eMudhra CPS

eMudhra CERTIFICATION PRACTICE STATEMENT

VERSION 2.6
(eMudhra/DOC/CPS/2.6)

Date of Publication: 24th February, 2016

eMudhra CA – Mauritius Operations

Email: info@eMudhra.mu
Website: www.eMudhra.mu

eMudhra CA CERTIFICATION PRACTICE STATEMENT

Document Name	eMudhra/DOC/CPS/2.6
Release	Version 2. 6
Status	Release
Issue Date	24th February, 2016
CCA Approval Date	

Revision History

Version	Section	Change
2.4	3.1.8 Authentication of Identity	Added identity verification of individuals of Foreign origin or residing in Foreign countries.
2.4	3.1.10 Validation of Documents	Added details for validation documents for identity verification of individuals of Foreign origin or residing in Foreign countries.
2.5	1.8.3 eMudhra eProcurement	Newly added section to incorporate new class under eMudhra Mauritius PKI hierarchy.
2.5	3.1.8.3 eProcurement Certificate	Newly added section to highlight the process of certificate issuance for eProcurment Class.
2.5	3.1.9 Verification of Documents	Minor modification to incorporate new class of certificate.
2.5	4.2.1 Issuance of End-user Subscriber Certificate	Minor modification to incorporate new class of certificate.
2.5	6.3.3 Root Certificate and Trust Chain Validation	Newly added section to highlight the importance of root certificate installation.
2.6	All sections	Renamed the General Class to Class 3, eProcurement Class to Class 2 and eFiling Class to Class 1. Also changed the “Relying party agreement” to “Relying party terms and conditions”
2.6	1.8	Added table to provide differentiation between various classes of digital certificate
2.6	1.8.1 -1.8.4	Modified to accept individuals and organisations for Class 3 and Class 2.
2.6	3.1.8.1 – 3.1.8.3	Changed the verification guideline appropriately to reflect the classification of certificates
2.6	3.1.9	Added “In-person verification or video verification will be performed to confirm the physical presence of the individual” in Class 3 validation procedure.

NOTICE

Any person who uses the digital certificate in an improper manner or violate the provisions detailed under this eMudhra CA Certification Practice statement shall render himself/herself liable for civil/criminal action and be proceeded against as per the provisions of applicable civil/criminal laws and ETA or any other act/acts that are relevant and in force from time to time.

DEFINITIONS

The following definitions are to be applied while reading this CPS. The following terms shall bear the meanings assigned to them hereunder and such definitions shall be applicable to both the singular and plural forms of such terms:

- "eMudhra" refers to the brand under which certification and trust services are offered by eMudhra CA. It comprises of eMudhra CA Certification Authority in India licensed by Controller of Certifying Authorities (CCA) under Information Technology Act, 2000 to issue digital signature certificates and also duly recognized by Controller of Certification Authorities (CCA), ICTA of Mauritius, as Foreign Certifying Authority, under Electronic Transactions Act 2000, Electronic Transactions (Certifying Authorities) Regulations 2010 to issue digital signature certificates in Mauritius. "eMudhra" is the brand owned by eMudhra Limited., a company incorporated under the Indian Companies Act, 1956 .
- "CA" refers to eMudhra Certification Authority recognized by CCA, Mauritius to issue digital signature certificate.
- Unless otherwise specified the word 'ACT' OR 'ETA' in this CPS refers to Electronic Transactions act 2000 and amendments there to made from time to time.
- "Applicant" means a person, entity or organization that has requested for a digital signature certificate.
- "User" or "Subscriber" means a person, entity or organization in whose name the Digital Signature Certificates have been issued by eMudhra CA.
- "Auditor" means an Auditor appointed by eMudhra CA for auditing its CA operations.
- "Digital Signature Certificate (DSC)" or "Certificate" refers to a digital signature certificate issued by eMudhra CA to the Applicant.
- "Controller" means the Controller of Certification Authorities, Mauritius
- Unless otherwise specified, the word CPS used throughout this document refers to Certification Practice Statement of eMudhra CA
- Private key is that part of the cryptographic key pair generated & held privately by the subscriber.
- "Persons" means Individuals and Individuals representing organizations in Mauritius
- "Local Agent" means an entity or organization which is a local agent of eMudhra CA under regulation 10 of the ETA (Regulations) 2010 and has the obligation to verify the credentials of the applicant or subscriber before approving the request for issuance, revocation, suspension or renewal of DSC. National Computer Board, located at 7th Floor, Stratton Court, La Poudriére Street, Port Louis, Mauritius will act as the Local Agent in the purview of this CPS.

Note: The contextual meaning of the terms may be considered for such terms that are used but not defined.

EXECUTIVE SUMMARY OF eMudhra CPS

This Certification Practice Statement (CPS) describes the practices followed with regard to the lifecycle management of the Certificates issued to Persons in Mauritius by eMudhra CA .

a. eMudhra Certification and Trust Services

eMudhra CA business objectives are:

- To enable consumers to manage their financial and statutory obligations and need through technology enabled process and by changing the way they have been transacting.
- To empower consumers by aiding with secured technology that will help them achieve safe and secured digital transactions.

eMudhra DSC consumers in India use DSC to transact over the internet in a secured way. Digital Signature protected online transaction concept is relatively new and with Digital Signature Certificates consumers will be comfortable to transact online in respect of any financial or e-commerce transactions.

This Certification Practice Statement (CPS) describes the practices followed with regard to the lifecycle management of the Certificates issued by eMudhra CA and recognized in Mauritius.

b. Rights and Obligations

By applying for a certificate to be issued by eMudhra CA , the applicant accepts and agrees to abide by this CPS and to all who reasonably rely on the information contained in the certificate that, at the time of acceptance and throughout the validity period of the certificate, until notified otherwise by the certificate owner, of the following points:

a. The information submitted by the certificate applicant to eMudhra CA and included in the certificate is considered to be true and accurate as submitted by the applicant.
b. No other person has ever had access to subscriber's private key.

By accepting the certificate, the subscriber agrees to retain the control of his private key, and to make use of his certificates in a trustworthy system, and to take necessary precautionary measures to prevent its loss, disclosure, modification or unauthorized use. When there has been theft, tampering, loss, compromise of his private key, the user must request eMudhra to revoke his certificate.

The subscriber also accepts that the data provided by him / her in the application or supporting documents are correct irrespective of whether verified or not by Local Agent.

c. Liability

Without limiting subscriber's obligations stated in this CPS, subscribers are liable for any misrepresentation they make in the digital signature certificates and on which third parties reasonably rely believing the same to be true.

For more information visit,
www.eMudhra.mu
Or contact: info@eMudhra.mu

LIST OF ACRONYMS AND ABBREVIATIONS USED IN THIS CPS

Acronym	Term
ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation.1
CA	Certification Authority
CCA	Controller Of Certification Authorities, Mauritius
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DSC	Digital Signature Certificates
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol With SSL
IETF	Internet Engineering Task Force
ITU	International Telecommunications Union
LA	Local Agent
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Directory Interchange Format
MCAP	Mauritius Certification Authority Partner
NRDC	National Repository Of Digital Signature Certificates
OID	Object Identifier
PAC	Policy Approval Committee
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PUK	PIN Unlock Key
RA	Registration Authority
RFC	Request For Comment
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URI	Uniform Resource Indicator
URL	Uniform Resource Locator
VPN	Virtual Private Network

Table of Contents

INTENTIONALLY LEFT BLANK

1. INTRODUCTION

This Certification Practice Statement (CPS) details the practices that eMudhra CA adopts to provide Digital Signature Certificates and related services to Persons in Mauritius. The CPS is the principal practice statement governing the services provided by eMudhra CA and establishes conformity with the requirements of the Electronic Transactions Act – 2000 (ETA) of Mauritius. The ETA provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents.

1.1 SERVICES OFFERED

eMudhra operates a PKI hierarchy to offer a range of 'Trust' services. The following services are being offered by eMudhra:

1.1.1 Certification Services

eMudhra offers Digital Signature Certificates to Persons or specific devices (web servers) based on the validation requirements specified by eMudhra. The certificates issued under this service can be used for digital signing, web server authentication, code signing, web form signing, efiling, online transaction and e-commerce.

1.1.2 OCSP (Online Certificate Status Protocol) Validation Services

eMudhra offers OCSP validation services to relying parties for certificate status verification in real time.

1.2 CERTIFCATION AUTHORITY

The term “Certification Authority” or CA as used in this CPS, represents eMudhra as the entity, recognized by the Controller of Certification Authorities (CCA), Mauritius and operated by it under the brand name of eMudhra.

eMudhra offers Certificates through their local agent in Mauritius.
The responsibilities related to the Certificates issued rests with:

- Local Agent with respect to collection, validation or verification of DSC requests for issuance or revocation and storage and management of subscriber documents or information management in Mauritius in adherence with local laws including Data protection Act.
- eMudhra CA for issuance or revocation of DSCs and maintenance of database of valid DSCs for verification by relying parties. These certificates will be managed from eMudhra’s CA facility hosted in India and licensed by the CCA Mauritius
- eMudhra CA with respect to security procedures in CA facility in India
- Local Agent with respect to security procedures in Mauritius towards storage and management of subscriber data in accordance with Local Laws including Data Protection Act

1.3 LOCAL AGENT

Local Agent (LA) is a local person or entity of Mauritius, appointed by eMudhra CA to carry out the role of Local Agent as detailed but not limited to below:

- to receive requests for issuance of DSCs from applicants and to evaluate, validate, verify and approve or reject the applications in accordance with this CPS.
- to ensure data confidentiality both digital as well as physical data in compliance with this CPS, ETA, Data Protection Act of Mauritius or any other local laws. This will also include acquiring necessary approvals or registration to comply with relevant statutory laws.
- to ensure security levels in storage of data, IT infrastructure, physical access and so on as is applicable to a CA in Mauritius.
- LA may carry out its operations through its representatives with the same levels of authority, responsibility and obligations as specified for LA.
- LA shall own the sole responsibility of its activities performed in Mauritius in the DSC issuance or revocation processes.

1.4 COMPONENTS OF eMudhra PUBLIC HIERARCHY

eMudhra public hierarchy consists of eMudhra CA (the CA certificate recognized by CCA). eMudhra CA in turn could create and sign various issuing CAs from time to time.

These issuing CAs shall be used to sign digital signature certificates to the subscribers.

Notes:

1. eMudhra may choose to have only a subset of the hierarchy and services mentioned based on commercial and operational considerations. The service and offerings mentioned above could be changed in the subsequent versions of the CPS.
2. eMudhra reserves the sole right to accept applications for its certificates and issue digital signature certificates. The validation and verification procedures for the Certificates will be as mentioned in this CPS and in accordance with the ETA to be strictly adhered by the LA.

1.5 ROLE OF CPS AND OTHER DOCUMENTS

This CPS explains specific practices of eMudhra with respect to issuance and management of the certificates.

Security and operational documents listed hereunder are in addition to the CPS:

- Technical Specifications of CA System: The principles which define eMudhra PKI security requirements and standards followed.
- IT Security Policy: Defines the guidelines covering the security implementation across various areas such as Physical, Key Operations, People etc. and also the audit requirements
- Operating Procedure Manuals: Sets the operations guidelines governing the PKI operations
- Key Ceremony Guide: Key Management Operations guidelines policy and manuals gives the detail procedure for carrying out various activities.
- Agreement documents including the Subscriber Agreement, Relying party terms and conditions and the LA agreement are the legal agreements that bind the various participants such as subscribers, Relying Parties, LA to eMudhra standards

eMudhra CA may rely on the ancillary documents as may be required in addition to the CPS for referring to any specific detailed standards.

1.6 RELATIONSHIP WITH CONTROLLER OF CERTIFICATION AUTHORITIES

The Controller of Certification Authorities, Mauritius has authorized eMudhra as a recognized Foreign Certification authority to issue Digital signature certificates for use in Mauritius.

1.7 COMPLIANCE WITH ET ACT

eMudhra CA complies with Electronic Transactions Act , Rules and Regulations. As required by ETA, this CPS conforms the adherence to framework provided in ITU RFC 1422 (X.509 version 3 certificates) in order to make interoperation easier for person who is intending to use eMudhra services.

