no potential security risks exists as a consequence of multiple roles held by individuals, and to ensure that no conflicts of interest exist where staffs are assigned multiple roles.

The trusted roles defined for MANGO personnel and the policies employed in assigning staff members to these roles are designed to guarantee best practice is maintained in relation to information security, while at the same time providing flexibility required by the business in maximizing employee productivity.

5.2.1 Trusted Roles

MANGO has designated a number of trusted roles for Certificate Authority operations.

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are drawn in terms of four roles listed below:

1. **CA Administrator** – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
2. **CA Technical Administrator** – authorized to request or approve certificates or certificate revocations.
3. **Audit Administrator** – authorized to view and maintain audit logs.
4. **System Administrator** – authorized to perform system backup and recovery.

The following sections define these and other trusted roles.

5.2.2 CA Administrator

The administrator shall be responsible for:

1. Installation, configuration, and maintenance of the CA;
2. Establishing and maintaining CA system accounts;
3. Configuring certificate profiles or templates and audit parameters, and;
4. Generating and backing up CA keys.

Administrators shall not issue certificates to subscribers.

5.2.3 CA Technical Administrator

The CA Technical Administrator shall be responsible for issuing certificates, that is:

1. Registering new subscribers and requesting the issuance of certificates;
2. Verifying the identity of subscribers and accuracy of information included in certificates;
3. Approving and executing the issuance of certificates, and;
4. Requesting, approving and executing the revocation of certificates.

5.2.4 Audit Administrator

The Audit Administrator shall be responsible for:

1. Reviewing, maintaining, and archiving audit logs;
2. Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

5.2.5 System Administrator

The System Administrator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.6 Registration Authority

An RA's responsibilities are:

1. Point of contact for customer support relating to registration
2. Verifying identity
3. Entering Subscriber information, and verifying correctness;
4. Notification of authenticated digital certificate request to the CA;
5. Authentication of subscriber’s identification information, which is necessary to issue a digital certificate, to the CA

6. Acceptance and verification of digital certificate revocation requests and notification of the verified requests to the CA

The RA role is highly dependent on public key infrastructure implementations and local requirements.

5.2.7 CSP Roles

A CSP shall have at least the following roles.

The CSP administrator shall be responsible for:

1. Installation, configuration, and maintenance of the CSP;
2. Establishing and maintaining CSP system accounts;
3. Configuring CSP application and audit parameters, and;
4. Generating and backing up CSP keys.

The CSP Audit Administrator shall be responsible for:

1. Reviewing, maintaining, and archiving audit logs;
2. Performing or overseeing internal compliance audits to ensure that the CSP is operating in accordance with its CPS;

The system administrator shall be responsible for the routine operation of the CSP equipment and operations such as system backups and recovery or changing recording media.

5.2.8 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components that are named as public key certificate subjects. The PKI Sponsor works with the RAs to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.1, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

Besides the above, there are other roles that fall under different categories as follows:

Certificate Authority Technical Operation and Support

- Quality Assurance (QA) Management
- Database Administrator
- CA Application Support Engineer
- Operations Support Engineer

Hardware Security Module (HSM) Operations

- HSM Operator
- HSM Security Officer
- HSM Key Component Holder

MANGO has allocated a number of trusted qualified personnel to each one of the named role types.

The **responsibilities** of the persons assigned to these roles include:

QA Management

- General management of QA environment and testing principles.
- Ensure integrity of developed software.

- Testing newly developed software prior to sign-off and release into live environment.

Database Administrator

- Standard DBA administration tasks (e.g.: Archiving, Standby and Replicated Database Configuration, Checking Logs, Tuning, Hardening, Security Scanning) for databases used in the CA infrastructure.

CA Application Support Engineer

- Expert support in PKI and Cryptography technology used
- Assist in review and design of PKI architecture
- Trouble shooting
- Installation, build, configuration and testing of CA equipment
- Setup and support of local backup and Disaster Recovery infrastructure
- Provide training to other MANGO operations staff
- Out of hours on call support

The following responsibilities are carried out under multi person control:

- Root and Operational CA private key generation and PIN storage
- Root and Operational CA private key activation and recovery

Operations Support Engineer

- Carry out scheduled backups of database, logs, files etc.
- Ensure backups are stored securely and cycled correctly according to the policies employed by MANGO for offsite storage and tape cycling
- Ensure that integrity of backups are verified periodically and that the MANGO data retention policy is adhered to correctly
- Provide trouble shooting and on call out of hours support for common hosting infrastructure supporting MANGO operations. This includes networks, firewalls, Intrusion Detection Systems, routers, switches etc.

HSM Operator

- Change or view network settings for the HSM

HSM Security Officer

The following operations require one security officer:

- Place the HSM online/offline

The following operations require two security officers:

- Backup / Restore of encrypted application keys to/from smartcards
- Backup / Restore of HSM encrypting keys to/from smartcards
- Creation / Removal / Replacement of HSM encrypting keys
- Issue security officer smartcards and PINs
- Backup of security officer smartcards and PINs to secure storage locations
- Erase all keys from the HSM
- Set the HSM real time clock
- Re-initialize the HSM

HSM Key Component Holder

- Custodian of smartcard backups of encrypted application keys and HSM encrypting keys exported in N of M components onto backup smartcards and stored in secure locations.
- Adherence to MANGO HSM backup smartcard custody procedures when responding to requests for access to any backup components. These procedures are designed to ensure at least dual control (2 persons) is employed when backups of Root or Operational CA private key backups are requested.
- Custodian of backups of other private key container files, PINs, passwords etc. used in the operation of the CA and held in secure storage locations.

5.2.9 Number of Persons Required Per Task

The duties to be performed by each of the trusted personals in the MANGO CA Organizational structure are defined in such a manner that no single person would take control of the certificate issuance/revocation process.

At least two people are assigned to each trusted role to ensure adequate support at all times.

Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the CA infrastructure, most especially the MANGO CA private keys, and customer private keys if held temporarily by MANGO during the registration process.

CA key-pair generation and initialization of each of the CAs shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also required the active participation and oversight of senior management.

Two or more persons shall be required to perform the following tasks:

1. CA key generation;
2. CA signing key activation; and
3. CA private key backup.

5.2.10 Identification and Authentication for Each Role

The persons filling the trusted roles must undergo an appropriate security screening procedure, described as per Human Resource Policy of MANGO CA.

Identification and authentication mechanisms (such as passwords and tokens) are used to control account access for each role. All access by each role to accounts requires password and/or token identification and authentication. Separate accounts and passwords to those used for general operations, will be used for MANGO specific equipment and operations. These will be changed periodically in line with the MANGO password change policy and procedures.-

5.2.11 Roles Requiring Separation of Duties

Role separation, when required as set forth below, may be enforced either by the equipment, or procedurally, or by both means.

Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role.

5.3 Personnel Controls

MANGO employees who possess the expert knowledge will operate all services, experience and qualifications necessary to perform allocated duties. In accordance with the requirements for specific duties, employees undergo An Post security clearance prior to being granted permission to partake in the service and or related operations.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel appointed to the trusted roles will be chosen in accordance with MANGO hiring practices for positions of this sensitivity.

Personnel in key operational positions will:

- Not be assigned other duties that may conflict with their duties and responsibilities;
- Not as far as is known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Have received proper training in the performance of their duties.
- Be aware of disciplinary measures for breaches of security controls/processes.

5.3.2 Background Check Procedures

Background checks shall be carried out and staff fulfilling sensitive roles shall be formally appointed. Staff shall not take up their duties until any such vetting/clearance process has been completed.

5.3.3 Training Requirements

The persons identified would have undergone adequate training to handle Mango CA Office operations, understand PKI concepts, exposure to software and hardware of PKI, computer security, and operation of Mango CA functions.

5.3.4 Retraining Frequency and Requirements

Every year the Mango CA personal would undergo skills up gradation training programs or whenever there is requirement due to the change or up gradation in the technology.

5.3.5 Job Rotation Frequency and Sequence

Mango CA personnel will undergo job rotation practices as per the Human Resources Policy of Mango.

5.3.6 Sanctions for Unauthorized Actions

Unauthorized actions are liable for strict disciplinary action. Anyone who abuses his position would lose authorization permanently. Action will be taken according to the Law of the Country.

5.3.7 Independent Contractor Requirements

The people who would be contracted in Mango CA Office would also be qualified and trustworthy professionals.