1.8 POLICY OVERVIEW

In accordance to the guidelines of ETA, eMudhra proposes to issue following classes of certificates for use in Mauritius. The classes of digital certificates will be differentiated based on the parameters defined in the following table

	Class 1	Class 2	Class 3
Physical verification required	Not required	Not required	In-person verification or video verification required
Nationality supported	Only for Mauritius	Mauritius citizens and	Mauritius citizens and

for digital certificate issuance	Citizens	Foreign individuals	Foreign individuals
Certificate issued to Individual/Organisation	Individual only	Individual and Organisation	Individual and Organisation
Storage medium of private key	Soft token only	Soft or Hard token	Hard token only
Customer identity verification (KYC) conducted by	Regulated relying parties	CA	CA
Assurance level	Medium	Medium	High
Use cases	Digitally signing of application forms and other documents for Banks, Insurance companies, telecom companies and other registered entities	Filing and statutory returns with registrar of companies, revenue authorities, tax authorities, eProcurement etc	Online fund transfer, financial transactions and other high risk transactions

1.8.1 eMudhra Class 1 Digital Certificate

Customers – Class 1 certificates are issued to individuals including Foreign nationals.

Validation – Class 1 Certificates are issued to Applicants after validating the application information and such validation process is carried out as per section 3.1.8 and 3.1.9 of this CPS. Class 1 certificate issuance process relies on the regulated relying party's (like Banks, Telecom companies etc) procedures to obtain confirmation of the identity of individual applicants.

Class 1 certificates are appropriate for digital signing of documents including application forms, reports, letters and other communications with specific Relying Party or Relying Parties .

1.8.2 eMudhra Class 2 Digital Certificate

Customers – Class 2 certificates are issued to individuals and individual representing organisations including Foreign nationals.

Validation – Class 2 Certificates are issued to Applicants after validating the application information and such validation process is carried out as per section 3.1.8 and 3.1.9 of this CPS.

Class 2 certificates are appropriate for usage in any type of applications including eFiling of statutory forms, eProcurement etc.

1.8.3 eMudhra Class 3 Digital Certificate

Customers – Class 3 certificates are issued to individuals and individual representing organisations including Foreign nationals.

Validation – Class 3 Certificates are issued to Applicants after validating the application information and such validation process is carried out as per section 3.1.8 & 3.1.9 of this CPS.

Class 3 certificates are appropriate for authenticating and signing any online and mobile activities including online banking, ecommerce, electronic documents, contracts etc., .

Class 3 certificate issuance process makes use of various procedures to obtain strong confirmation of the identity of the applicants.

1.8.4 eMudhra Device Class

Customers - Device Class Certificates are applied for by authorized individuals (administrators) who are responsible for the security of the corresponding private keys and are appropriate for server authentication; message, software, and content integrity; and confidentiality encryption. Device certificates are used for Object signing and/or Secure Web Server.

Validation - The validation process is carried out as per section 3.1.8 & 3.1.9 of this CPS. The validation procedures for Device Certificates issued to devices are based on a confirmation that the subscriber organization does in fact exist, that the organization has authorized the certificate application, and that the person submitting the certificate application is authorized to do so.

Device certificate issuance processes make use of various procedures to obtain strong confirmation of the identity of the device.

1.8.5 Types of Certificates

eMudhra –can issue four types of certificates namely Signature, SSL Client, SSL Server, and Code Signing.

1.8.5.1 Signature Certificate

The signature certificate is corresponding to the signing private key. It will be used by individuals or organizations for signing purpose. The key pair will be generated by applicant/subscriber in a secure medium and is inherent to keep the private key in safe custody. The signature certificate is issued by eMudhra after the validation process mentioned in this CPS. The relying parties can make use of this certificate for signature verification.

1.8.5.2 SSL Client Certificate

SSL client certificates are used for the authentication of browser client by a secure server.

1.8.5.3 SSL Server Certificate

SSL server certificates are digital identifications containing information about web server and the organization that owns the server's web content. An SSL server certificate enables users to authenticate the server, check the validity of web content, and establish a secure connection.

1.8.5.4 Code Signing Certificate

Code signing certificate helps user to develop confidence in downloaded code. It allows users to identify the signer to determine if codes have been modified by someone other than the signer. Signed codes can be Java Applets, Javascripts, plugins, ActiveX controls of any other kind of code.

1. 9 IDENTIFICATION

This CPS is called eMudhra Certification Practice Statement. eMudhra CA manages the life-cycle of digital signature certificates under eMudhra, and the contact details are mentioned in section 1.11.2 of this CPS.

1.10 COMMUNITY AND APPLICABILITY

The community governed by this CPS is eMudhra Public Key Infrastructure (PKI) that accommodates a large, public community of users in Mauritius with diverse needs for communication and information security.

The parties involved in eMudhra PKI are:

1.10.1 Certification Authority and Hierarchy

The term Certification Authority refers to all entities signing certificates in accordance with eMudhra PKI hierarchy pertaining for each class of certificates, as mentioned under section 1.4 of this CPS.

1.10.2 Local Agent

A Local Agent ("LA") is refered an entity who have signed an agreement with eMudhra CA under the requirements of Section 10 of ETA regulations to receive the applications from the applicant/subscriber and verify the details contained in the application. If the verification is successful, then the request is digitally signed and approved by LA. Such approved requests are sent to eMudhra, recommending to issue certificate Issuing CA under eMudhra PKI hierarchy.

National Computer Board, located at 7th Floor, Stratton Court, La Poudriére Street, Port Louis, Mauritius will act as the Local Agent in the purview of this CPS.

1.10.3 End Entities

The end entities / end users of the Digital signature certificates in business and other communication applications are:

Applicants - An applicant is a person, entity, or organization that has applied for, but has not yet been issued a eMudhra Digital signature certificate.

Subscribers - A Subscriber is a person, entity, or authorized representative of an organization that has been issued a eMudhra Digital Signature Certificate.

Relying parties – A Relying Party is a person, entity, or organization that relies on or uses eMudhra Digital signature certificates and/or any other information provided in eMudhra repository to verify the identity and public key of a subscriber and/or use such public key to send or receive encrypted communications to or from a subscriber.

eMudhra digital signature certificates are intended to support the security needs as mentioned in this CPS. eMudhra shall not be responsible for any liabilities howsoever or whatsoever arising from the use of any Certificate unless eMudhra has expressly undertaken to assume such liabilities in this CPS. More generally, certificates shall be used only in consistent with all applicable laws, rules and regulations and in particular shall be used only to the extent permitted by applicable laws and regulations, including laws relating to data transfer and export and import of goods and services.

1.11 CONTACT DETAILS

1.11.1 Specification Administration Organization

This CPS is administered by eMudhra CA. The CPS shall be revised from time to time as and when needed by the CA, upon approval from the CCA, with sufficient notification to the end users.

1.11.2 Contact Person

eMudhra can be contacted at the following address.

eMudhra CA,
3rd Floor, Sai Arcade,
Outer Ring Road,
Devarabeesanahalli,
Bangalore – 560103
Karnataka, India
Email: info@eMudhra.mu
Website: www.eMudhra.mu

For more information, refer to eMudhra's website at www.eMudhra.mu or contact administrator at info@eMudhra.mu.

1.11.3 Person Determining CPS Suitability for the Policy

The suitability of the CPS is determined by a committee designated by eMudhra CA. However any versions of this CPS can be adopted only after the CCA approval

2. GENERAL PROVISIONS

The responsibilities of various parties, participating in the eMudhra PKI as established by this CPS has been defined in this section. The obligations of various parties have been detailed.
The provisions of the Data Protection Act shall act as a contractual guideline and standard until proclamation of the same, and shall be mandatory upon proclamation.

2.1 OBLIGATIONS

2.1.1 CA Obligations

The CPS specifies obligations for eMudhra CA throughout this document.

Broadly the eMudhra CA shall have the following obligations:

- performing activities as per the policies, procedures and processes as designed to secure the certificate management process including certificate issuance, suspension, activation, revocation, CRL publication and audit trails
- to protect its private key from compromise.
- Issuing a Digital Signature Certificate to the applicants whose applications have been verified / validated and approved for DSC issuance by the Local Agent.
- Creating and maintaining audit trail of all CA operations.

In addition eMudhra CA will make reasonable efforts to bind the subscriber, Local Agent and relying party through the Subscriber Agreements, LA agreement and the Relying party terms and conditionsterms and conditions. Subscriber will not be enrolled or issued a certificate without consent/ agreement to the standard Subscriber Agreement published in the eMudhra Mauritius website. Relying party terms and conditions

2.1.2 Local Agent obligations

- To Maintain the CCA approved CPS with previous versions / revisions as and when changes are made and Implement the practices described in this CPS.
- To receive applications for DSC Issuances. Collect, Verify and validate the application forms and relevant supporting documents provided by the applicant as per the identity verification methods specified in this CPS and approve for issuance or rejection.
- Storing of the customer data including the physical application forms and supporting documents as a custodian of eMudhra CA with high levels of security as required by law for the period specified under ETA Regulations.
- Processing revocation or renewal of the Digital Signature Certificate upon the request from the subscriber as per the terms and conditions in eMudhra CPS.
- Ensuring that all requirements, representations, warranties as mentioned in this CPS are adhered to when performing the Certificate issuance operations and CA services.
- Creating and maintaining various records and related audit trails of various transactions
- Ensuring full compliance with all the local laws and regulations of Mauritius and amendments thereof, including but not limited to “ETA”, “ICTA” and “Data Protection Act”.

2.1.3 Subscriber Obligations

The Subscriber shall have the following obligations:

- To ensure that the information / data provided in the application for certificate request is true, accurate, current and without errors, omissions or misrepresentations.
- Use secure medium as specified in the eMudhra CPS to generate the key pair and use the certificate for authorized purposes consistent with this CPS.

- To protect the generated private key in a trustworthy, secure medium.
- To keep the private key safe and protect it from any disclosure or unintended use
- Notify eMudhra immediately when the information included in the Subscriber's Digital Signature Certificate is inaccurate, false or incomplete.
- Notify eMudhra immediately upon any actual or suspected compromise of the Subscriber's private key.
- Comply with any other additional obligations as mentioned in the Subscriber agreement.
- .
- Read and accept the policies and procedures as specified in this CPS.

2.1.4 Relying Party Obligations

Relying Party obligations apply to Relying Parties by way of eMudhra CA Relying party terms and conditionsterms and conditions.

- Relying Parties must independently assess the appropriateness of the use of a Digital signature certificate for any given purpose.
- Relying parties must use appropriate utilities or tools to perform digital signature verification or other operations. The utilities/ tools should be able to identify the certificate chain and verifying the digital signature on all certificates in the chain and only on successful verification should rely on the certificate.
- Relying parties are deemed to have read, understood and consented to the "Relying Party Terms and Conditions" published in the eMudhra Mauritius website.Relying party terms and conditions
- The relying parties have to determine the appropriateness of the use of a certificate. The terms and conditions states that eMudhra CAs and Local Agent are not responsible for assessing the appropriateness of the use of a Certificate.

2.1.5 Repository obligations

eMudhra CA is responsible for the repository functions for all eMudhra CAs in its PKI hierarchy. eMudhra CA shall publish the Certificates issued by it in its repository which shall be updated whenever there is any change in any of them including revocations. Every week the CRLs shall be published and updated in eMudhra Repository

2.2 LIABILITY

2.2.1 Certification Authority Liability

eMudhra CA provides the service on reasonable effort basis.

- The security and suitability of the service will not be guaranteed by eMudhra CA. eMudhra CA shall not be liable for delay or omission to issue a digital certificate or any other consequences arising from events beyond the control of eMudhra CA.
- eMudhra CA shall not be liable for any damages arising from its operations or use of certificates it issues.
- eMudhra CA shall not be liable, for any certificates (especially the identity validation of certain class of digital certificates specified in Section 1.8) obtained from it by false representation, or inaccurate, misleading or untrue information
- eMudhra CA shall not be liable for the lapses in the obligations specified in this CPS of the Local Agent

All warranties and any disclaimers thereof, and any limitations of liability among eMudhra CA, its Intermediaries (Resellers/ Local Agent) and their respective customers shall be in strict adherence to the terms and conditions of the Agreement amongst them.

2.2.1.1 Warranties to Subscribers and Relying Parties

eMudhra's Subscriber Agreements and that issued by the intermediaries (resellers, Local Agent etc.) shall include, a warranty to subscribers that:

- No information is materially misrepresented or introduced in the certificate by the entities approving the certificate application or issuing the certificate.
- The entities issuing and approving certificates have exercised reasonable care in managing the application and creating the certificate and no errors exist in the information in the certificates that was introduced by these entities.
- The certificates conform to certificate management requirements such as revocation services, use of a repository and other material requirements as laid down in the CPS.

Similarly eMudhra's Relying party terms and conditions contain a warranty to relying parties that:

- Information in or incorporated by reference in Digital Signature Certificate, except non verified subscriber Information, is accurate as provided by the subscriber
- The requirements of this CPS have been complied with while issuing the certificate.

2.2.1.2 Disclaimers of Warranties

eMudhra CA and other Subscriber agreements along with the relying party terms and conditions, expressly disclaims, within lawfully permissible limits, all warranties including warranty of merchantability or fitness for a particular purpose.

2.2.1.3 Limitations of liability

The verification for certificate issuance by eMudhra is based on reasonable effort basis and neither eMudhra CA nor local agent can underwrite the activities or conduct of the subscribers.

- eMudhra CA shall not be liable for any indirect, exemplary, special, punitive, incidental, and consequential losses, damages, claims, liabilities, charges, costs, expenses or injuries (including without limitation loss of use, data, revenue, profits, business and for any claims of Subscribers or Users or partners or Local Agent other third parties including Relying parties).
- eMudhra CA shall not be liable for any delay, default, failure, breach of its obligations under the Subscribers Agreement, Relying party terms and conditions and Local Agent Agreement

2.2.1.4 CA Liability Caps

Notwithstanding anything contained, the maximum aggregate liability of eMudhra CA towards all parties including the Relying Party (whether in contract, tort or otherwise) and subscribers shall under no circumstances exceed the amount realized by eMudhra for issuance of the concerned certificate. The amount shall not exceed MUR 3000 per certificate.

2.2.1.5 Force Majeure

To the extent permitted by applicable law, eMudhra CA's subscriber agreements, Local Agent agreement and Relying party terms and conditions include, and other subscriber agreements

shall be subject to the conditions of force majeure clause. eMudhra CA, Local Agent and Relying party shall not be responsible for any delay/default/inadequate performance/ non-performance / failure in their performance under the Subscribers Agreement, Relying party terms and conditions or Local Agent Agreement if the same is caused by Force Majeure circumstances like extraordinary weather conditions or other natural catastrophes, acts of god, war, riots, strikes, lockouts or other industrial disturbances, or acts of any governmental agencies.

2.2.2 Local Agent Liability

The obligations and the liabilities of the Local Agent including its warranties towards CA while assisting the CA in issuing certificates to the subscribers are more particularly set out in the Local Agent Agreement signed between the parties

2.2.3 Subscriber Warranties and Private Key Compromise

2.2.3.1 Subscriber Warranties

Subscriber agreement of eMudhra CA mandates its subscribers to warrant that:

- At the time of digital signature creation the certificate is valid and operational and not Expired or Revoked.
- The subscriber's private key was not disclosed and haven't been accessed by any third party.
- The Subscriber has only provided information in the certificate application which is true and accurate and is the same is contained in the certificate.
- The Private Key shall not be used for any unlawful and unauthorized transactions.
- The Digital certificate obtained by the end user subscriber is not used for digitally signing any issuing CA certificates, Certificates and CRL.

2.2.3.2 Private Key Compromise (PKC)

The subscriber shall be solely responsible for the protection of their designated private key. The end subscriber is required to take necessary precautions to ensure storage of the private keys and to protect against disclosure.

2.2.4 Relying Party Liability

All relying parties, who rely on the information provided in the Digital Signatures, under any Agreement, are required to make an informed decision based on the sufficiency of the information before them and eMudhra CA shall not guarantee or be liable for any decision so taken by a relying Party,

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification by Subscribers

eMudhra CA Subscriber Agreement mandates all its Subscribers to, within lawfully permissible limits; indemnify eMudhra CAs or Local Agent for:

- Any inaccurate, False or misrepresentation of information in the subscriber's certificate application, as provided by the subscriber.

- Suppression of a material fact on the certificate application, if the omission was made negligently or with intent to deceive any party,
- Failing to protect the private key of the subscriber and failure to use a trustworthy system or failing to take necessary precautions to,
- Failure to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key.
- Any infringement of IPR of a third party caused by the subscriber's use of name (or any other term not limiting to use of Common name, domain name, email address).

2.3.2 Indemnification by relying parties

eMudhra CA's relying party terms and conditions mandates all relying parties, to indemnify, within lawfully permissible limits, eMudhra CAs or Local Agent s for:

- Any failure by the Relying Party to perform the legal obligations of relying party as detailed in this CPS and
- For any failure by the relying party to check the status of the certificate (revoked or expired.)

2.3.3 Fiduciary Relationships

All eMudhra Subscriber Agreements and relying party terms and conditions disclaim, within lawful limits, any fiduciary relationship deemed to be existing between eMudhra CA or Local Agent on one side, and the Subscriber or Relying Party on the other.

2.3.4 Administrative Processes

eMudhra CA agrees that, during the subsistence of this Agreement, it shall have financial resources and infrastructure sufficient to perform the operations and duties thereof.

2.4 INTERPRETATION AND ENFORCEMENT

Notwithstanding anything to the contrary, this CPS shall be construed in accordance with the provisions of the ETA.

2.4.1 Governing Law

This CPS is governed by the ETA, rules, regulations and any amendments made to the Act from time to time.

2.4.2 Severability, Survival, Merger, Notice

It is hereby required under this CPS that all eMudhra CA Agreements (Subscribers, relying Party's, Local Agent's or otherwise) required to be entered into for the purposes mentioned herein, must contain clauses for severability, survival, notice and merger clauses for the following purposes:

- Severability: While interpreting the clauses of an Agreement which are severable from the rest, the invalidity of such clause shall not affect the validity of the other clauses of the agreement.
- Survival: While interpreting the clauses of an Agreement, certain specific clauses shall be deemed to survive the expiry or termination of the Agreement wherein such clauses are incorporated.
- Merger: while interpreting the clauses of an agreement it is deemed that all clauses that require understanding of the relationship between the parties and the purpose thereof are merged or provided in the Agreement.

Notice: The Agreements shall specify all the circumstances that require a notice to be provided by the Parties and where and to whom such notices shall be forwarded.

2.4.3 Dispute Resolution Procedures

2.4.3.1 Disputes among eMudhra CA /Local Agent

Disputes between eMudhra CA/Local Agent and one of its end users, subscribers or relying party shall be resolved according to dispute resolution clause in the respective agreements as approved by the CCA of Mauritius.

2.4.3.2 Disputes with End-User Subscribers or Relying Parties

Please refer section 2.4.3.1 of this CPS.

2.5 FEES

eMudhra CA is entitled to charge

- Subscribers fees for management and issuance of certificates
- Repository Access Fees for accessing the certificate information from the repository. The certificate search facility is provided through www.eMudhra.mu/repository/certs

Details of these fees will be available on the company's website at www.eMudhra.mu and will be updated from time to time.

eMudhra shall update and make available the CRL, free of charge for access by relying parties (www.eMudhra.mu/repository/crl). However any OCSP validation services as well as provision of OCSP services would be charged based on the specific agreement between the parties.

eMudhra will be providing access to policy information documents such as CPS free of charge (www.eMudhra.mu/repository/cps). This is however limited to the specific purpose of viewing. Any reproduction, derivative work creation, modification etc, would be subject to license agreement with eMudhra.

The refund policy and other payments terms would be governed as per the terms in the subscriber agreement. In case the application is rejected the full amount would be refunded to the subscriber.

The above terms and fee structure are subject to change at the sole discretion of eMudhra.

2.6 PUBLICATION AND REPOSITORY

eMudhra CA shall maintain an online repository of information relevant to the operations of PKI services under eMudhra hierarchy on best effort basis. The information in the eMudhra repository is subject to change and published periodically.

eMudhra reserves the right not to publish any information that eMudhra considers as confidential or not to be disclosed due to the sensitivity of the information

2.6.1 Publication of CA Information

The information published in eMudhra repository include

- eMudhra Certification Practice Statement.
- The Digital Signature Certificates issued under eMudhra hierarchy. The Digital Signature Certificates and public keys of eMudhra CA hierarchy.
- The Certification Revocation List of eMudhra hierarchy.
- Fee structures for the various services.
- Search facility for Digital Signature Certificates.

2.6.2 Frequency of Publication

eMudhra CPS and the CA certificate under eMudhra hierarchy shall be published as soon as they are updated and approved by CCA.
The CRL shall be published in the repository once in 7 days with validity of not more than 30 days

2.6.3 Access Control

The information published in eMudhra online repository is publicly accessible information and eMudhra CA provides read only access to the contents of the repository. eMudhra CA has in place sufficient safeguards and precaution to prevent any unauthorized access of repository entries.

2.7 COMPLIANCE AUDIT

As per the third schedule of the ETA (Certification Authority) regulations and its associated rules, regulations and amendments eMudhra would be subject to compliance audits.

2.7.1 Frequency of Audit

Compliance audits will be performed as deemed necessary by the ETA / CCA.

2.7.2 Auditors relationship to audited party

The Audit firm would be independent of eMudhra CA and will not have other business dealings with eMudhra CA.

2.7.3 Topics covered by Audit

The scope of audit will be as per ETA and its associated rules and regulations and will include security guidelines, licensing conditions, CPS and its adherence, regulation prescribed by controller and any other items deemed necessary by eMudhra CA

2.7.4 Actions taken as result of deficiency

Significant exceptions and non conformity as reported by the auditors will be reviewed by eMudhra CA Policy approval committee. If the exceptions are deemed to provide immediate risk to the security of the system corrective actions will be planned and implemented by eMudhra CA within a reasonable commercially viable time frame. eMudhra CA Policy approval committee will be responsible for remedial planning and implementation of a remedial measure.

2.7.5 Communication of results

Compliance Audit results of eMudhra CA, as per ETA shall be submitted to CCA Mauritius. eMudhra reserves the right to share the results to other parties as deemed fit.

2.8 CONFIDENTIALITY AND PRIVACY

2.8.1 Types of Information to be kept Confidential and Private

The following records of Subscribers are kept confidential and private ("Confidential/Private Information"):

- Information pertaining to digital signature certificate applications shall be kept confidential. Digital signature certificate information collected from the subscriber as part of registration and verification records but not included in the information contained in the Digital signature certificate shall also be kept confidential. Requirements of law pertaining to protection of personal and sensitive data shall be adhered to.
- Transactional records.
- Audit reports and any information that is considered sensitive shall be disclosed only to, and in strict adherence with, eMudhra CA authorized and trusted personnel and the CCA. The information thus obtained or disclosed shall not be used for any purpose other than as specified by law.
- Audit trail records created and or retained by eMudhra or a Customer.
- Contingency planning and disaster recovery plans.
- Security measures controlling the operations of eMudhra hardware and software and the administration of Certificate services and designated enrolment services.
- Any other records / data / information mandated to be kept confidential and private by the ETA, its associated rules and regulations and as deemed by eMudhra.

2.8.2 Types of information not considered confidential or private

The following shall not be considered as Confidential or Private Information: :

- Information included in the issued Digital signature certificate.
- Information included in the CRL.
- Information that is publicly available at the time of its disclosure; or
- Information that becomes publicly available by disclosure of third parties; or
- Information that is already known to or was in the possession of eMudhra prior to disclosure under Subscriber Agreement or Relying party terms and conditions or; or
- Information that is disclosed to eMudhra from a third party, which party is not bound by any obligation of confidentiality; or
- Information that is or has been independently developed by eMudhra without using the Confidential Information;
- Information that is disclosed with the prior consent of the disclosing party.
- Any subscriber specific information approved by subscriber for disclosure.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

eMudhra CA shall publish list of certificates that are Revoked / Suspended. The reason code of the revoked / suspended certificate shall not be confidential. Any other information related to revocation / suspension shall not be disclosed to anyone other than the subscriber or as required by law.