5.3.8 Documentation Supplied to Personnel

The staff would be provided with all the guidelines and documents for performing various functions in Mango CA. Manuals of hardware and software, operational practice and procedural documents, including this CPS are also provided.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

MANGO CA will archive the records in accordance to the standards specified in the IT (CA) Rules 2010.

All security auditing capabilities of the CA, CSP, and RA operating system and the CA, CSP, and RA applications required by this CPS shall be enabled. As a result, most of the events identified in the table below shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, and
4. The identity of the entity and/or operator that caused the event.

MANGO CA Installation Procedure: All events involved in the generation of the MANGO CA key pairs (the Root MANGO CA Key, all MANGO Operational CA keys and all associated backup key pairs) will be recorded. This includes all configuration data used in the process. The configuration of all the MANGO PKI components will also be recorded at this stage. This will ensure that all the necessary security procedures will be adhered to during PKI creation and that important configuration details are recorded.

Private Key and Password holders within the MANGO PKI: The MANGO CA will consist of several passwords and key pairs, which are crucial to the administration, operation and fundamental security of the PKI environment. Details of the individuals within MANGO who have access to particular key pairs and passwords will be carefully audited. Key pair access will take the form of PIN protected smart cards. Access to the database will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smart card and another individual having access to the corresponding PIN to unlock the smart card. This ensures that a minimum of two people being present to perform certain tasks on the MANGO PKI system.

All End User Registration Data All data involved in each individual digital certificate registration process will be carefully recorded for future reference if needed.

The Certification process including certificate/key pair delivery: All data and procedures involved in the certification and distribution of digital certificates will be recorded. Most of this information will be recorded in the form of event logs recorded in the database (the underlying DBMS used by the PKI software). This includes information such as Digital certificate request acceptance

- Key pair generation
- Digital certificate generation
- All request and response information sent between the various PKI modules themselves
- Digital certificate distribution mechanisms

Certificate and CRL Publication: All data relevant to the publication of digital certificates and CRLs by the MANGO CA to the MANGO LDAP server will be recorded. Digital certificates are issued to the LDAP server immediately after issuance. Information relating to this transaction can be viewed from the event logs maintained by the MANGO CA (in the database). A CRL is issued to the LDAP server immediately after a digital certificate gets revoked and also at periodic intervals as configured in

the MANGO CA (generally once a day). Again details of this can be viewed in the MANGO CA event log.

Certificate Revocation All digital certificate revocation request details will be recorded including reason for revocation.

Firewall monitoring: As the MANGO PKI environment will consist of several important machines hosting the various PKI modules, careful monitoring of all communication between these machines will take place to ensure that only legitimate connections with legitimate transactions take place. A firewall with rigid rules will restrict malicious users from making non-legitimate connections. Logs recording all network traffic to and from these machines will be recorded.

Database Auditing As several of the important PKI components rely on making database client logins to a database server for their operations, database auditing will be set-up to monitor all client logins to ensure that only clients from the legitimate terminals and profiles make connections. Any breach of this will be promptly noticed and investigated.

Backup and Recovery procedures on the MANGO PKI All aspects of the configuration of the MANGO backup site will be recorded. Backing up the MANGO PKI involves making a backup of the important PKI key pairs at PKI creation, backing up important module specific files necessary for private key access and making regular backups of the database used by the individual PKI components themselves. All procedures involved in the backup process will be recorded.

In the event that backup and recovery procedures come into play, the entire procedures surrounding the restoration of the MANGO PKI will be recorded.

System Maintenance and Error detection As the MANGO PKI environment will involve maintenance by appointed system administrators (SAs), all details of maintenance performed on the machines will be recorded. The SAs will also log all error messages detected on any of the designated machines.

Backup of Records/Audit Material All data recorded as mentioned in the above sections will be backed up. Therefore there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios.

- Subscriber's Application Form
- Subscriber Registration & Verification Records
- Digital Certificates
- Suspension Notice
- Information on Suspended Certificates
- Information on the Activation of Suspended Certificates
- Information on the Expiry of Certificates

5.4.2 Frequency of Processing Log

Frequency of processing log will be maintained as per CCA determined.

5.4.3 Retention Period for Audit Log

Retention period of audit log will be maintained as per CCA determined.

5.4.4 Protection of Audit Log

Archives shall be retained and protected against modification or destruction. Audit log will be securely protected and will be accessible only by authorized personnel of CA.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries will be backed up in manual form using access log.

5.4.6 Audit Collection System (Internal Versus External)

Audit log collection system is internal to the Mango CA.

5.4.7 Notification to Event-Causing Subject

This CPS imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The relevant audit data collect shall be regularly analyzed by the appointed MANGO personnel for any attempts to violate the integrity of any element of the MANGO PKI. In the unlikely event that this situation arises it will be quickly detected and acted upon.

5.5 Records Archival

5.5.1 Types of Records Archived

Mango CA, CSP, and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued.

5.5.2 Retention Period for Archive

The minimum retention periods for archive data are listed below for the various assurance levels. This can vary based on CCA directions.

Assurance Level	Archive Retention Period
Class 1	7 Years
Class 2	7 Years
Class 3	7 Years

5.5.3 Protection of Archive

No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA and CSP, the authorized individuals are Audit Administrators. For the RA, authorized individuals are someone other than the RA (e.g., Information Assurance Officer or IAO). The contents of the archive shall not be released except as determined by the CCA, the Licensed CA, or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSP, or RA) with physical and procedural security controls equivalent or better than those for component.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

All events that are recorded within MANGO CA Service include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating. MANGO uses procedures to review and ensure that all servers within the PKI maintain accurate time synchronized from CCA provided NTP location.

Trusted time synchronizing Time Stamping Service using NTP will be implemented during installation.

5.5.6 Archive Collection System (Internal or External)

Archive collection system is internal to the Mango CA.

5.5.7 Procedures to Obtain and Verify Archive Information

Upon proper request (see Sections 9.3 and 9.4) and payment of associated costs, Mango CA will create, package and send copies of archive information. Archived information is provided and verified by reference to the time stamps associated with such records as described in Section 5.5.5. Access to archive data is restricted to authorized personnel in accordance with Mango CA internal security policies.

5.6 Key Changeover

In case of change in CA's key pair, the subscribers will be notified through website.

Once an issued digital certificate has expired the subscriber may be required to reapply for a new digital certificate in the same manner as they originally applied. The subscriber will be notified in advance of the expiration date and they will be given details as to how they must reapply for their new digital certificate. This process will involve the subscriber obtaining a new private and public key.

Depending on the digital certificate policy chosen by the subscriber, there will be the option to automatically reissue the subscriber with a new digital certificate prior to the expiry date of the original digital certificate. Mango CA does not renew subscriber's certificate. Subscriber must follow the re-key procedure. The re-key is the process of generating new key pair before or after the expiry of the certificate.

The subscriber will be made fully aware of the key lifetime once they apply for a digital certificate. The subscriber will also be notified as to how they will need to reapply for a new digital certificate once the expiration date has passed. As mentioned in some cases the subscriber will be automatically issued a new digital certificate without any manual intervention.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

MANGO CA has implemented a robust combination of physical, logical, and procedural controls to minimize the risk and potential impact of a key Compromise or disaster.

The DR Plan would consist of a detailed manual covering all the aspects of compromise and disaster recovery like key compromise, crashing of systems both software and hardware, corruption of systems

both the hardware and software, communication failures, problems arising out of strike, fire, flood or any other natural disaster.

The staff would be identified and trained to conduct these operations if, any disaster happens.

If Mango CA detects a potential hacking attempt or other form of compromise, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA or CSP needs to be rebuilt, only some certificates need to be revoked, and/or the CA or CSP key needs to be declared compromised.

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

The MANGO disaster recovery plan incorporates measures to minimize system down time for all critical components of the PKI system, including the hardware, software and keys, in the event of a failure or compromise of one or more of these components.

Using the backups and archives necessary software, hardware and databases shall be restored for functioning. In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to Review Committee of CCA and MANGO CA's incident handling actions are endorsed. Such procedures involve appropriate escalation, incident investigation, and incident response. If required, MANGO CA's or disaster recovery procedures will be implemented. MANGO CA maintains offsite backups of important CA information which includes, but is not limited to: application logs, database records for all Certificates issued.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of MANGO CA private key, MANGO CA's disaster recovery procedures are enacted-

- MANGO CA shall inform subscribers and relying parties through website
- All certificates will be revoked and CRL will be generated.
- No new certificates will be generated with compromised key pair.
- MANGO CA will generate a new key pair.
- Subscribers need to reapply for getting new certificate after the notification by MANGO CA.