2.8.4 Release to Law Enforcement Officials

Any Confidential information may be released by eMudhra CA and its Local Agent to the courts or Tribunal or law enforcement agencies in accordance with applicable legal requirements.

2.8.5 Release as Part of Civil Discovery

eMudhra CA may also disclose any confidential information in response to Judicial or legal process, or in the course of any arbitration, litigation or judicial or quasi-judicial or mediation proceedings. In any such disclosure, eMudhra shall make reasonable efforts to restrict the disclosure of the information to the extent reasonably required by the proceedings.

2.8.6 Disclosure upon Owner's Request

All confidential Information of an owner shall not be disclosed by eMudhra under any circumstances, except when such confidential information is requested by the owner and the same shall be revealed to him upon such owner establishing the proof of identity to eMudhra.

2.8.7 Other Information Release Circumstances

The Exemptions provided in respect of disclosure of data set out in Part VII of the Data Protection Act shall also be treated as circumstances under which data may be disclosed by Local Agent / eMudhra CA.

2.9 INTELLECTUAL PROPERTY RIGHTS

2.9.1 Property Rights in Certificates and Revocation Information

All Intellectual Property Rights in and to the certificates and revocation information that is issued under eMudhra hierarchy, shall be the sole and exclusive property of eMudhra CA. eMudhra CA and customers grant permission to reproduce and distribute certificates as well as use revocation information to perform relying party function on a nonexclusive basis subject to the relying party terms and conditions referenced in the certificate and the applicable CRL usage agreement or any other agreements.

2.9.2 Property Rights in the CPS

All Intellectual Property Rights in and to this CPS, is recognized by the Participants including Subscribers, relying party, customers, and Local Agent , to vest absolutely and irrevocably in the custody of eMudhra CA.

2.9.3 Property Rights in Names

All rights subsisting in any trademark, service mark or trade name as provided for in any certificate application and all distinguished name(s) in the certificate issued to the certificate applicant shall vest with such certificate applicant.

2.9.4 Property Rights in Keys and Key Material

CA and the Subscriber shall retain all rights, including intellectual property rights, in the key Pairs corresponding to the certificate to which they are subject, irrespective of the medium where the key pairs may be stored or protected

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

The applicant shall submit the application online or offline along with the prescribed supporting documents.

3.1.1 Types of Names

All names issued by eMudhra CA, in the Digital signature certificates, shall confirm to the X.520 naming conventions. The Digital signature certificates issued by eMudhra shall use Distinguished Names (DN) to facilitate the identities to subscribers. Distinguished Name may comprise of the following fields.

- Common Name (CN): It is a unique name of the Subscriber as provided in the identity documents for the personal certificates and FQDN (fully qualified domain name) for the server certificate Organization
- (O). Name of the organization
- Organizational Unit (OU): to distinguish various organizational groups like department or sub-divisions within the same organization.
- City or Locality (L)
- State or Province (S),
- Country(C): the country to which the Subscriber belongs.

In addition to the above mentioned fields, eMudhra may include more fields in subscriber certificates to indicate issuing CA or any other details stipulated by CCA.

3.1.2 Need for names to be meaningful

The subject distinguished names in a certificate must be meaningful and must be able to determine the identity of the subject. Such name shall be generally accepted personal name for individuals and a fully qualified domain name for servers.

For certificates issued to devices the common name is either a domain name (for server Certificates) or the legal name of the organization, or a unit within the organization or any other name identifying the device and legally owned or assigned to the organization.
The name used for the organization may be legally owned or assigned to the organization or assigned to the organizational unit.

The organization name (O) attribute type, when present in the subject distinguished name, represents the legal name of the Subscriber organization.

3.1.3 Rules for Interpreting Various Name Forms

The names shall be interpreted as specified in the section 3.1.1 and 3.1.2 of this CPS. Uniqueness of an existing name can be enhanced forth by applying any numbers, characters or letters to it.

3.1.4 Uniqueness of Names

The Distinguished names form the basis for the uniqueness of each assigned name.
As specified in the CPS, the same Applicant/Subscriber can have multiple Digital signature certificates of different class or purpose.

In addition to the above, eMudhra Digital Signature certificate shall also have a unique serial number which enables identification, suspension, activation and revocation of the certificates issued

3.1.5 Name Claim Dispute Resolution Procedure

All disputes and claims arising with regard to names shall be settled as per the dispute resolution procedure mentioned in Section 2.4.3 of this CPS. In addition to above, all certificate applicants are prohibited from using names that infringe on the Intellectual Property Rights of others.

3.1.6 Recognition, Authentication, and Role of Trademarks

Any Trademark, upon satisfactory proof of ownership produced to eMudhra, shall be reserved by eMudhra to its registered owner

3.1.7 Method to prove possession of private key

The Private key corresponding to the Public Key displayed in the Digital Signature in the hand of the Certificate Subscriber shall be verified by eMudhra through the use of digitally signed certificate request pursuant to PKCS#10 or other cryptographically equivalent standard and any other demonstration approved by eMudhra.

3.1.8 Authentication of Identity

The responsibility for verifying the identity of the individual or authorized representative of the organization which has requested for the certificates will be as in 3.1.8.1, 3.1.8.2 and 3.1.8.3. On a best effort basis, the person responsible shall perform appropriate validation and/or verification based on the information provided in the application form and the supporting documents (as mentioned in section 3.1.9) in order to establish the identity of the individuals or authorized representatives of the organizations.

In cases where the applicant is a foreign national or Mauritian national residing in foreign country, the identity and document verification shall be done by a competent authority in the respective countries. The competent authorities can be any one of the following:

- Mauritian Embassy/High Commission in respective country (in case of Mauritian citizen residing in foreign country)
- The respective Embassy/High Commission in Mauritius (in case of Foreign national residing in Mauritius)
- Attorney
- Notary

In such cases, the application shall be certifiedby the competent authority which shall contain the competent authority's name, designation, contact address including telephone number and statement mentioning that he/she has verified the applicant's identity/document judiciously. The applicant shall apply online along with the prescribed forms/documents/details as mentioned in section 3.1.9 . After validation of the same, the digital signature certificate is issued.

An application for a certificate must be made

- personally by an individual in the case of individual certificates or,
- by the duly authorized representative of the organization in the case of organization certificates

For device certificates, in addition the customers will have to submit proof on existence of the servers/ devices and also proof that the organization has authorized the issuance of a secure ID to the devices.

The Local Agent would only send the Distinguished Name data which are required for certificate issuance to eMudhra. All other identification data of the subscribers would be retained and managed by the Local Agent and will not be shared or sent to eMudhra in accordance with the Data Protection Act.

3.1.8.1 Class 1 Certificate

The Local Agent would not perform any validation of the identification data of the subscribers for this class of certificates and would solely rely on the data provided by the regulated relying party and confirmed by the subscriber. The identification data as provided by the Relying Party system will be displayed to the subscribers for their confirmation after which digital certificate request will be approved for digital certificate issuance. The supporting documents for identification would not be obtained by the Local Agent. The regulated relying parties shall maintain supporting documents for the respective subscriber identification for each digital certificate request

3.1.8.2 Class 2 Certificate

The Local Agent will obtain the subscriber identification documents as prescribed in section 3.1.9 electronically and
would solely rely on the data provided and confirmed by the subscriber. The digital certificate will be issued based on the validation of identity proof produced by subscriber for which the Local Agent would approve for certificate issuance.

eMudhra warrants the relying parties who accepts the digital signature certificate issued under this class of certificate that the certificate is issued based on the details provided by applicant only and no physical verification is performed to confirm the identity of applicant. eMudhra is not responsible (which overrides the Limitation of Liability clause) to relying parties or any person who accepts the certificate for any misrepresentation of identity data, or fraud or any consequential financial loss.

3.1.8.3 Class 3 Certificate

For Class 3 Certificates, apart from the verification procedures indicated in section 3.1.8.2, the Local Agent will also perform a physical or video verification of the subscriber to confirm his/her identity and existence. The Class 3 certificates will only be issued on FIPS 140-2 level 2 and above certified hardware crypto device. Thus Class 3 certificates provide a high level of assurance.

3.1.8.4 Device Class Certificate

In addition to subscriber identification an additional Authority letter from the company will be required, where the certificate is intended to be used for Web form signing, User authentication, Code signing, VPN client purposes or for securing servers and VPN devices. Domain name shall be identified based on documentary proof from the relevant Registrar of Domains. Similarly for certificates for VPN devices, the proof of ownership of the VPN device shall be obtained from the certificate applicant.

3.1.9 Verification documents required

The verification documents required for digital signature certificate are available at www.eMudhra.mu/repository/validationdocuments.

Certificate	Verification documents required
Class 1 Certificate	Confirmation (electronic or paper) from the regulated Relying Party like Banks, Telecom Companies, Insurance Companies etc on the subscriber data information
Class 2 Certificate	Electronic submission of identity and address proof by the applicant as per the following document set: a. Attested photocopy of documents such as: Passport/Driving License/Citizen identification Number/Any document issued by a Government Agency b. Attested photocopy as address proof of documents such as : Latest telephone bill (landline or mobile)/Latest electricity bill/Insurance policy receipt / any other document issued by the Government agency c. Any other identification document as approved by the CCA d. In the case of authorized representatives of Organization, documents validating the identity of the organizations would also be required. These may include o Company Registration o Society Registration o Memorandum of Understanding o Article of Association o Documents pertaining to Commercial establishment o Bank details for a Current Account o Partnership Deed / Agreement etc o Trade Mark Registration Certificate, if any o Any other documents as specified in the CPS or by CCA. o Proof that the person representing the organization is duly authorized to do so, is also required In case of applicant residing in Foreign country or Foreign national residing in Mauritius, a certified copy of identity verification documents by a competent authority as mentioned in section 3.1.8 shall be accompanied along with the application. The certification shall contain the competent authority's name, designation, contact address with telephone number, applicants' name and time of verification.
Class 3 Certificate	a. Attested photocopy of documents such as: Passport/Driving License/Citizen identification Number/Any document issued by a Government Agency b. Attested photocopy as address proof of documents

	such as : Latest telephone bill (landline or mobile)/Latest electricity bill/Insurance policy receipt / any other document issued by the Government agency c. Any other identification document as approved by the CCA d. In the case of authorized representatives of Organization, documents validating the identity of the organizations would also be required. These may include ○ Company Registration ○ Society Registration ○ Memorandum of Understanding ○ Article of Association ○ Documents pertaining to Commercial establishment ○ Bank details for a Current Account ○ Partnership Deed / Agreement etc ○ Trade Mark Registration Certificate, if any ○ Any other documents as specified in the CPS or by CCA. ○ Proof that the person representing the organization is duly authorized to do so, is also required In-person verification or video verification will be performed to confirm the identity and existence of the subscriber. In case of applicant residing in Foreign country or Foreign national residing in Mauritius, a certified copy of identity verification documents by a competent authority as mentioned in section 3.1.8 shall be accompanied along with the application. The certification shall contain the competent authority's name, designation, contact address with telephone number, applicants' name and time of verification.

3.2 REKEY AND RENEWAL PROCESS

For Class 2 certificates and Class 3 Certificates the procedure of Rekey will be followed. The subscriber should apply for renewal at least 15 days prior to expiration of his existing certificate. A new key pair has to be generated and a new certificate is issued against the request. The renewal of certificates would comply with section 26 of the ETA.

3.3 REKEY AFTER REVOCATION

Once a Digital Signature Certificate is revoked by eMudhra, irrespective of the reasons, it shall never be renewed by eMudhra. Any subscriber who wants to use Digital Signature Certificate issued by eMudhra, has to complete the registration process as outlined in this CPS.

3.4 REVOCATION REQUEST

eMudhra verifies, whether the request for revocation of a certificate, is raised by the subscriber or the local agent who approved the subscriber's application for certificate, before revoking a certificate. In addition, the procedures for authenticating a request for revocation may include one or more of the following :

- If applicable, having the subscriber submit the challenge question (As part of the certificate application process, subscribers optionally choose and submit a challenge phrase with their enrollment information), , and revoking the certificate if it matches the challenge phrase on record,
- Receiving a message purportedly from Subscriber who requested for revocation, containing the Digital Signature of the certificate to be revoked, and
- Online request from Subscriber. The Subscriber submits an online revocation request, or the Subscriber sends a revocation request message that is not digitally signed with reference to the certificate to be revoked. In these cases, Local Agent confirms the revocation request by sending an e-mail to the certificate subscriber (to the e-mail address listed in the certificate to be revoked) and requests the subscriber to respond confirming the revocation. eMudhra revokes the certificate only after receiving the confirmation / approval from Local Agent. eMudhra local agent shall have the right to request for revocation of any Subscriber certificate whose applications are authenticated by them, using their access control rights given to them through their certificate. eMudhra may revoke the certificates based on the online request without digital signature from the subscriber login that is made available for the subscriber.

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The initial registration process shall include the submission of application either by online or offline mode by the applicant for issuing Digital signature certificate along with the supporting documents. Any such application shall be verified / validated by the local agent, with whom the application is submitted

4.1.1 Certificate Applications for End-User Subscriber Certificates

Any end-user certificate applicant requesting for eMudhra certificate, needs to go through the registration process consisting of:

- Completing and submitting Application form for certificate along with required information/ documents
- Generating a key-pair
- Delivering his/ her, or its public key, directly or through the local agent , to eMudhra
- Demonstrating to eMudhra that the Applicant has possession of the Private Key corresponding to the public key sent to eMudhra
- Giving consent to the Subscriber Agreement of eMudhra, in force at that time

Applications so submitted may be approved or rejected. In case of approval, the issuance of the certificate will be done by one of the Issuing CA in eMudhra PKI hierarchy.

4.1.2 Certificate Application for Local Agent Certificates

eMudhra enters into a contract with eMudhra. Local Agent provides its credentials as required, demonstrating their identity. Issuing CA, Local Agent certificate request is created and approved by authorized eMudhra personnel through a controlled process that requires the participation of multiple trusted individuals. In addition eMudhra CAs' certificates requests are also created and approved by authorized eMudhra personnel.

4.2 CERTIFICATE ISSUANCE

4.2.1 Issuance of End-User Subscriber Certificates

On receipt of a completed application, the local agent shall approve or reject. After thorough verification of all required information/procedures, based on Certificate requirement, if everything is found appropriate, then the local agent approves the certificate application otherwise the local agent can reject the certificate application. On receipt of the local agent's approval to issue the Certificate application, a certificate is created and issued based on the information in the certificate application.

4.2.2 Issuance of Certificate to Local Agent

The local agent certificate are authenticated by eMudhra. The certificates are issued to perform the local agent functions prescribed by eMudhra. eMudhra shall enter into a contract with local agent applicant after confirming their identity based on the credentials submitted. The execution of such a contract indicates the complete and final approval of the application by eMudhra. The decision to approve or reject customer application is solely at the discretion of eMudhra. Following such approval, eMudhra issues the certificate to the local agent.

4.3 CERTIFICATE ACCEPTANCE

A notification is sent to subscriber that the certificate is ready to be downloaded. Certificates are made available by allowing subscribers to download them from eMudhra web site. Downloading the certificate constitutes the subscriber's acceptance of the certificate.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for Revocation

4.4.1.1 Circumstances for Revocation of Subscriber Certificate

eMudhra shall revoke a subscriber certificate under the following circumstances:

- The local agent approving the subscriber's certificate application has reason to believe that
    - There has been a compromise of the subscriber's private key,
    - The certificate was issued in a manner not materially in accordance with the procedures required by this CPS,
    - The subscriber's data in the certificate is suspected to be inaccurate;
- The information provided by applicant in the certificate application is false or untrue;
- The local agent who approved the Subscriber's application for CERTIFICATE, finds out that one/some of the pre-requisites for CERTIFICATE issuance was not complied with properly or done inadequately;
- In case of organizational certificates, the subscriber's organization name or constitution changes or the relationship between the organization and the representative to whom the certificate was issued has ceased to exist;
- The subscriber has breached materially an obligation or representation or warranty as per the Subscriber Agreement of eMudhra, in force at that time;
- The subscriber/eMudhra prefers to disagree on one or some or all the points of Subscriber Agreement with the subscriber, and expresses his/its intention to terminate the Subscriber Agreement;
- The subscriber requests revocation of the certificate; and / or
- To comply with any judicial/ law enforcement proceedings.

4.4.1.2 Circumstances for Revocation of Issuing CA or LA Certificates

eMudhra may revoke a Issuing CA or Local agent Certificate if:

- It has credible information or reason to believe that the Private Key of the Issuing CA or Local agent is compromised
- on termination of the agreement between eMudhra and the Local agent
- It has credible information or has reason to believe that the certificate was issued in violation of the procedures laid out in this CPS
- It has credible information or reason to believe that the certificate was issued to some entity other than the one named as Subject in the certificate or Certificate was issued without proper authorization from the entity named as Subject in the certificate.
- It realizes that some material pre-requisite for certificate issuance was not satisfied fully or partially
- The Local agent requests revocation of the certificate.

4.4.2 Who Can Request Revocation

4.4.2.1 Who Can Request Revocation of Subscriber Certificate

eMudhra shall accept revocation requests from

- The subscriber of the Certificate or his/her legal heir in case the Subscriber has expired
- The authorized personnel or representative of the organization
- The Local Agent that approved or processed the subscriber's certificate application request.

eMudhra could initiate the revocation / request on its own for the above mentioned entities.

4.4.2.2 Who Can Request Revocation of an Issuing CA or LA Certificate

Revocation requests for eMudhra, Issuing CA, Local agent , certificates could be initiated by the concerned entity or an authorized agent / entity. eMudhra could initiate the revocation / request on its own for the above mentioned entities.

4.4.3 Procedure for Revocation Request

4.4.3.1 Procedure for Revocation Request of Subscriber Certificate

An entity requesting for revocation shall be a Subscriber or duly authorized representative, as applicable. Any such request is to be communicated to eMudhra or the local agent that was involved in the issuance process.

The request will be online through a challenge phrase or in an offline mode through signed revocation request. On receipt of a valid revocation request eMudhra on a reasonable best effort basis will immediately revoke the certificate and notify the subscriber about the certificate revocation. For offline revocation requests, the requests will be processed on the next working day. The updation and publishing the CRL will be done as detailed in this CPS.

4.4.3.2 Procedure for Revocation Request of an Issuing CA or Local Agent Certificate

A Local agent may request eMudhra for revocation of Local agent certificate. Authorized eMudhra personnel may request eMudhra for revocation of Issuing CA certificate. Upon receiving a valid revocation request eMudhra will promptly revoke that certificate and notify the requester about the successful revocation. In case of the revocation of a Issuing CA certificate, eMudhra will also notify the concerned local agent and subscribers about the same.

4.4.4 Revocation Request Grace Period

Revocation requests are to be verified on receipt and action should be taken as detailed in the section 4.4.3.1 of this CPS

4.4.5 Circumstances for Suspension

eMudhra does not offer suspension services for Issuing CA or subscriber certificates.

4.4.6 Who can Request Suspension

Not Applicable

4.4.7 Procedure For Suspension Request

Not Applicable

4.4.8 Limits On Suspension Period

Not Applicable

4.4.9 CRL Issuance Frequency

eMudhra updates and publishes the CRLs for subscriber Certificates at least once every week.

4.4.10 Certificate Revocation List Checking Requirements

Relying parties must verify the validity of a certificate against the recent/latest CRL that is published in the eMudhra repository to rely on the subject certificate.
The CRLs will be available in eMudhra's repository www.eMudhra.mu/repository/crl.

4.4.11 On-Line Revocation/Status Checking Availability

In addition to publishing the CRL, eMudhra will also provide a web query mechanism to check the status of Certificates in the repository. In addition eMudhra will also provide OCSP service to relying parties who require such services. This will be a charged service and the exact mode will be communicated with the relying parties.

4.4.12 On-Line Revocation Checking Requirements

In case a relying party does not check certificate status using CRL, they will have to adopt one of the checking mechanisms mentioned in section 4.4.11.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation

4.4.14 Special Requirements Regarding Key Compromise

In case there has been a key compromise of any eMudhra CA, eMudhra will make additional reasonable efforts to notify the relying parties.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 Types of Events Recorded

eMudhra would maintain the Trustworthy transaction logs as required in Regulation 22 of ETA Regulations.

4.5.2 Retention Period for Audit Log

Trustworthy transaction logs as defined in Regulation 22 of ETA Regulations, are retained for a period of 10 years as required under Regulation 23 of ETA Regulations.

4.5.3 Protection of Audit Log

Only authorized eMudhra / local agent personnel have access to view and process audit log files. Audit logs are protected from unauthorized viewing, modification, deletion, or other tampering through the use of any or all of various access control mechanisms.

4.5.4 Audit Log Backup Procedures

Backup of audit logs on physical removable media are created periodically and protected from unauthorized personnel. In addition, audit logs and audit summaries are backed up or copied if in manual form.

4.5.5 Audit Collection System

Audit data is collected in a combination of automated and manual process and is protected from unauthorized access, viewing, modification, deletion or tampering.

4.5.6 Notification to Event-Causing Subject

No notice is required to be served/ given to the individual, organization, device, or application that caused any event, which is logged by the audit collection system.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Recorded

eMudhra and its local agent record

- Events as mentioned in Regulation 22 of ETA Regulations.
- Records are kept in the form of either computer-based messages or paper-based documents. It is ensured that the indexing, storage, preservation, and reproduction of records are accurate, legible and complete.

4.6.2 Retention Period for Archive

Records are retained as per Regulations 22 and 23 of ETA regulations.

4.6.3 Protection of Archive

eMudhra and its local agent protect archived records and ensure that access to such record is made available only to authorized personnel. The archived records are protected from unauthorized viewing, modification, deletion, or other tampering. The media containing the archive data and the systems used to process the archived data are maintained properly so that the archived data is accessible for the time period required by ETA.

4.6.4 Archive Backup Procedures

eMudhra and its local agent create backup copies of archives as and when the archives are created. All such Backup copies and copies of other paper-based records are maintained in an off-site disaster recovery/ warehouse facility.

4.6.5 Requirements for Time-Stamping Of Records

All significant records including Certificates, CRLs, and other revocation database entries contain time and date information.

4.6.6 Archive Collection System

Archives are handled by trusted & authorized personnel of eMudhra.

4.6.7 Procedures to Obtain and Verify Archive Information

Only eMudhra trusted personnel and CCA Mauritius on request are permitted to access the archived data.

4.7 KEY CHANGEOVER

Changeover of Keys of eMudhra CA, Local agent and Subscribers shall be carried out as stipulated by the ETA. eMudhra shall give adequate notice in case of any change in key pair of eMudhra CA, used to sign DSC issued under eMudhra hierarchy, to the subscribers, Local Agent & relying parties. Subscriber's keys will not be changed in the case of a compromise.

On or before expiry of an existing certificate, the subscribers shall generate a new key pair and submit the public key along with the new application or upon generating a new Certificate.

4.8 DISASTER RECOVERY AND KEY COMPROMISE

Backup of CA and Issuing CA private keys are generated and maintained and will be made available in the event of disaster. eMudhra maintains a Disaster Recovery center as per the requirements of guidelines of CCA & ETA Regulations which will be able to handle Issuance and revocation of certificates and publishing of CRL.

In the event of eMudhra key compromise, the key management and operations personnel of eMudhra including the security, cryptographic operations, administration and management representatives will act as per the incident management and disaster recovery plan which has been approved by eMudhra CA Policy approval committee.