In the case of end entity key compromise:

- Inform the RA (in this case MANGO CA itself) and relying parties
- Request the revocation of the end entity's certificate.

5.7.4 Business Continuity Capabilities After a Disaster

Mango CA manages its backup, archive, and offsite storage in accordance with its backup policy, and contingency and recovery plan.

5.8 CA Termination

Before ceasing to act as a Certifying Authority, MANGO CA shall:

- give notice to the Controller of its intention to cease acting as a Certifying Authority, ninety days before ceasing to act as a Certifying Authority or ninety days before the date of expiry of license;

- advertise sixty days before the expiry of license or ceasing to act as Certifying Authority, as the Mango case may be, the intention in such daily newspaper or newspapers and in such manner as the Controller may determine;
- notify its intention to cease acting as a Certifying Authority to the subscriber and Cross Certifying Authority of each unrevoked or unexpired Digital Certificate issued by it, by giving notice of at least sixty days before ceasing to act as a Certifying Authority or sixty days before the date of expiry of unrevoked or unexpired Digital Certificate, as the case may be;
- the notice will be sent to the Controller, affected subscribers and Cross Certifying Authorities by digitally signed e-mail and registered post;
- revoke all Digital Certificates that remain unrevoked or unexpired at the end of the ninety days notice period, whether or not the subscribers have requested revocation;
- make a reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding Digital Certificates;
- make reasonable arrangements for preserving the records for a period of ten years;
- pay reasonable restitution (not exceeding the cost involved in obtaining the new Digital Certificate) to subscribers for revoking the Digital Certificates before the date of expiry;
- after the date of expiry mentioned in the license, MANGO CA will destroy the certificate–signing private key and confirm the date and time of destruction of the private key to the Controller.

6. Technical Security Controls

The MANGO CA private keys are protected within a hardware security module ("HSM"). The use of a HSM, with FIPS-140 level 3 capabilities ensures that MANGO are adhering to the highest industry standard regarding the generation and protection of the Operational CAs' private keys. Access to the modules within the MANGO environment including the Operational CAs' private keys are restricted by the use of token/smartcards and associated pass phrases. These smartcards and pass phrases are allocated among the multiple members of the MANGO management team. Such allocation ensures that no one member of the team holds total control over any component of the system.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.2 CA Private Key

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. The CA Key pair will be generated and stored in accordance with FIPS 140-2 level 3 standards. The activities executed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for ten years as per CCA requirement. The CA personnel will generate key pair and either download certificate in smart card/hardware token or the downloaded version to be installed by the end entity.

6.1.3 Subscriber Private Key

In the case of end entity, the key pair should be generated preferably by the end entity and certificate to be installed by the end entity.

MANGO will offer the facility to allow subscribers to generate their own private key prior to submitting of a digital certificate request. This service will involve the subscribers generating their own private key pair and submitting a digital certificate request direct to the MANGO CA Service. MANGO subscribers will be made fully aware of how to avail of the services on offer and how that can apply for the various digital certificates on offer.

MANGO can also generate the subscriber's public and private key pair. The subscriber will be required to provide all the necessary identification and authentication information when the digital certificate is being requested. Once all the registration information is collected by the MANGO CA system the subscriber's public and private key pair is generated within a secure environment. Mango will not store any private key of it's subscriber at any circumstances.

6.1.4 Private Key Delivery to Subscriber

Subscribers' private keys (except encryption keys) are generated by them and required no delivery.

Once the subscriber certificate request has been signed by the MANGO CA system the subscriber's digital certificate and private key will be distributed via a secure channel whereby only the subscriber will have access to his/her private key. Refer to **Appendix A** for the various methods of distribution.

6.1.5 Public Key Delivery to Certificate Issuer

Generally digital certificate is delivered to the certificate issuer by means of an on-line exchange utilizing functionalities of CA software.

The digital certificate will be delivered to the subscriber in one of the defined methods as specified in **Appendix A.**

6.1.6 CA Public Key Delivery to Relying Parties

The CA public key is made available by means that can be trusted by the users, protected in self–signed certificate, licensed by CCA.

The MANGO CA certificate will be made available to the general public from the dedicated MANGO LDAP directory service. It is also available from the MANGO Web site for download.

6.1.7 Key Sizes

6.1.8 CA Key Size

The key length of the MANGO CA modules will be 2048 bit.

6.1.9 Subscriber Key Size

The key sizes issued to subscribers will depend on the digital certificate policy chosen by the subscriber. There are a number of digital certificate policies in place within the MANGO CA environment and each one documents the key size.

The length of a private key must be at least 2048 bits. Mango CA cannot certify an entity key pair with key length less than 2048 bits.

6.1.10 Public Key Parameters Generation and Quality Checking

RSA keys shall be generated in accordance with FIPS 186-2.

Key parameters generation: Whichever entity is generating the key pair i.e. CA or subscriber, its application will generate the parameters used to create public keys.

Key parameters quality checking: The application software used by subscriber should check the quality of parameter in the case of key pair generation.

6.1.11 Key Usage Purposes (As Per X.50vkey Usage Field)

The purposes for which a key can be used may be restricted by MANGO CA through the Key Usage extension in the certificate.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

MANGO CA has put into practice a combination of physical, logical, and procedural controls to ensure the security of private keys. Logical and procedural controls are described in this section. Physical access controls are described in Section 5 and its sub section. Subscribers are required to take essential precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

The generation and maintenance of both the Root and Operational CAs' private keys are facilitated through the use of an advanced cryptographic device known as a HSM (Hardware Security Module). The HSM used in the case of the MANGO CA is designed to provide FIPS-140 Level 3 security standards in both the generation and the maintenance in all Operational CA private keys.

6.2.2 Private Key (N out of M) Multiperson Control

MANGO CA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. CA makes use of split passphrase needed to make use of a CA private key, which are held by trained and trusted individuals called CA Coordinators. m out of n multi-person control for particular hardware cryptographic module is required to activate a MANGO CA private key stored on the module.

6.2.3 Private Key Escrow

MANGO CA will not escrow the private keys of subscribers.

6.2.4 Private Key Backup

Mango CA Private Keys are generated and stored inside the cryptographic hardware. MANGO CA creates backup copies of CA private keys for usual recovery and disaster recovery purposes. Where such keys must be transferred to other media for backup and disaster recovery purposes, they are transferred and stored in an encrypted form in specialized key storage devices. All CA private keys are backed up in accordance with controls described in Section 6.1.1. Backup tokens containing CA private keys are stored securely off-site for backup and disaster recovery purposes.

End entity may back up its keys and store them in an encrypted file.

6.2.5 Private Key Archival

MANGO CA key pair will be archived for a period for 10 years when it reaches the end of their validity period. Archived key pairs will be securely stored using hardware cryptographic modules that meet the requirements of MANGO CPS. The same will be securely destroyed upon the end of the archive period.

MANGO CA does not archive copies of RA and Subscriber signing private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

MANGO CA Private Key is generated onboard, stored in encrypted form and remains in encrypted form and it is decrypted only when it is used. When CA key pair is backed up to another hardware cryptographic module, such key pair is transported between modules in encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.6

6.2.8 Method of Activating Private Key

The activation of the MANGO CA private key pair requires more than one person. The activation procedure will require the relevant persons, to possess between them, a series of smart cards and pass phrases to unlock the MANGO CA private key.

In case of subscriber, private keys are activated by the client application. Subscriber private key is activated by a PIN or password.

6.2.9 Method of Deactivating Private Key

MANGO CA private key is deactivated upon removal from the token reader.

In all cases, subscribers have an obligation to adequately protect their private key(s).

6.2.10 Method of Destroying Private Key

At the expiry of MANGO CA's private key, remaining copies of the CA private key are securely destroyed after archival. In addition, archived CA private keys are securely destroyed at the conclusion of their archive periods. The same methods will be followed for destruction of private key in case of key compromise.

In case of subscriber, for Smart card based keys, the private keys can be deleted by personalization/Initialization of card/token.

6.2.11 Cryptographic Module Rating

MANGO CA shall utilize hardware cryptographic modules rated FIPS-140-level 3 to perform all digital signing operations. All cryptographic module engineering security threats are assessed and addressed.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All certificates containing public keys (including MANGO CA as well as its subscribers) are archived by MANGO CA upon expiry as part of CA's routine backup procedures and kept for a period of ten years as per the Act.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The MANGO CA private key will have a key validity period of 5 years. MANGO retains the right to extend the validity period of the MANGO CA certificate with prior approval of CCA. The validity period of subscriber certificates will be dependent on the class of digital certificate in question. Refer to **Appendix B** for details of the various validity periods.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

After personalization, no activation data other than access control mechanisms (PIN) are required to operate cryptographic modules

6.4.2 Activation Data Protection

Pass phrases or PIN shall not be accessible to anyone except the operator and the certificate holder.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

MANGO CA has established security for both the hardware and software security systems.

Mango CA servers and support-and-vetting workstations run on trustworthy systems. Mango CA computer systems are configured and hardened using industry best practices. All operating systems require individual identification and authentication for authenticated logins and provide discretionary access control, access control restrictions to services based on authenticated identity, security audit capability and a protected audit record for shared resources, self-protection, and process isolation. All systems are scanned for malicious code and also protected against spyware and viruses.

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA, CSP and shall include the following functionality:

1. Require authenticated logins
2. Provide Discretionary Access Control
3. Provide a security audit capability
4. Require a trusted path for identification and authentication
5. Provide domain isolation for process
6. Provide self-protection for the operating system

The computer system shall be configured with minimum of the required accounts and network services.

6.5.2 Computer Security Rating

As guided by the CCA security is provided.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Application development takes place in controlled environment. All quality control checks are conducted at regular frequency.

The System Development Controls are as follows:

1. Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with.
2. All hardware are shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location
3. The hardware and software are dedicated to performing the PKI activities. There are no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.
4. Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the PKI operations are obtained from sources authorized by local policy.
5. Hardware and software are scanned for malicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

The MANGO CA environment will adhere to best practices in relation to security controls. The objective will be to ensure that these computer systems have the minimum number of accounts required, use passwords which meet the required policy, have only the required network services enabled, and have appropriate discretionary access controls on all security-relevant directories and files.

Change control processes consist of change control data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. In this manner, Mango CA can verify whether a change to the system has been properly evaluated for risk mitigation and authorized by management.

6.6.3 Life Cycle Security Controls

All potential life cycle security risks are observed and taken care.

6.7 Network Security Controls

The MANGO CA and RA environments will be accessed through a secure DMZ environment.

Appropriate security measures are employed to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. These firewall rules are configured to allow the minimal amount of connectivity. Only those protocols identified as being necessary to accomplish the CA or RA functions shall be allowed to pass through; all others will be disabled.

Unused network ports and services shall be turned off. Protocols that provide network security attack vector(s) shall not be permitted through the boundary control devices. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time-Stamping

System time for Mango CA computers are updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). The synchronization of NTP is provided from CCA facility.

All components shall regularly synchronize with the time service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Revocation of a Subscriber's Certificate
- Posting of CRL updates
- OCSP or other CSP responses

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events as listed in Section 5.4.1.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The MANGO operational CA certificate(s) is signed by the CCA of Bangladesh. The CCA of Bangladesh acts as the source of trust. The MANGO CA will sign all operational MANGO CA entities.

To ensure global compatibility and conformity to public key standards, the MANGO CA will utilize the "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999" (ITU-T X.509 version 3) digital certificate standard.

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.1 Version Number(s)

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.2 Certificate Extensions

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.3 Algorithm Object Identifiers

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.4 Name Forms

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.5 Name Constraints

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.6 Certificate Policy Object Identifier

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.7 Usage of Policy Constraints Extension

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.8 Policy Qualifiers Syntax and Semantics

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

For a detailed description of the certificate profile refer to **Appendix B** and **Appendix C**.

7.2 CRL Profile

To ensure global compatibility and conformity to public key standards, MANGO CA will utilize the "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999"

(ITU-T X.509 version 2) Certificate Revocation List standard. An X.509 version 2 CRL contains a signed list of digital certificates that have been revoked with the date and other useful information used in the certificate verification process.

For a detailed description of the MANGO CA CRL profile refer to **Appendix D**.

7.2.1 Version Number(s)

For a detailed description of the MANGO CA CRL profile refer to **Appendix D**.

7.2.2 CRL and CRL Entry Extensions

For a detailed description of the MANGO CA CRL profile refer to **Appendix D**.

7.3 OCSP Profile

OCSP requests and responses shall be in accordance with RFC 2560 as listed below.

For a detailed description of the MANGO CA OCSP profile refer to **Appendix H**.

7.3.1 Version Number(s)

For a detailed description of the MANGO CA OCSP profile refer to **Appendix H**.

7.3.2 OCSP Extensions

For a detailed description of the MANGO CA OCSP profile refer to **Appendix H**.

8. Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The frequency of audit shall be governed by CCA Rules.

MANGO CA shall conduct,-

(a) **Half yearly** audit of the Security Policy, physical security and planning of its operation;
(b) **Quarterly** audit of its repository.

8.2 Identity/Qualifications of Assessor

A certified Information Security Auditor empanelled by the CCA shall audit services of the MANGO CA and any designated authorized agents on an annual basis. MANGO reserves the right to appoint this independent external auditor.

8.3 Assessor's Relationship to Assessed Entity

(1) The auditor shall be independent of the MANGO CA and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to MANGO CA.

(2) the auditor for the purpose shall be enlisted to the CCA being satisfied that that the auditor has sufficiently equipped, technically skilled, expertise, manpower and technology for auditing Certifying Authority ;

(3) The auditor and MANGO CA shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

8.4 Topics Covered by Assessment

The compliance audit mechanism is to ensure that the requirements of this CPS are being implemented and enforced.

8.5 Actions Taken as a Result of Deficiency

If deficiencies are found in the audit reports, MANGO CA will implement appropriate correction within a reasonable time frame.

Any failure to comply with the specified requirements of MANGO CPS shall be addressed by the MANGO CA or its authorized agent as soon as is operationally possible.

8.6 Communication of Results

MANGO CA shall submit copy of each compliance report to the Controller within four weeks of the completion of such audit and where irregularities are detected in such audit or submitted report, the Certifying Authority shall take immediate appropriate steps.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fees for Certificates issuance and renewal services provided by MANGO CA will be set forth in the MANGO CA website (http://mangoca.com/es.aspx). These fees are subject to change, and any such changes shall become effective immediately after posting in the MANGO CA website.

9.1.2 Certificate Access Fees

There are no charges for access to any certificate.

9.1.3 Revocation or Status Information Access Fees

MANGO CA does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a MANGO CA issued certificate through the use of Certificate Revocation Lists. MANGO CA may execute the right to establish and charge a reasonable fee for providing certificate status information services via OCSP.

9.1.4 Fees for Other Services

Fees for any other services such as access to archive records or key recovery will be reasonable and will set forth in the MANGO CA website.

9.1.5 Refund Policy

Alongwith the fees for Certificates issuance and renewal services, the refund policy will be set forth in the MANGO CA website.

9.2 Financial Responsibility

The MANGO CA does not make any representation and does not give any warranties on the financial transactions, which the subscribers and the relying parties undergo using the Digital Certificate obtained from the MANGO CA. The subscribers and the relying parties shall be responsible for any loss, damages or any consequences due to such transactions.

MANGO is not the agent, fiduciary or other representative of any subscriber and/or certificate holder and must not be represented by the subscriber and/or certificate holder to be so. Subscribers and/or certificate holders have no authority to bind MANGO by contract or otherwise, to any obligation.

9.2.1 Insurance Coverage

Not Applicable.

9.2.2 Other Assets

MANGO CA shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to PKI Participants described in Section 1.3 of this CPS.

9.2.3 Insurance or Warranty Coverage for End-Entities

MANGO CA does not offer protection to end entities that extends beyond the protections provided in this CPS. Any such protection shall be offered at commercially reasonable rates set forth in the MANGO CA website.

Subscribers should refer to the Subscriber Agreement that they have with MANGO CA.
Relying Parties should refer to the Relying Party Agreement. Both are located at:
http://www.mangoca.com./repository/.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

MANGO CA keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys
- Any activation data used to access private keys or gain access to the CA system
- Any business continuity, incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any information held by MANGO CA as private information in accordance with Section 9.4
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5, including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS)

9.3.2 Information Not Within the Scope of Confidential Information

Subscriber application data identified herein as being published in a digital certificate is considered public and not within the scope of confidential information. Subscribers acknowledge that revocation data of all certificates issued by the MANGO CA is public information and is periodically published 3 times a day at the MANGO CA repository.