4.9 CA TERMINATION

In case of termination of a Issuing CA, or eMudhra CA, eMudhra will create and publish a termination plan that reasonably minimizes disruption to customers, subscribers, and relying parties. The termination plan covers issues including but not limited to:

- Providing notice to subscribers, relying Parties with which eMudhra has established contacts, customers, and the CCA who may be affected by such a termination.
- Revocation of certificate issued to the Issuing CA by eMudhra,
- Preservation of the archives and records as required in this CPS and ETA
- Providing Customer service, revocation service & publishing of CRLs.
- Compensation for any certificates revoked under the termination plan or assisting issuance of new certificate in lieu of the revoked certificate from another CA.
- The procedure / process of destructing private keys of the CA and/or the issuing CA.
- Provisions needed for the transition of services to a successor issuing CA.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The system components and operation of eMudhra shall be located in a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information.
eMudhra primary site consists of several physical tiers with security and physical controls. The system and facility is set-up in India and licensed by the Controller of Certifying Authorities, India.

5.1.2. Physical Access

eMudhra operation premises including sensitive area inside the premises shall be actively monitored.

The security of Multiple tiers of the operation site is enforced through proximity cards and biometric access devices. Any visitor access shall be logged in the appropriate register or log. Any visitor shall be escorted by eMudhra's trusted personnel only after obtaining required permissions.

The facility shall be continually monitored (24x7), by manned security.

5.1.3. Power and Air Conditioning

Primary and backup power systems / sources are available for providing uninterrupted power supply to the eMudhra CA's operational facility.

5.1.4. Water Exposures

eMudhra's CA facility is reasonably protected against large volume of water exposure including flood water and other water exposure.

5.1.5 Fire Prevention and Protection

eMudhra CA facility is equipped to prevent and extinguish fires. Appropriate equipments have also been implemented to minimize the damage due to smoke and fire exposure. These measures meet applicable fire safety regulations.

5.1.6 Media Storage

eMudhra CA data and information as required by ETA are backed up and stored within primary or offsite locations. The access to such location is controlled through various access control mechanism and the access is limited to eMudhra authorized personnel.

5.1.7. Waste Disposal

Paper documents and materials as found unusable shall be disposed. eMudhra shall dispose various materials using appropriate equipment or mechanism or as per manufacturers guidelines.

5.1.8. Off-Site Backup

All critical data shall be backed up periodically and such backup copies shall be stored securely at an offsite location as identified by eMudhra.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The trusted roles pertain to roles, performed by eMudhra and its local agent personnel handling the following functions, but not limited to:

- validating information in applications
- accepting, rejecting, or other processing of applications, revocation requests, or renewal requests, or enrollment information
- issuance, or revocation of certificates,
- accessing restricted portions of eMudhra's repository

5.2.2 Number of Persons Required Per Task

eMudhra shall identify individuals to perform each trusted role to ensure the integrity of its CA operations. Where required, eMudhra shall implement m out of n control to handle certain sensitive functions.

5.2.3 Identification and Authentication for Each Role

eMudhra shall verify the identity of personnel seeking to become trusted personnel by conducting a background check. Additionally eMudhra shall request the personnel to appear physically before particular authorized personnel or check the identity through a government issued identification. eMudhra ensures that a person achieves trusted status to access the facility or to obtain logical access to perform the activity in eMudhra systems. eMudhra CA will require it's Local Agent to carry out a similar method of verification for the designated personnel from its local agent entity.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel seeking to become trusted persons must be technically and professionally competent and must provide necessary proof of qualifications, and experience required to perform their job responsibilities.

5.3.2 Background Check Procedures

eMudhra conducts background checks, which shall include the following:

- Previous employment history,
- Search of Police records,
- Education verification
- Reference check.
- eMudhra shall avail the services of a private agency or government agency to conduct such background check.

The factors like

- Misrepresentations made
- Highly unfavorable or unreliable personal references and
- Certain criminal convictions, etc.,

revealed in a background check or otherwise, may be considered as valid reasons for rejecting a person's candidature for becoming Trusted Personnel or even for removal of existing trusted personnel. eMudhra HR policy shall form the basis of such actions.

5.3.3 Training Requirements

eMudhra shall ensure that well qualified and trained personnel are appointed for the trusted role to perform the job satisfactorily. Any such personnel is provided training in the ETA and its IT Security policy, eMudhra policies, procedures and process and any relevant technical training.

eMudhra may provide adequate training to personnel to perform their role. The adequacy of such training will be determined by eMudhra from time to time.

5.3.4 Retraining Frequency and Requirements

eMudhra provides periodic security awareness and any new technology changes training is provided on an ongoing basis based on the newer versions or releases of the products. The frequency of such training will be determined by eMudhra from time to time.

5.3.5 Job Rotation Frequency and Sequence

Not stipulated

5.3.6 Sanctions for Unauthorized Actions

Any violations or unauthorized actions of eMudhra policies and procedures will invite eMudhra disciplinary actions. Such Disciplinary actions may include termination of employment.

5.3.7 Contracting Personnel Requirements

Independent contractors and consultants are permitted access to eMudhra secure facilities only to the extent they are escorted and directly supervised by trusted persons.

5.3.8 Documentation Supplied to Personnel

All the personnel involved in eMudhra services shall be required to read this CPS and other policy documents.

Relevant documents required to perform the roles are provided to personnel. Such relevancy will be determined by eMudhra based on the role performed by the personnel.

eMudhra shall make available to the personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

eMudhra CA key pairs will be generated by multiple trained and trusted personnel in pre-planned key generation ceremonies as per the guidelines laid down in the Key Ceremony Handbook, Key Management Tool user's guide and security policy. Key pairs for eMudhra CAs is generated in a hardware security module (HSM) certified to meet the requirements of FIPS 140-1 level 3 or higher.
The Local agent key pair will be generated in smart card/hardware token which follows FIPS 140-1 level 2 or higher.
Subscribers shall use 1024 as the minimum key length while generating the key pair. Any such generation should preferably be on a FIPS 140-1/2 level 1 validated cryptographic module.

6.1.1 Private Key Delivery to Entity

Generally the end subscriber private key will be generated by the end subscriber. In the case of hardware based tokens or smart cards, appropriate tokens with pre-generated keys may be procured by Subscriber or sent by eMudhra to the subscribers and the associated PIN will be sent by an out of band process. Where required, the local agent could generate the subscriber keys in a non-exportable medium and deliver to the subscriber

6.1.2 Public Key Delivery to Certificate Issuer

PKCS#10 requests containing the public key of the subscriber is sent to the CA server. This will be accomplished using the client software/driver which will initiate an online session with the CA server and deliver the signed certificates to the subscriber. The online session will be secured by SSL.

6.1.3 CA Public Key Delivery to Users

eMudhra makes its CA Public Keys Certificates available to relying parties in repository available at www.eMudhra.mu/repository/cacerts.

6.1.4 Key Sizes

The key length of eMudhra CAs (including Issuing CAs) shall be equivalent to 2048-bit RSA key pair. Local Agent and subscribers shall be required to use key pairs that are minimum 1024 bits long or higher, if stipulated by eMudhra.

6.1.5 Public Key Parameters Generation

Not stipulated.

6.1.6 Parameter Quality Checking

Not stipulated.

6.1.7 Hardware/Software Key Generation

eMudhra CA generates key pairs in FIPS 140-1 Level 3 compliant hardware security modules.

6.1.8 Key Usage Purposes

The purposes for which a key can be used may be restricted by eMudhra through Key Usage extension in the certificate (Refer section 7.1.2 of this CPS).

6.2 PRIVATE KEY PROTECTION

eMudhra 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 5.1 of this CPS.

6.2.1 Standards for Cryptographic Modules

eMudhra performs all cryptographic operations with its own CA/Issuing CA private keys and client Issuing CA private keys on hardware cryptographic modules rated at a minimum of FIPS 140-1 level 3.

Local agent performs cryptographic operations with their own private keys on hardware cryptographic modules. Subscribers have the option of protecting their private keys by using a FIPS 140-1/2 level 1 validated cryptographic module.

6.2.2 Private Key (N out of M) Multi-Person Control

eMudhra has implemented multi-person control to protect the activation data needed to activate CA/Issuing CA private keys within eMudhra PKI. eMudhra segregates the private key or activation data needed to operate the private key into separate parts called “Secret Shares” Each ‘secret share’ is held by a distinct eMudhra trusted personnel referred to as the Custodian. A threshold number of secret shares (n) out of the total number of secret shares (m) are required to operate the private key. eMudhra also uses similar method to protect the data needed to activate private keys of its disaster recovery site.

6.2.3 Private Key Escrow

eMudhra will only escrow Subscriber’s encryption private keys. The procedures as approved by CCA will be in place for escrowing subscriber private keys

6.2.4 Private Key Backup

eMudhra creates backup of CA private keys. These are stored in encrypted form in a hardware cryptographic module.

6.2.4 Private Key Archival

At the end of the validity period, CA private key will be deleted and will not be archived. These keys will be destroyed as per requirements specified in section 6.2.9 of this CPS.

6.2.5 Private Key Entry into Cryptographic Module

CA key pairs of eMudhra are generated on the hardware cryptographic modules in which the keys will be used. eMudhra ensures a copy of such key pairs for disaster recovery purposes. All such copies are transferred in an encrypted form.

6.2.6 Method of Activating Private Key

In case of eMudhra CAs, activation of private key shall require m out of n secret shares as mentioned in section 6.2.2 and will be from the cryptographic hardware device that follows FIPS 140-1level 3 standards.

In case of local agent and subscriber, private keys are activated by the client application either by a PIN or password.

6.2.7 Method of Deactivating Private Key

eMudhra private keys are deactivated upon removal of cryptographic module. Local agent's private keys (used for authentication to the Local Agent application) are deactivated upon system log off or removal from card/token reader.
Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card/token from the reader depending upon the authentication mechanism employed by the user. In all cases, the responsibility lies with the subscribers to adequately protect their private key(s).

6.2.8 Method of Destroying Private Key

At the conclusion of an eMudhra CAs' operational lifetime, the private keys are securely destroyed. CA key destruction activities require the participation of multiple trusted personnel.

Wherever required, on best effort basis, eMudhra shall destroy CA private keys in such a way to reasonably ensure that there are no residuals remains of the key which could lead to the possible reconstruction of the key.
eMudhra utilizes the zeroization function of its hardware cryptographic modules to ensure proper destruction of its private keys. Any such activity is logged.
eMudhra may adopt and perform different methods to destroy its private keys based on the advancement of the technology.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

All certificates containing public keys (including those of eMudhra CA, local agent and Subscribers) are archived upon expiry as part of eMudhra's routine backup procedures and kept for a period of Ten (10) years as per ETA Regulations.

6.3.2. Usage Periods for the Public and Private Keys

The expiry date of eMudhra CA certificate will be as provided by CCA. eMudhra may consider stopping issuance of new certificates at a suitable date prior to the expiration of its certificate under eMudhra hierarchy so that no certificate issued by a issuing CA in the hierarchy expires after the expiration of the corresponding parent CA certificate

Certificate	Validity
All certificates issued including local agent Subscriber	One year or 2 years based on the requirement of applicant.

6.3.3. Root Certificate and Trust Chain Validation

eMudhra CA certificate is issued under CCA Mauritius PKI hierarchy. The root node is CCA Mauritius and the root certificate is issued for a period of 10 years. Most of the relying party applications use web browsers to validate the trust chain. Currently, the public key certificate of the CCA of Mauritius is not embedded in the different web browsers for the automatic validation of the trust chain. In order to avoid subscribers in getting a trust chain validation error at the first time of use of their private key certificate, eMudhra has automated the installation process of the root node into the web browser of the subscriber's computer.

In this respect, for Internet Explorer and Chrome browsers, the subscriber will be prompted for the automatic installation of this root node once the USB token is inserted in the computer. Subscribers are, therefore, requested to allow the application to install the root node in their Internet Explorer browsers.

For Firefox web browsers, the installation of the root node will need to be done manually by the subscriber. For this purpose, visit www.eMudhra.mu. Click on "CRLs & Root Certificates" link on the left side of the webpage. Under the CA Certificates section of the next webpage, click on "eMudhra CA" link and follow the installation wizard instructions.

For Safari web browsers on Windows and Mac, the installation will also need to be done manually by the subscriber. For this purpose, visit www.eMudhra.mu. Click on "CRLs & Root Certificates" link on the left side of the webpage. Under the CA Certificates section of the next webpage, click on "eMudhra CA" link to download the root node. Double-click on "install certificate". In the Certificate Import wizard pop up, click "Next", choose the "place certificate in the following store" option, then click on the "browse" button and choose the "Trusted Root Certification Authorities" folder and click "ok". Click on the "Next" button, click "Finish" and click "Accept" in the installation request pop up.

6.4 ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

After personalization or initialization of HSM/Smart card/token, no activation data other that access control mechanisms (PIN) are required to operate cryptographic modules.

6.4.2. Activation Data Protection

Passwords or PIN shall not be accessible to anyone except the authorized personnel or certificate holder.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

eMudhra and the local agent ensure that the systems maintaining CA software and data files are trustworthy systems secure from unauthorized access. eMudhra uses firewalls to protect the production network from any internal and external intrusion. Direct access to databases supporting eMudhra repository is limited to trusted persons in eMudhra/local agent operations group having a valid business reason for such access.

6.5.2 Computer security rating

No stipulation

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

eMudhra develops implements and maintains Applications, as per its System Development and Change Management Standards.

6.6.2 Security Management Controls

eMudhra has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. The hash is generated and used to verify the integrity of such software/system manually. Upon installation and periodically thereafter, eMudhra validates the integrity of its CA systems. Such periodicity will be defined by eMudhra as required.

6.6.3 Life Cycle Security Ratings

No stipulation

6.7 NETWORK SECURITY CONTROLS

eMudhra performs all its CA and local agent functions using networks secured in accordance with the security policies and procedures to prevent unauthorized access. eMudhra protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

eMudhra shall utilize hardware cryptographic modules rated minimum FIPS 140-1 Level 3 to perform all digital signing operations. All cryptographic module engineering threats are assessed and addressed.

7. CERTIFICATE AND CRL PROFILE

7.1 CERTIFICATE PROFILE

eMudhra Certificates confirm to

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

At a minimum, eMudhra X.509 Certificates contain the basic X.509 Version 1 fields and indicated prescribed values or value constraints

BASIC FIELD	VALUE OR VALUE CONSTRAINT
Version	Version 3
Serial number	Integer value, unique for each certificate issued by the issuer
Signature Algorithm	Algorithm used by the issuer to sign the certificate
Issuer DN	The X.500 distinguished name of the entity signing the certificate
Validity	The certificate validity period represented by two dates: Validity not before - the date on which the certificate validity period begins, and validity not after - the date on which the certificate validity period ends.
Subject DN	The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate
Subject Public Key	Encoded in accordance with RFC 2459
Signature	Generated and encoded in accordance with RFC 2459

7.1.1 Version Number(s) Supported

All eMudhra Certificates are X.509 version 3 Certificates.

7.1.2 Certificate Extensions

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

EXTENSION	VALUE OR VALUE CONSTRAINT	CRITICALITY
Key Usage	For eMudhra CAs: keyCertSign, CRLSign	TRUE
	For Subscribers: digital Signature, nonrepudiation, key Encipherment, data Encipherment, code Signing	FALSE
Basic Constraints	For eMudhra CAs: CA	TRUE
	For Subscribers: End Entity	

	For eMudhra CAs: not stipulated	FALSE
Extended Key Usage	For Subscribers: ServerAuth, ClientAuth, Code Signing, Email Protection, OCSPSigning	FALSE
Authority Key Identifier	SHA-1 hash value of issuer's public key	FALSE
Subject Key Identifier	SHA-1 hash value of subscriber's public key	FALSE
Subject Alternative Name	As per RFC 2459	FALSE
Issuer Alternative Names	As per RFC 2459	FALSE
CRL Distribution Points	URI of the CRL	FALSE

7.1.3 Algorithm Object Identifiers

eMudhra issued certificates are signed using sha1 With RSA Encryption algorithm.

7.1.4 Name Forms

eMudhra issued certificates are populated with an issuer and subject distinguished name.

7.1.5 Name Constraints

No Stipulation.

7.1.6. Certificate Policy Object Identifier

No stipulation.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

eMudhra populates all certificates with a CPS pointer policy qualifier with corresponding OID having a value pointing to the URL of eMudhra CPS.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.2 CRL PROFILE

eMudhra CAs issue CRLs that conform to RFC 2459.

BASIC FIELD	VALUE OR VALUE CONSTRAINT
Version	Version 2
Signature Algorithm	Algorithm used by the issuer to sign the CRL
Issuer DN	The X.500 distinguished name of the entity signing the certificate
Effective Date	Issue date of the CRL. eMudhra issued CRLs is effective upon issuance
Next Update	Date by which the next CRL will be issued
Revoked Certificates	List of revoked certificates, including the serial number of revoked certificate and revocation date.

7.2.1. Version Number(s) Supported

All eMudhra CRLs are X.509 version 2 CRLs

7.2.2 CRL AND CRL Entry Extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Amendments to this CPS shall be made by eMudhra Policy Approval Committee and need to be approved by the CCA before they become effective. Updates can be a new document containing the revised CPS or it can contain only the updated information. Proposed new versions or updates shall be posted in eMudhra repository.

8.1.1. Items that Can Change Without Notification

eMudhra will notify non-material changes such as corrections of typographical errors, changes to URLs, and changes to contact information to the CCA. These changes will be updated in the next release of CPS with the approval of CCA.

8.1.2. Items that Can Change with Notification

8.1.2.1 List of Items

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

8.1.2.2 Notification Mechanism

Except as noted under section 8.1.1, eMudhra Policy Approval Committee shall submit the proposed updates in electronic and/or paper form to the CCA for approval. After obtaining the CCA's approval the proposed updates to the CPS shall be posted in eMudhra repository, which is located at www.eMudhra.com/repository/cps

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

8.2.1 Items not published in the CPS

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

8.2.2 Distribution of the CPS

This latest version of this CPS is available for viewing in electronic form within eMudhra repository at www.eMudhra.mu/repository/cps

eMudhra also makes the CPS available upon request sent to:
info@eMudhra.mu

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

eMudhra CA,

3rd Floor, Sai Arcade,
Outer Ring Road,
Devarabeesanahalli,
Bangalore - 560036
Karnataka, India

Phone: +91 80 42275300
Fax: +91 80 42275306
Email: info@eMudhra.mu
Website: www.eMudhra.mu

8.3 CPS APPROVAL PROCEDURES

eMudhra Policy Approval Committee approves the CPS that is intended for use within eMudhra PKI. The final approval of the CPS will be made by the CCA.

9. GLOSSARY

9.1 DEFINITIONS

A DIGITAL SIGNATURE CERTIFICATE
To demonstrate approval of a Digital signature certificate by a Digital signature certificate applicant while knowing or having notice of its informational contents.

ACCESS
Gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

ACCESS CONTROL
The process of limiting access to the resources of a computer system only to authorized users, programs or other computer systems.

AUTHORITY REVOCATION LIST (ARL)
A list of revoked Certification Authority Certificates. An ARL is a CRL for Certification Authority cross-Certificates.

ARCHIVE
To store records and associated journals for a given period of time for security, backup, or auditing purposes.

ASYMMETRIC CRYPTO SYSTEM
A system of a secure key pair consisting of a private key for creating a Digital Signature and a public key to verify the Digital Signature.

AUDIT
A procedure used to validate that controls are in place and adequate for their purposes, which includes recording and analyzing activities to detect intrusions into or abuses in an information system. Inadequacies found by an audit are reported to appropriate management personnel.

AUDIT TRAIL
A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

AUTHENTICATION
A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit. (*See also* VERIFY (a DIGITAL SIGNATURE))

AUTHORIZATION
The granting of rights, including the ability to access specific information or resources.

AVAILABILITY

The extent to which information or processes are reasonably accessible and usable, upon demand, by an authorized entity; allowing authorized access to resources and timely performance of time-critical operations.

BACKUP
The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.

CERTIFICATE
A Digital signature certificate issued by Certification Authority.

CERTIFICATE CHAIN
An ordered list of Certificates containing an end-user Subscriber Certificate and Certification Authority Certificates (*See* **VALID CERTIFICATE**).

CERTIFICATE EXPIRATION
The time and date specified in the Digital signature certificate when the operational period ends, without regard to any earlier suspension or revocation.

CERTIFICATE EXTENSION
An extension field to a Digital signature certificate which may convey additional information about the public key being certified, the certified Subscriber, the Digital signature certificate issuer, and/or the certification process. Standard extensions are defined in Amendment 1 to ISO/IEC 9594-8:1995 (X.509). Custom extensions can also be defined by communities of interest.

CERTIFICATE ISSUANCE
The actions performed by a Certification Authority in creating a Digital Signature Certificate and notifying the Digital signature certificate applicant (anticipated to become a
Subscriber) listed in the Digital signature certificate of its contents.

CERTIFICATE MANAGEMENT [MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE]
Certificate management includes, but is not limited to, storage, distribution, dissemination, accounting, publication, compromise, recovery, revocation, suspension and administration of Digital signature certificates. A Certification Authority undertakes Digital signature certificate management functions through its Local Agent for Subscriber Digital signature certificates. A Certification Authority designates issued and accepted Digital signature certificates as valid by publication.

CERTIFICATE POLICY
A specialized form of administrative policy tuned to electronic transactions performed during Digital signature certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Digital signature certificates. Indirectly, a Certificate policy can also govern the transactions conducted using a communications system protected by a Certificate based security system. By controlling critical Certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

CERTIFICATE REVOCATION (*SEE* **REVOKE A CERTIFICATE) CERTIFICATE REVOCATION LIST (**CRL**)**
A periodically (or exigently) issued list, digitally signed by a Certification Authority, of identified Digital signature certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next

scheduled CRL issue, the suspended or revoked Digital signature certificates' serial numbers, and the specific times and reasons for suspension and revocation.

CERTIFICATE SERIAL NUMBER
A value that unambiguously identifies a Digital signature certificate generated by a Certification Authority.

CERTIFICATION / CERTIFY
The process of issuing a Digital signature certificate by a Certification Authority.

CERTIFICATION AUTHORITY SYSTEM
All the hardware and software system (e.g. Computer, PKI servers, network devices etc.) used by the Certification Authority for generation, production, issue and management of Digital signature certificates.

CERTIFICATION PRACTICE STATEMENT (CPS)
A statement issued by a Certification Authority to specify the practices that the Certification Authority employs in issuing Digital signature certificates.

CERTIFIER (See **ISSUING AUTHORITY) CHALLENGE PHRASE**
A set of numbers and/or letters that are chosen by a Digital signature certificate applicant, communicated to the Certification Authority with a Digital signature certificate application, and used by the Certification Authority to authenticate the Subscriber for various purposes as required by the Certification Practice Statement. A challenge phrase is also used by a secret shareholder to authenticate himself, herself, or itself to a secret share issuer.

CERTIFICATE CLASS
A Digital signature certificate of a specified level of trust.

CLIENT APPLICATION
An application that runs on a personal computer or workstation and relies on a server to perform some operation.

COMMON KEY
Some systems of cryptographic hardware require arming through a secret-sharing process and require that the last of these shares remain physically attached to the hardware in order for it to stay armed. In this case, “common key” refers to this last share. It is not assumed to be secret as it is not continually in an individual’s possession.

COMMUNICATION/NETWORK SYSTEM
A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities (covering ISDN, lease lines, dial-up, LAN, WAN, etc.).

COMPROMISE
A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. (*Cf.,* DATA INTEGRITY)

COMPUTER
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.

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

CONFIRM
To ascertain through appropriate inquiry and investigation. (*See also* AUTHENTICATION; VERIFY A DIGITAL SIGNATURE)

CONTINGENCY PLANS
The establishment of emergency response, back up operation, and post-disaster recovery processes maintained by an information processing facility or for an information system.
Establish the strategy for recovering from unplanned disruption of information processing operations. The strategy includes the identification and priority of what must be done, who performs the required action, and what tools must be used.

A document developed in conjunction with application owners and maintained at the primary and backup computer installation, which describes procedures and identifies the personnel necessary to respond to abnormal situations such as disasters. Contingency plans help managers ensure that computer application owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

CONTROLS
Measures taken to ensure the integrity and quality of a process.

CORRESPOND
To belong to the same key pair. (*See also* PUBLIC KEY; PRIVATE KEY)

CRITICAL INFORMATION
Data determined by the data owner as mission critical or essential to business purposes.

CROSS-CERTIFICATE
A Certificate used to establish a trust relationship between two Certification Authorities.

CRYPTOGRAPHY (*See also* **PUBLIC KEY CRYPTOGRAPHY)**
The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.
A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses.

DAMAGE
Means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

DATA
Means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a 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.

DATA CONFIDENTIALITY (See CONFIDENTIALITY**)**

DIGITAL SIGNATURE CERTIFICATE APPLICANT
A person that requests the issuance of a public key Digital signature certificate by a Certification Authority. (*See also* CA APPLICANT; SUBSCRIBER)

DIGITAL SIGNATURE CERTIFICATE APPLICATION
A request from a Digital signature certificate applicant (or authorized agent) to a Certification Authority for the issuance of a Digital signature certificate. (*See also* CERTIFICATE APPLICANT; CERTIFICATE SIGNING REQUEST)

DIGITAL SIGNATURE
Means authentication of any electronic record by a Subscriber by means of an electronic method or procedure in accordance with the ETA

DIGITAL SIGNATURE CERTIFICATE
Means a Digital signature certificate issued under ETA

DISTINGUISHED NAME
A set of data that identifies a real-world entity, such as a person in a computer-based context.

DOCUMENT
A record consisting of information inscribed on a tangible medium such as paper rather than computer-based information. (*See also* MESSAGE; RECORD)

ELECTRONIC FORM
With reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, microfilm, computer generated microfiche or similar device.

ELECTRONIC MAIL ("E-MAIL")
Messages sent, received or forwarded in Digital form via a computer-based communication mechanism.

ELECTRONIC RECORD
Means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche.

ENCRYPTION
The process of transforming plaintext data into an unintelligible form (cipher text) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

EXTENSIONS
Extension fields in X.509 v3 Certificates. (*See* X.509)

FIREWALL/DOUBLE FIREWALL
One of several types of intelligent devices (such as routers or gateways) used to isolate networks. Firewalls make it difficult for attackers to jump from network to network. A double firewall is two firewalls connected together. Double firewalls are used to minimize risk if one firewall gets compromised or provide address translation functions.

FUNCTION
In relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer.

GENERATE A KEY PAIR
A trustworthy process of creating private keys during Digital signature certificate application whose corresponding public keys are submitted to the applicable Certification Authority in a manner that demonstrates the applicant's capacity to use the private key.

HASH (HASH FUNCTION)
An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that: (i) A message yields the same result every time the algorithm is executed using the same message as input.
ii) It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.

It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

IDENTIFICATION / IDENTIFY
The process of confirming the identity of a person. Identification is facilitated in public key cryptography by means of Certificates.

IDENTITY
A unique piece of information that marks or signifies a particular entity within a domain. Such information is only unique within a particular domain.

INFORMATION
Includes data, text, images, sound, voice, codes, computer programmes, software and databases or microfilm or computer generated microfiche.

INFORMATION TECHNOLOGY SECURITY
All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability.

INFORMATION TECHNOLOGY SECURITY POLICY
Rules, directives and practices that govern how information assets, including sensitive information, are managed, protected and distributed within an organization and its Information Technology systems.

KEY
A sequence of symbols that controls the operation of a cryptographic transformation
(E.g. encipherment, decipherment, cryptographic checks function computation, Signature generation, or Signature verification).

KEY GENERATION
The trustworthy process of creating a private key/public key pair.

KEY MANAGEMENT
The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

KEY PAIR
In an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a Digital Signature created by the private key.

LICENCE
Means a license granted to a Certification Authority.

LOCAL AREA NETWORK (LAN)
A geographically small network of computers and supporting components used by a group or department to share related software and hardware resources.

MANAGEMENT OF DIGITAL SIGNATURE CERTIFICATE (SEE CERTIFICATE MANAGEMENT)

MEDIA
The material or configuration on which data is recorded. Examples include magnetic tapes and disks.

MESSAGE
A Digital representation of information; a computer-based record. A subset of RECORD. (*See also* RECORD)

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

NETWORK
A set of related, remotely connected devices and communications facilities including more than one computer system with the capability to transmit data among them through the communications facilities.

NON-REPUDIATION
Provides proof of the origin or delivery of data in order to protect the sender against a false denial by the recipient that the data has been received or to protect the recipient against false denial by the sender that the data has been sent. Note: Only a trier of fact (someone with the authority to resolve disputes) can make an ultimate determination of non-repudiation. By way of illustration, a Digital Signature verified pursuant to this Certification Practice Statement can provide proof in support of a determination of non-repudiation by a trier of fact, but does not by itself constitute non-repudiation.

ON-LINE
Communications that provide a real-time connection.

OPERATIONS ZONE
An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment (TRA), and should preferably be accessible from a Reception Zone.

OPERATIONAL PERIOD
The period starting with the date and time a Digital signature certificate is issued (or on a later date and time certain if stated in the Digital signature certificate) and ending with the date and time on which the Digital signature certificate expires or is earlier suspended or revoked.

ORGANISATION
An entity with which a user is affiliated. An organization may also be a user.

PASSWORD (PASS PHRASE; PIN NUMBER)

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

PC CARD (SEE ALSO SMART CARD)
A hardware token compliant with standards promulgated by the Personal Computer Memory Card International Association (PCMCIA) providing expansion capabilities to computers, including the facilitation of information security.

PERSON
Means any company or association or individual or body of individuals, whether incorporated or not.

PERSONAL PRESENCE
The act of appearing (physically rather than virtually or figuratively) before a Certification Authority or its designee and proving one's identity as a prerequisite to Digital signature certificate issuance under certain circumstances.

PKI (PUBLIC KEY INFRASTRUCTURE) / PKI SERVER
A set of policies, processes, server platforms, software and workstations used for the purpose of administering Digital signature certificates and public-private key pairs, including the ability to generate, issue, maintain, and revoke public key Certificates.

PKI HIERARCHY
A set of Certification Authorities whose functions are organized according to the principle of delegation of authority and related to each other as subordinate and superior Certification Authority.

POLICY
A brief document that states the high-level organization position, states the scope, and establishes who is responsible for compliance with the policy and the corresponding standards. Following is an abbreviated example of what a policy may contain:
Introduction
Definitions
Policy Statement identifying the need for “something” (e.g. data security)
Scope
People playing a role and their responsibilities
Statement of Enforcement, including responsibility

PRIVATE KEY
The key of a key pair used to create a Digital Signature.

PROCEDURE
A set of steps performed to ensure that a guideline is met.

PUBLIC KEY
The key of a key pair used to verify a Digital Signature and listed in the Digital signature certificate.

PUBLIC KEY CERTIFICATE (*See* CERTIFICATE)

PUBLIC KEY CRYPTOGRAPHY (*See* CRYPTOGRAPHY)
A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or

verify a Digital Signature; the private key is kept secret by its holder and can decrypt information or generate a Digital Signature.

PUBLIC KEY INFRASTRUCTURE (PKI)
The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. It includes a set of policies, processes, server platforms, software and workstations, used for the purpose of administering Digital signature certificates and keys.

PUBLIC/PRIVATE KEY PAIR (See **PUBLIC KEY; PRIVATE KEY; KEY PAIR)**

RECIPIENT (of a **DIGITAL SIGNATURE)**
A person who receives a Digital Signature and who is in a position to rely on it, whether or not such reliance occurs. (*See also* RELYING PARTY)

RECORD
Information that is inscribed on a tangible medium (a document) or stored in an electronic or other medium and retrievable in perceivable form. The term "record" is a superset of the two terms "document" and "message". (*See also* DOCUMENT; MESSAGE)

RE-ENROLLMENT (*See also* **RENEWAL)**

RELY / RELIANCE (on a **CERTIFICATE** and **DIGITAL SIGNATURE)**
To accept a Digital Signature and act in a manner that could be detrimental to oneself were the Digital Signature to be ineffective. (*See also* RELYING PARTY; RECIPIENT)

RELYING PARTY
A recipient who acts in reliance on a Certificate and Digital Signature. (*See also* RECIPIENT; RELY OR RELIANCE (on a CERTIFICATE and DIGITAL SIGNATURE))

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

REPOSITORY
A database of Digital signature certificates and other relevant information accessible on-line.

REPUDIATION (*See also* **NONREPUDIATION)**
The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REVOKE A CERTIFICATE
The process of permanently ending the operational period of a Digital signature certificate from a specified time forward.

RISK
The potential of damage to a system or associated assets that exists as a result of the combination of security threat and vulnerability.

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

SECURITY

The quality or state of being protected from unauthorized access or uncontrolled losses or effects. Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations.

SECURITY POLICY
A document which articulates requirements and good practices regarding the protections maintained by a trustworthy system.

SERIAL NUMBER (*See* CERTIFICATE SERIAL NUMBER)

SERVER
A computer system that responds to requests from client systems.

SMART CARD
A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

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

SUBJECT (OF A CERTIFICATE)
The holder of a private key corresponding to a public key. The term “subject” can refer to both the equipment and device that holds a private key and to the individual person, any, who controls that equipment or device. A subject is assigned an unambiguous name, which is bound to the public key contained in the subject’s Digital signature certificate.

SUBJECT NAME
The unambiguous value in the subject name field of a Digital signature certificate, which is bound to the public key.

SUBSCRIBER
A person in whose name the Digital signature certificate is issued.

SUBSCRIBER AGREEMENT
The agreement executed between a Subscriber and a Certification Authority for the provision of designated public certification services in accordance with this Certification Practice Statement.

SUBSCRIBER INFORMATION
Information supplied to a certification authority as part of a Digital signature certificate application. (*See also* CERTIFICATE APPLICATION)

SYSTEM ADMINISTRATOR
The person at a computer installation who designs, controls, and manages the use of the computer system.

THREAT
A circumstance or event with the potential to cause harm to a system, including the destruction, unauthorized disclosure, or modification of data and/or denial of service.

TOKEN

A hardware security token containing a user's private key(s), public key Certificate, and, optionally, a cache of other Certificates, including all Certificates in the user's certification chain.

TRANSACTION
A computer-based transfer of business information, which consists of specific processes to facilitate communication over global networks.

TRUST
Generally, the assumption that an entity will behave substantially as expected. Trust may apply only for a specific function. The key role of this term in an authentication framework is to describe the relationship between an authenticating entity and a Certification Authority. An authenticating entity must be certain that it can trust the Certification Authority to create only valid and reliable Digital signature certificates, and users of those Digital signature certificates rely upon the authenticating entity's determination of trust.

TRUSTED POSITION
A role that includes access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of Digital signature certificates, including operations that restrict access to a repository.

TRUSTWORTHY SYSTEM
Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

TYPE (OF CERTIFICATE)
The defining properties of a Digital signature certificate, which limit its intended purpose to a class of applications uniquely, associated with that type.

UNIFORM RESOURCE LOCATOR (URL)
A standardized device for identifying and locating certain records and other resources located on the World Wide Web.

USER
An authorized entity that uses a Certificate as applicant, Subscriber, recipient or relying party, but not including the Certification Authority issuing the Digital signature certificate. (*See also* CERTIFICATE APPLICANT; ENTITY; PERSON; SUBSCRIBER)

VALIDATION (OF CERTIFICATE APPLICATION)
The process performed by the Certification Authority or its agent following submission of a Digital signature certificate application as a prerequisite to approval of the application and the issuance of a Digital signature certificate. (*See also* AUTHENTICATION; SOFTWARE VALIDATION)

VERIFY (A DIGITAL SIGNATURE)
In relation to a Digital Signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether —
(a) The initial electronic record was affixed with the Digital Signature by the use of private key corresponding to the public key of the Subscriber;
(b) The initial electronic record is retained intact or has been altered since such electronic record was so affixed with the Digital Signature.

VULNERABILITY
A weakness that could be exploited to cause damage to the system or the assets it contains.

WEB BROWSER
A software application used to locate and display web pages.

WORLD WIDE WEB (WWW)
A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

X.509
The ITU-T (International Telecommunications Union-T) standard for Digital signature certificates. X.509 v3 refers to Certificates containing or capable of containing extensions.