9.3.3 Responsibility to Protect Confidential Information

MANGO CA observes applicable rules on the protection of personal data deemed by law or the MANGO CA privacy policy (see Section 9.4 of this CPS) to be confidential.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The contents of digital certificates issued by MANGO are public information. MANGO hereby guarantees that it will not divulge any additional subscriber information to any third party for any reason, unless compelled to do so by law or by order of the Court of law or by competent regulatory authority.

9.4.2 Information Treated as Private

All information other than that going into the digital certificate or held in publicly available repositories will be kept strictly confidential.

9.4.3 Information Not Deemed Private

All information going into the digital certificate or held in publicly available repositories will not be kept and treated as confidential.

9.4.4 Responsibility to Protect Private Information

Each party shall protect the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like import, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

9.4.5 Notice and Consent to Use Private Information

In the course of accepting a digital certificate, all subscribers have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the MANGO CA, and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

MANGO CA shall treat the following information confidential, namely:--

(a) Application for Electronic Signature Certificate, whether approved or rejected;

(b) Information relating to Electronic Signature Certificate collected from the subscriber or elsewhere as part of the registration and verification record but this will not include information contained in the Digital Signature Certificate information;

(c) Executed subscriber agreement.

Access to Confidential Information shall be as follows-

(1) Access to confidential information by MANGO CA operational staff shall be on a "need-to-know" and "need-to-use" basis.

(2) Paper based records, documentation and backup data containing all confidential information as prescribed by CCA shall be kept in secure and locked container or filing system, separately from all other records.

(3)No confidential information shall be allowed to be taken outside the country; however, the CCA may grant permission for taking confidential information outside the country if the same is required for performing constitutional obligation or any document is produced before him which legally obliges him to grant such permission.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

MANGO CA shall not release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom MANGO CA owes a duty to keep information confidential.

- The party requesting such information.
- A court order, if any.

9.4.7 Other Information Disclosure Circumstances

All other information disclosure circumstance shall be governed by the requirements of laws of Bangladesh concerning the protection of personal data.

9.5 Intellectual Property Rights

All Intellectual Property Rights in the MANGO CA Service and any associated documentation (including any and all functional and performance specifications (the "Specifications")) shall vest in MANGO Limited and/or its licensors. For the purposes of this document, "Intellectual Property Rights" shall mean all patents, copyrights (including copyright in computer software), design rights, trademarks, trade names, service marks, know-how, trade secrets and technical data, together with all goodwill attaching or relating thereto and all other industrial or intellectual property rights of whatever nature arising anywhere in the world, (and whether any such rights are registered or unregistered, including any application for registration in respect of any such rights).

The subscriber and each relying party shall ensure that in using the MANGO CA Services it will do nothing illegal or infringe upon any third party rights and in particular will ensure that any material that it supplies or transmits is not illegal, libelous, and does not infringe upon any Intellectual Property Right of MANGO or any third party.

The subscriber and relying parties are given a non-exclusive, non-transferable, royalty free, limited license to use the Intellectual Property Rights in the MANGO CA Service only to the extent and solely for the purpose of availing of the MANGO CA Service. The granting of this limited license is conditional on the **subscriber's and relying party's agreement** to and compliance with all of the terms and conditions of MANGO CPS.

Nothing in this document shall be taken or inferred as any endorsement by MANGO of the subscriber, its business, goods or services.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The nature of the steps MANGO takes to verify the information contained in a digital certificate vary according to the digital certificate fee charged, the nature and identity of the subscriber, and the applications for which the digital certificate will be marked as trusted.

MANGO CA warrants that:

a) It has taken reasonable steps to verify that the information contained in any digital certificate is accurate at the time of issue
b) Digital certificates shall be revoked if MANGO believes or is notified that the contents of the digital certificate are no longer accurate, or that the key associated with a digital certificate has been compromised in any way
c) To publish the accepted Digital Certificates in the MANGO CA repository
d) To put the revoked certificates into the CRL and publish the updated CRL in the MANGO CA repository as specified in this MANGO CA CPS.

9.6.2 RA Representations and Warranties

RA Confirms the following:

- It is the Point of Contact (POC) of any subscriber for certificates.
- It has taken reasonable measures to Authenticate subscriber's identification information, which is necessary to issue a digital certificate, to the CA;
- Confirming that verification of the information provided by the subscriber for the digital certificate application has been accurately transcribed to the digital certificate;
- Interacting on acceptance and verification of digital certificate revocation requests and notification of the verified requests to the CA.
- Verifying documents presented in support of applications

9.6.3 Subscriber Representations and Warranties

MANGO CA requires Subscribers to warrant that:

a) Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
b) No unauthorized person has ever had access to the Subscriber's private key,
c) All representations made by the Subscriber in the Certificate Application the Subscriber submitted are accurate,
d) All information supplied by the Subscriber and contained in the Certificate is accurate,
e) The Certificate is being used solely for authorized and legal purposes, consistent with MANGO CPS, specifically for the purpose as stipulated/stated by the submission in the certificate application only, and
f) The Subscriber is an end-user Subscriber and not a CA,

9.6.4 Relying Party Representations and Warranties

It is unreasonable for any party to rely on a digital certificate issued by MANGO if the party has actual or constructive notice of the compromise of the digital certificate or its associated private key. Such notice includes but is not limited to the contents of the digital certificate and information incorporated in the digital certificate by reference, as well as the contents of MANGO CPS and the current set of revoked digital certificates published by MANGO.

Relying Parties acknowledge that they have satisfactory information to make an educated decision as to the extent to which they decide to rely on the information in a Certificate, that they are solely accountable for deciding whether or not to rely on such information, and that they shall bear the lawful consequences of their failure to act upon the Relying Party obligations.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

MANGO makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

a) The MANGO CA disclaims all other warranties except as expressly stated in MANGO CA CPS.
b) The MANGO CA does not warrant accuracy, reliability, correctness and authenticity of the unverified information contained in the Digital Certificate.
c) The MANGO CA does not warrant the reliability of the technique used in generation and storage of the private key by the applicant/subscriber.

d) The MANGO CA does not warrant any loss, damage or consequences arising out of the compromise of digital certificates or private keys of users, which are not expressly brought to the knowledge of the MANGO CA by the respective users.

9.8 Limitations of Liability

MANGO CA will not be lawfully responsible in any way, for any imprecision, mistake, delay, or lapse, in the issuance or verification of any Digital Certificate, or for non-performance including suspension, activation and revocation or the failure to suspend, activate or revoke, or due to any reason beyond MANGO CA's control.

MANGO CA will have no legal responsibility to a Subscriber, occurring from or concerning issuance, management or use of an MANGO CA Digital Certificate that is issued or sustained in confidence upon or as an outcome of any false or deceptive information provided by the Subscriber or any material lapse in any information provided by the Subscriber in connection with his/her request for MANGO CA Digital Certificate or otherwise.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, MANGO CA requires, Subscribers to indemnify MANGO CA for:

a) Deception or falsification of fact by the Subscriber on the Subscriber's Certificate Application,
b) The Subscriber's failure to guard 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,
c) Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made neglectfully or with intent to deceive any party, or
d) 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.

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, MANGO CA requires, Relying Parties to indemnify MANGO CA for:

a) The Relying Party's failure to act upon the obligations of a Relying Party,
b) The Relying Party's confidence on a certificate that is not reasonable under the circumstances, or
c) The Relying Party's failure to check the status of such certificate to find out if the certificate is expired or revoked

9.10 Term and Termination

9.10.1 Term

This CPS and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CPS as amended from time to time shall remain in force until it is replaced by a new version or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of Termination and Survival

The conditions and effect resulting from termination of this document will be communicated via the MANGO CA Repository (http://www.mangoca.com.bd/repository) upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual Notices and Communications With Participants

MANGO CA accepts notices related to this CPS by means of digitally signed messages or in paper form addressed to the locations specified in Section 2.2 of this CPS. Upon receipt of a valid, digitally signed acknowledgment of receipt from MANGO CA , the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the street address specified in Section 2.2.

9.12 Amendments

9.12.1 Procedure for Amendment

The following bodies will verify MANGO CPS approval procedure and must sanction MANGO CPS for use within MANGO CA.

- MANGO CA Policy Approval Committee
- MANGO CA Legal Department

However, the final approval to the CPS will be made by the Controller of Certifying Authorities, Ministry of Information and Communication Technology, Government of the People's Republic of Bangladesh.

Policy Approval Committee decides on the changes in this CPS and the corresponding procedural adjustments to be made. Substantial changes will require revision of this policy. It is at the discretion of MANGO CA to determine the changes required if any, and whether a change is minor or substantial. In the case of major changes all the entities would be informed.

Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates shall be published in the MANGO CA Repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS.

9.12.2 Items that can change without notification

MANGO CA reserves the right to amend the CPS devoid of notification for amendments that are not material, including without restraint corrections of typographical errors, changes to URLs, and changes to contact information. MANGO CA's decision to designate amendments as material or non-material shall be within MANGO CA's solitary prudence.

9.12.3 Changes with notification

MANGO CA shall make material amendments to the CPS in accordance with this section.

9.12.4 List of items

Material amendments are those changes that MANGO CA considers to be material.

a) Any item in this certificate policy statement may be changed with 45 days' notice.
b) Changes to items which, in the judgment of the policy administration organization, will not materially impact a substantial majority of the subscribers or relying parties using this policy may be changed with 15 days' notice.

9.12.5 Notification mechanism

MANGO CA's Policy Approval Committee will post amendments to MANGO CPS in the MANGO CA Repository.

9.12.6 Comment period

No Stipulation

9.12.7 Mechanism to handle comments

No Stipulation

9.12.8 Period for final change

No Stipulation

9.12.9 Items whose change requires a new policy

If a policy change is determined to have a material impact on a significant number of subscribers **and relying parties** of the policy, MANGO may, at its sole discretion, assign a new object identifier to the modified policy.

9.12.10 Notification Mechanism and Period

MANGO CA's Policy Approval Committee will post amendments to MANGO CPS in the MANGO CA Repository.

This CPS and any subsequent changes shall be made publicly available within seven days of approval.

9.12.11 Circumstances Under Which OID Must Be Changed

If a change in MANGO CA's Certification Practices is determined by the MANGO CA Policy Authority to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CPS will also contain a revised OID for that type of certificate.

9.13 Dispute Resolution Provisions

Dispute resolution between MANGO CA, the Subscribers, and the Relying parties will be as per the ICT Act 2006. Resolution of disputes should be overall governed by the ICT Act 2006, and will be referred to the CCA from time to time for arbitration. Any person found violating the principles and procedures mentioned in the MANGO CPS and any other procedures supplementing the operation of MANGO CA, will be punished according to the rules pertained in the ICT Act 2006.

In the event of any dispute or claim arising from the issue of a MANGO digital certificate, the complainant undertakes to notify MANGO in writing of the exact nature of the dispute and to follow

the MANGO complaint processing and dispute resolution policy and procedure available for examination at Mango CA Legal secsion .

9.14 Governing Law

In order to ensure uniform procedures and interpretation of all subscribers and relying parties, irrespective of their country of residence or nationality, the laws of Bangladesh shall govern the enforceability, construction, interpretation and validity of MANGO CSP.

The Information and Communication Technology Act, 2006 and IT (CA) Rule, 2010, by Government of the People's Republic of Bangladesh, and The Rules and Regulations for Certifying Authorities formulated by Controller of Certifying Authorities (CCA) under ICT division shall govern the enforceability, construction, interpretation, and validity of MANGO CPS, irrespective of the contract or other choice of legal provisions and without the requirement to establish a commercial nexus.

9.15 Compliance With Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CP/CPS the parties shall also take into account the international scope and application of the services and products of MANGO CA as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CP/CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.
Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS. If/when this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CPS and any other document that relate to MANGO CA, then the sections benefiting MANGO CA and preserving MANOG CA's best interests, at MANGO CA's sole determination, shall prevail and bind the
applicable parties.

9.16.2 Assignment

Parties to this CPS may not assign any of their rights or obligations under this CPS or applicable agreements without the written consent of MANGO CA.

9.16.3 Severability

To the extent permitted by applicable law, Subscriber Agreements, Agreements and Relying Party Agreements under the Mango CA shall contain severability, survival, merger, and notice clauses. A severability clause in an agreement prevents any determination of the invalidity or enforceability of a clause in the agreement from impairing the remainder of the agreement. A survival clause specifies the provisions of an agreement that will 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.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

MANGO CA reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CPS, no delay or omission by any party to exercise any right, remedy or power it has under this CPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CPS shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between MANGO CA and the parties to this CPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

MANGO accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, civil unrest, strikes, flood, epidemics, power or telecommunication services failure, fire, and other natural disasters; any provision of any applicable law, regulation or order; civil, government or military authority; the failure of any electrical communication or other system operated by any other party over which it has no control; or other similar causes beyond its reasonable control and without its fault or negligence.

9.17 Other Provisions

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CPS applies to. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

APPENDIX A - REGISTRATION, CERTIFICATION AND DELIVERY

The procedure which MANGO follows for registration, certificate generation, and certificate distribution is described below for each type of certificate issued. Please note that the precise registration process and types of information gathered can vary from that described below depending on the specific application and customer requirements. Additionally specific certificate policies and MANGO liability arrangements not described here may be drawn up under contract for individual customers.

Certificate Procedure:

INITIAL REGISTRATION

An application for a MANGOINDIVIDUAL / ORGANIZATION / GOVERNMENT / SSL Server Certificate must complete a MANGO Certificate Registration form. The certificate request form will vary depending upon the class of certificate (Class 1, 2, or 3) and type of End Entity (Individual / Company/ Government / Device etc.) and will be available on MANGO CA website.

The registration supporting documents are listed below but not limited to as the updated registration procedure is available on http://www.mangoca.com

Depending upon type of End Entity applicant, the following information needs to be provided during the registration process along with appropriate filled out application :

- Applicant's Name (Individual/ Company Name/ Organization name)
- Address
- Domain Name (if applicable)
- Certificate Signing Request generated on the Web server requiring the certificate (if applicable)

For Individuals

- Attested passport size photograph of the Applicant
- Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back)
- Valid Tax Identification Number or Birth Registration Number

For Public & Private Limited Companies (NOTARIZED or Attested by Gazetted officers copy required)

- Attested passport size photograph of the Applicant
- Certified true copy of Memorandum of Association & Article of Association duly signed or authenticated at each page by the Managing Director/Chairman
- Certified copy of company incorporation certificate
- Resolution of the Board of Directors for obtaining & operation of digital certificate, duly attested by the Managing Director or Chairman.
- List of Director's with name, father's name, mother's name, spouse's name, date of birth & signature (up-to-date) in letterhead pad of the company duly signed by the Chairman or Managing Director
- Valid Trade License

- Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory
- TIN certificate
- VAT registration certificate
- Certified copy of commencement of Business duly authenticated by the Chairman or Managing Director (in case of public limited company)

For Partnership Firms (Notarized copy or Attested by Gazetted officers required)

- 2 copies of attested Passport size photograph of the applicant.
- Valid Trade License
- Resolution signed by the partners to obtain & operate digital certificate.
- Notarized copy of partnership deed duly signed by all partners
- Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory
- TIN Certificate
- VAT registration certificate

For Proprietorship Firms

- 2 copies of attested Passport size photograph of the Applicant.
- Valid Trade License
- Proprietorship declaration in letterhead pad.
- Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Applicant
- TIN certificate
- VAT registration certificate

For Trust

- Two copies of attested passport size photograph of the Authorized Signatory
- Up to date list of members of the Trustee Board
- Certified copy of Deed of Trust
- Certified copy of the Resolution of the Trustee Board for obtaining & operation of digital signature.
- Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory

For Club/Society/School/College

- Two copies of attested passport size photograph of the Applicant
- Registration Certificate
- Certified true copy of Memorandum of Association & Article of Association duly attested by the Chairman/Secretary

- Resolution for obtaining & operation of the digital signature duly attested by the chairman/secretary.

- Up to date list of office Bearers/Governing Body/Managing Committee duly certified by the chairman/secretary.

- Passport/Commissioner certificate of signatory

- Copy of valid Passport (1 to 7 page) or Copy of National ID Card (front and back) of Authorized Signatory

During the registration process, it is a requirement for the applicant to accept a certificate subscriber agreement. This details the terms and conditions under which the certificate is being supplied including the subscriber's obligations.

IDENTIFICATION AND AUTHENTICATION

It is mandatory during the registration process for the individual or organization information provided to be verified by MANGO. Therefore the individual or organization will be asked to submit a number of documents to aid in the verification process. The documents may include the following:

- ✓ **Relevant document providing proof of address.**
- ✓ Relevant document providing proof of organization registration
- ✓ Relevant document providing proof of domain registration

MANGO may at its discretion take steps to verify the documentation received, for example it may:

- ✓ Verify domain details with the relevant Domain Registration Authority
- ✓ Verify National ID or Passport Record Details
- ✓ Contact management of the applicant organization to authenticate requests for certificates.
- ✓ Resolution of the Board of Directors for opening & operation of digital certificate, duly attested by the Managing Director or Chairman

The MANGO Registration Authority Administrator (RAA) will verify the information supplied and is the person with the final authority to permit a certificate application to proceed to completion.

REGISTRATION COMPLETION

All registration details provided and the Certificate Signing Request generated will be stored on the MANGO registration database as soon as they are received.

These details will remain on the registration database while any verification is being completed.

Following successful completion of the verification phase, the certificate request is flagged as ready for processing.

CERTIFICATE GENERATION

All successful certificate requests will be processed by the MANGO CA. The CA will apply to the certificate request:

- ✓ A unique serial number
- ✓ Mango CA's signature

CERTIFICATE DELIVERY

Following the certification process, the certificate may be distributed to the customer via one of the following media:

- ✓ Download over the Internet or
- ✓ CD or Floppy Disk or
- ✓ E-mail or
- ✓ Smart Card or E-Token or
- ✓ USB Dongle or
- ✓ Mobile PKI Token

The subscriber, end user or relying party should ensure that the certificate received was indeed issued by the MANGO CA by verifying the thumbprint of the issuing CA certificate against that published for the MANGO CA at http://cert.mangoca.com

APPENDIX B – CERTIFICATE PROFILE (SUBSCRIBER)

This appendix describes the various classes of digital certificate that MANGO issues, and the limitations on liability in respect of each of these. The profile of each digital certificate type is also detailed. Note that the specific details described in each certificate profile may vary in any implementation from those described below.

The Digital Certificates issued by Mango CA confirm to "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999".

B1. Basic Fields

At a minimum, Mango CA X.509 Certificates contain the basic fields and indicated prescribed values or value constraints in Table below:

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA256 RSA
Issuer Distinguished Name	
Country (C)	BD
Organization (O)	Mango Teleservices Limited
Organizational Unit (OU)	CA
Common Name (CN)	Mango CA
Validity	
Valid from	05 July 2011 10:14:08
Valid to	04 July 2012 10:14:08
Subject	
Country (C)	User Entry
Organization (O)	User Entry
Organizational Unit (OU)	User Entry
Common Name (CN)	User Entry
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	2048 bit RSA

B2. Basic Content Description

B2.1 Version

The version field in the certificate is V3, indicating X.509v3 certificates.

B2.2 Certificate extensions

The following extensions are minimum extensions provided for the certificates issued by Mango CA as per this CPS.

B2.2.1 Key usage

Where X.509 Version 3 Certificates are used, Mango CA populates the Key Usage extension for the specific usage of the Digital Certificates.

The CA shall contain a key usage extension with **KeyCertSign**, **CRLSign** and **Digital Signature**. The criticality field of this extension shall be set to TRUE. All the End Entity certificates shall contain the following extension set as per the type of certificate.

- S/MIME (signing): This type of Certificate shall contain the key usage extension with Digital Signature, Non-repudiation and the extended key usage will have email protection (Secure Email).
- S/MIME (encryption): This type of Certificate shall contain the key usage extension with Key Encipherment and the extended key usage will have email protection (Secure Email).
- SSL Server: This type of Certificate will contain the key usage extension with Digital Signature and Key Encipherment. The extended key usage will have Server Authentication and Client Authentication.
- SSL Client: This type of Certificate will contain the key usage extension with Digital Signature and Non-repudiation. The extended key usage will have Client Authentication
- Object Signing: This type of Certificate will contain the key usage extension with Non-Repudiation, Digital Signature, and the extended key usage will have code signing.

B2.2.2 Certificate policies extension

No Stipulation.

B2.2.3 Subject alternative names

No Stipulation.

B2.2.4 Basic constraints

Mango CA populates X.509 Version 3 CA Certificates with a Basic Constraints extension with the Subject Type set to CA. End-user Subscriber Certificates are also populated with a Basic Constraints extension with the Subject Type equal to End Entity.

Mango CA X.509 Version 3 Certificates issued will have a Path Length Constraint field of the Basic Constraints extension set to the maximum number of CA certificates that may follow this Certificate in a certification path. This field is set to “None”. The critical field of these extensions shall be set to TRUE.

B2.2.5 Enhanced key usage

Mango CA makes use of the Enhanced Key Usage extension for the specific types of X.509 Version 3 Certificates. The value of Object Identifier for the purpose for the certificate to be used is mentioned in this field.

B2.2.6 CRL distribution point

Mango CA X.509 Version 3 Certificates use the CRL Distribution Points extension containing the URL of the location where a Relying Party can obtain a CRL to check the Mango CA Certificate’s status.

B2.2.7 Authority key identifier

No Stipulation.

B2.2.8 Subject key identifier

Where Mango CA populates X.509 Version 3 Certificates with a Subject Key Identifier extension, the Key Identifier based on the public key of the Subject of the Certificate is generated.

B2.3 Algorithm Identifiers

The following hashing/digest algorithms are supported:

- Secure Hash Algorithm-256
- Message Digest 5 (MD5)

The following padding algorithms are supported:

- PKCS# 1
- PKCS# 5

Encryption algorithms are classified into two classes, symmetric and asymmetric. The symmetric encryption algorithms being supported are:

- DES
- Triple DES

The asymmetric encryption algorithms being supported are:

- RSA
- DSA

B2.4 Name forms

Name fields and extensions shall be consistent with section 3.2

B2.4 Name constraints

Anonymous and pseudo names are not supported.

B3. Server SSL Certificate Profile Details

Server SSL Certificate Profile Details

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA256 with RSA Signature
Issuer Distinguished Name	
Country (C)	BD
Organization (O)	Mango Teleservices Limited
Organizational Unit (OU)	CA
Common Name (CN)	Mango CA
Validity	
Valid from	05 July 2011 10:14:08
Valid to	04 July 2012 10:14:08
Subject	

Country (C)	User Entry
Organization (O)	User Entry
Organizational Unit (OU)	User Entry
Common Name (CN)	User Entry
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	2048 bit RSA
Key Usage	
Digital Signature	Selected
Non Repudiation	Selected
Key Encipherment	Selected
Data Encipherment	Selected
Key Agreement	Selected
Key Certificate Signature	Selected
CRL Signature	Selected
Extended Key Usage	
2.2.1 Server Authentication	Selected
Certificate Policies	
Policy Identifier OID	2.16.50.1.8.1
Policy Notice	User Notice or CPS
Policy Qualifier	http://mangoca.com/download/cps.aspx

APPENDIX C - CERTIFICATE PROFILE (CA)

This appendix details the profiles of the MANGO CA certificates.

CA Certificate Profile Details

Corresponds to the key used to sign all certificates issued by MANGO to subscribers and end users.

Field	Content
1. X.509v1 Field	
1.1. Version	v3
1.2. Serial Number	Allocated automatically by issuing CA
1.3. Signature Algorithm	SHA256 with RSA Signature
1.4. Issuer Distinguished Name	
1.4.1. Country (C)	BD
1.4.2. Organization (O)	Mango Teleservices Limited
1.4.3. Organizational Unit (OU)	CA
1.4.4. Common Name (CN)	Mango CA
1.5. Validity	
1.5.1. Not Before	05 July 2011 10:14:08
1.5.2. Not After	05 July 2016 10:12:33
1.6. Subject	
1.6.1. Country (C)	User Entry
1.6.2. Organization (O)	User Entry
1.6.3. Organizational Unit (OU)	User Entry
1.6.4. Common Name (CN)	User Entry
1.7. Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
2. X.509v3 Key Details and Extensions	
2.1. Key Size & Algorithm	2048 bit RSA
2.2. Key Usage	

2.2.1. Digital Signature	Selected
2.2.2. Non Repudiation	Selected
2.2.3. Data Encipherement	Selected
2.2.4. Key Agreement	Selected
2.2.5. Key Certificate Signing	Selected
2.2.6. Off-line CRL Signing	Selected
2.2.7. CRL Signing	Selected
2.3. Certificate Policies	
2.3.1. Policy Identifier OID	2.16.50.1.8.1
2.3.2. Policy Notice	User Notice or CPS
2.3.3. Policy Qualifier	http://mangoca.com/download/cps.aspx
2.4. Basic Constraints	
2.4.1. Subject Type	CA
2.4.2. Path Length Constraint	3

APPENDIX D - CRL PROFILE DETAILS

D1. CRL Profile Basic Fields

The CRL issued by Mango CA confirm to "RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999". At a minimum, MANGO CA X.509 CRL contains the basic fields and indicated prescribed values or value constraints in Table below:

Field	Value or Value Constraint
Version	X.509 CRL version 2
Signature Algorithm	Algorithm used to sign the CRL. Mango CA CRL is signed using md5RSA in accordance with RFC 2459.
Issuer	Entity that has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in section 3.2.1.
Effective Date	Issue date of the CRL. MANGO CA CRL is effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of section 4.4.4.
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date.

D2. CRL Profile

Version: (version 2)
Effective Date:
Issuer:
Next Update:
Revoked Certificates
{
    User Certificate (Serial Number)
    Revocation Date
    Reason Code
    {
        Unspecified
        Key Compromise
        CA Compromise
        Affiliation Changed
        Superseded
        Cessation of Operation
        Certificate Hold
        Remove from Certificate Revocation List
    }
}
Signature Algorithm: (Algorithm Identifier)
Authority Key Identifier
Signature Value

APPENDIX E – ARCHITECTURE STANDARDS

MANGO CA follows following architecture standards and these may change as prescribed by the CCA from time to time.

The Product	The Standard
Public Key Infrastructure	PKIX
Digital Signature Certificates and Digital Signature revocation list	X.509. version 3 certificates as specified in ITU RFC 1422
Directory (DAP and LDAP)	X500 for publication of certificates and Certification Revocation Lists (CRLs)
Database Management Operations	Use of generic SQL
Public Key algorithm	RSA
Digital Hash Function	SHA256
RSA Public Key Technology	PKCS#1 RSA Encryption Standard (512,1024, 2048 bit) PKCS#5 Password Based Encryption Standard PKCS#7 Cryptographic Message Syntax standard PKCS#8 Private Key Information Syntax standard PKCS#9 Selected Attribute Types PKCS#10 RSA Certification Request PKCS#12 Portable format for storing/transporting a user's private keys and certificates
Distinguished name	X.520
Digital Encryption and Digital Signature	PKCS#7
Digital Signature Request Format	PKCS#10

APPENDIX F – CERTIFICATE STANDARD

All Electronic Signature Certificates issued by the MANGO CA Certifying Authorities shall conform to ITU **X.509 version 3** (or above) standard or similar standards and shall at a minimum contain the following data, namely:-

(a) **Unique Serial Number**, which is assigned by Certifying Authority in the Electronic Signature Certificate in order to distinguish it from other certificate;

(b**) Information for authentication of the algorithm process** used to compute signature, which is used by the Certifying Authority for authentication of the process of computing signature for signing an Electronic Signature Certificate;

(c) **Name of the issuer**, which shall include the name of the Certifying Authority;

(d) **Validity period** of the Electronic Signature Certificate;

(e) **Name of the subscriber**, which can authenticate the public key in the Certificate; and

(f) **Public Key information** of the subscriber.

APPENDIX G – CLASSES OF CERTIFICATE

MANGO CA supports four distinct certificate classes within its Certification services. MANGO CA reserves the right to introduce more classes than what has been specified herein and this CPS shall be appropriately amended as and when such classes are introduced. Each class provides for designated level of trust. The following subsections describe each certificate class.

G1. Class 0 Certificate

Test Certificate only

G2. Class 1 Certificate

Class 1 Certificate	
Subscriber	Class 1 certificates shall be issued to individual subscribers only.
Usage	It will authenticate an email address to its associated name or alias within the CA database. Can be used only with digitally signed email application
Subscription procedure	In case of online or offline certificate request for Class 1 Certificate, the applicant/subscriber submits online or paper application form to MANGO CA. MANGO CA verifies the name, e-mail address, and the postal address in the request. MANGO CA has the right to reject the certificate request if it finds the application is not meeting the criteria.
Physical presence	Physical presence may or may not be required, Mango CA would decide on case to case basis.
Validity	The validity period of Class 1 Certificates is one year.
Assurance level	The verification of the certificate request of this class represent a simple check of the certainty of the subject name within the MANGO CA repository, plus a limited verification of the address, other personal information and e-mail address.

G3. Class 2 Certificate

Class 2 Certificate	
Subscriber	Class 2 certificates are issued to individual or enterprise subscribers (sub class)
Usage	It will authenticate an email address or other digitally signed files & forms to its signature provider's associated name within the CA database. Can be used for digitally signed email application, file or form signing, client authentication, secure email, transactions or other applications.
Subscription procedure	In case of online/offline certificate request for Class 2 Certificate, the applicant/subscriber submits appropriate online or paper application form and required documents to MANGO CA. MANGO CA verifies the name, e- mail address, supporting documents and the postal address in the request. MANGO CA has the right to reject the certificate request if it finds the application is not meeting the criteria.
Physical presence	Physical presence may or may not be required, Mango CA would decide on case to case basis.
Validity	The validity period of Class 2 Certificates is one year.
Assurance level	Class 2 certificates are appropriate for digital signatures and encryption where assurance level is medium.

G4. Class 3 Certificate

Class 3 Certificate	
Subscriber	Class 3 Certificates are issued to Individuals Enterprises and Servers (sub class)
Usage	Can be used for email, files, forms signing, VPN, Client Authentication or other application, SSL server authentication or similar services & applications

	or for Code Signing or Time Stamping for various applications.
Subscription procedure	In case of online/offline certificate request for Class 3 Certificate, the applicant/subscriber submits appropriate online or paper application form and required documents to MANGO CA. MANGO CA verifies the name, e- mail address, supporting documents and the postal address in the request. MANGO CA has the right to reject the certificate request if it finds the application is not meeting the criteria The private key corresponding to the public key contained in a Class 3 certificate must be generated and stored in a trustworthy manner according to applicable requirements.
Physical presence	Physical presence may or may not be required, Mango CA would decide on case to case basis. In case of server sub class, along with the application form the authorized person must give the domain name or the Server IP address on which it needs the Certificate. The domain name must be registered and the proof must also be accompanied with the application.
Validity	Class 3 certificates are issued for one year.
Assurance level	Class 3 certificates are appropriate for digital signatures and encryption requiring a high assurance about the subscriber's identity

n

APPENDIX H – OCSP Profile

OCSP requests and responses shall be in accordance with RFC 2560 as listed below.

OCSP Request Format

Requests sent to Issuer PKI OCSP Responders are not required to be signed, but may be at the discretion of the Issuer PKI. See RFC2560 for detailed syntax. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

OCSP Response Format

See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	**Value**
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response will contain certificate id; certificate status[1], thisUpdate, nextUpdate[2],
Responder Signature	Sha256WithRSAEncryption {1 2 840 113549 1 1 5} or sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable certificates issued to the OCSP Responder
Response Extension	**Value**
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**
None	None

1. If the certificate is revoked, the OCSP Responder shall provide revocation time and revocation reason from CRL entry and CRL entry extension.
2. The OCSP Responder shall use thisUpdate and nextUpdate from CA CRL.

REFERENCES

IT (CA) Rules 2010 (Working Draft)

Final CA-application-Of-Mango and CPS

[ABA] American Bar Association, Section of Science & Technology, *Digital Signature Guidelines* (1996) (hereinafter ABA Guidelines). For information on ordering, see: http://www.abanet.org/scitech/home.html.

[FIPS] U.S. Department of Commerce, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication FIPS PUB 140-1, 1994. Available at: http://csrc.nist.gov.

[CHO] S. Chokhani and W. Ford, "Certificate Policy and Certification Practice Statement Framework," Internet Draft <draft-ietf-pkix-ipki-part4-00.txt>.

[HOU] R. Housley, W. Ford, T. Polk, D. Solo, *Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile*, Internet Draft: draft-ietf-pkix-ipki-part1-04.txt, 03/26/1997.

[TCSEC] U.S. Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, National Computer Security Center, Fort Meade, MD, December 1985. Available at http://www.disa.mil/MLS/info/orange/intro.html; http://csrc.nist.gov/secpubs/rainbow/std001.txt.

[TSDM] U.S. Department of Defense, "Trusted Software Methodology," Volume 1, SDI-S-SD-91-000007, Department of Defense, Strategic Defense Initiative Organisation, 17 June 1992.

[X509] ISO/IEC 9594-8, *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*. Also published as ITU-T X.509 Recommendation. For X.509 v3 certificates, see edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied.