



**ICTA**

INFORMATION & COMMUNICATION  
TECHNOLOGIES AUTHORITY



# Information Guide for the Mauritian PKI Ecosystem



**CCA**

CONTROLLER OF CERTIFICATION  
AUTHORITIES OF MAURITIUS

# Contents

<b>Introduction</b>	<b>2</b>
<b>Public key Infrastructure Basics</b>	<b>2</b>
• What is Public Key Infrastructure (PKI)?	2
<b>What are Digital Signatures?</b>	<b>3</b>
<b>Salient features of the Electronic Transactions Act 2000 (as amended) in Mauritius</b>	<b>3</b>
<b>Salient features of PKI Regulations</b>	<b>4</b>
• Financial Standing	4
• Operational Criteria	5
• Government Certification Authorities	5
• Foreign Certification Authorities	5
<b>Summary of the Legal Framework</b>	<b>6</b>
<b>Operational Aspects</b>	<b>6</b>
• Management of Certificates	6
• Digital Certificates	7
• Obtaining a Certificate	8
• Certificate Storage	8
<b>PKI Provides Four Security Assurances</b>	<b>9</b>
• Confidentiality	9
• Digital Signature Generation	10
• Verifying a Digital Signature	10
• Authenticity, Integrity & Non - repudiation with Certificates	11
<b>PKI based Application</b>	<b>12</b>
• Signed and Encrypted Email - S/MIME	12
• Securing Online Application with Digital Certificates	12
• Typical Scenario	12
• mBanking Authentication	13
• mBanking: transaction Validation	14
<b>Conclusion</b>	<b>14</b>

# Information Guide for the Mauritian Public key Infrastructure

## Introduction

With the coming into operation of the first Certification Authority (CA) in Mauritius in May 2012, the Mauritian Public Key Infrastructure (PKI) is now operational. This CA will start its operation by issuing digital certificates to Mauritian end-users who will in turn use these certificates to secure their online transactions in a comprehensive manner.

The purpose of this guide is to flag out to the public in general the basic information they need to be availed of in order to understand the PKI concepts so as to be able to make full use of this dedicated security infrastructure which is the PKI.

## Public Key Infrastructure Basics

### What is Public Key Infrastructure (PKI)?

PKI stands for Public Key Infrastructure, an architecture put in place to prove the identities of people, websites, computer programmes and other applications on the Internet as well to secure online transactions.

In simple terminology, PKI can best be described and understood if we make a comparison between the non-electronic and electronic world.

In the non-electronic environment

- Signature of someone represents and validates the person's identity

In electronic environment, the reality is that :

- There is No paper and No pen;
- Further, the Parties may not even meet each other

The solution to address the electronic environment reality is :

- The use of digital signatures
- The use of the legislation gives legal sanctity to digital signatures, as:
  - It gives legal sanctity to records, files or documents that are retained in electronic form.
  - Puts in place legal standards for the use of electronic transactions, both in the public as well as in the private sector.

## What are Digital Signatures?

Digital signatures

- Are not scanned paper-based signatures
- Mathematically generated through the use of asymmetric cryptosystem
- Stronger than paper based signatures
- Tamperproof
- Also guarantees integrity of the electronic document

Digital signatures work on the basis that

- there is a third party whom both parties trust, who can verify that the electronic signature
  - belongs to the sender, and
  - the digital signature applied by the sender to an electronic message is the same electronic signature which the recipient extracts from the received message.


This trusted third party is the “certification authority”, who is entrusted with the responsibility of verifying the message sender’s identity.

## Salient features of the Electronic Transactions Act (ETA) 2000 (as amended) in Mauritius

The ETA clarifies the rights and obligations of transacting parties by setting out provisions dealing with issues related to the formation of electronic contracts. It also gives legal recognition on the use of electronic records and signatures and their secure counterparts.

The main features of the ETA are as follows:

- facilitate electronic communications by means of reliable electronic records;
- facilitate e-commerce and the promotion of the development of the legal and business infrastructure necessary to implement secure electronic commerce;

- 
- facilitate electronic filing of documents with government agencies and statutory corporations and to promote efficient delivery of government services by means of reliable electronic records;
  - minimise the incidence of forged electronic records, the intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;
  - help to establish uniformity of rules, regulations and standards regarding the authentication and other electronic transactions; and
  - promote public confidence in the integrity and reliability of electronic records and e-commerce, and foster the development of e-commerce through the use of electronic signatures to provide authenticity and integrity to correspondence in any electronic medium.

## Salient features of PKI regulations

### The Regulations

- put in place a licensing scheme for certification authorities (CAs).
- lay down the administrative framework for licensing by the Controller of CAs against payment of appropriate fees.
- stipulate the criteria for a CA in Mauritius to be licensed/recognised/approved and the continuing operational requirements after obtaining a licence.
- Criteria against which CAs will be evaluated:
  - their financial standing;
  - operational policies and procedures; and
  - the trustworthiness of their personnel.

### Financial Standing

- The licensing scheme is intended for individuals/companies operating in Mauritius.
- The applicant must demonstrate through submission of its business plan that it has sufficient funds to operate a CA, and have adequate insurance coverage to cover major areas of liability.

## Operational Criteria

- Prior to licensing, the applicant must undergo and pass an initial audit to demonstrate that it has met the requirements stipulated in the Act and the Regulation.
- In addition, the applicant will also be audited for compliance with its own Certificate Practice Statements (CPS).
- CPS are documents which stipulate the policies and procedures a CA adopts for the certificates it issues.
- Audits are also required again before a licence can be renewed.

## Government CAs

- Under the Act, a public sector agency may be approved by the Minister to act as a CA with the benefits of a licensed CA.
- With the exception of certain requirements (e.g. financial criteria), the Regulations will also apply to such government CAs.
- The Regulations which apply to licensed CAs will apply to Government/Approved CAs.

## Foreign CAs

- Criteria for the recognition of foreign CAs have been defined so as to ensure international recognition of certificates issued through the Mauritian PKI.
- The Regulations which apply to licensed CAs will apply to foreign/recognised CAs.
- This recognition element sets the basis for regional cooperation among SADC member countries to undertake PKI-based secured e-business practices.



## Summary of the legal framework – Electronic Transactions Act and Regulations

- The ETA and its corresponding Regulations aim to provide a legal framework that will establish trusted CA services in Mauritius, serving both the domestic and international markets.
- In the long term, they provide the foundation to establish Mauritius as a trusted hub by providing a wide range of security products and services.
- With a harmonised legal framework within the countries of the SADC region, a common operational framework for the region can be envisaged for cost-effectiveness purposes which can boost regional e-commerce/e-business activities.

## Operational Aspects

### How PKI works?

- The sender, who may be a user or an organisation, first registers with the CA for an electronic identity.
- This electronic identity takes the form of a **“certificate” (public key)** issued by the certification authority and stored by the CA in its online repository.
- This public key has a corresponding unique electronic key issued to the sender, which is only known to the sender (**private key**).
- Like a secret personal code, the sender uses this private key, which is normally stored on a secure device such as a smart card to digitally sign his identity on the message.
- Upon receipt of a digitally signed message, the recipient consults the CA repository to ascertain the sender’s electronic identity.

## Management of Certificates

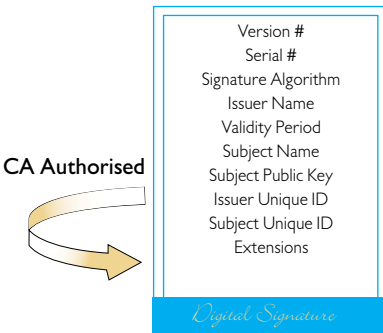
- In a PKI, the Certificate Authority (CA) issues Digital Certificates to applicants.
- A Digital Certificate on the Internet is similar to an ID card in the real world.
- The CA also verifies the identity of applicants, and publishes certificates on an on-line repository where people can look up others’ certificates.

- The management of certificates is a core function of a CA and is subject to strict requirements.
- The Controller must approve the methods used by the licensed CA to verify the identity of a subscriber before granting or renewing a subscription for a certificate.
- In accordance with the provisions of the Act, a licensed CA must also publish:
  - a notice of a certificate suspension or
  - revocation immediately after receiving an authorised request for a certificate suspension or revocation.

### Digital Certificates

- A Digital Certificate is an X.509 defined data structure with a Digital Signature.
- The data represents who owns the certificate, who signed the certificate, and other relevant information.

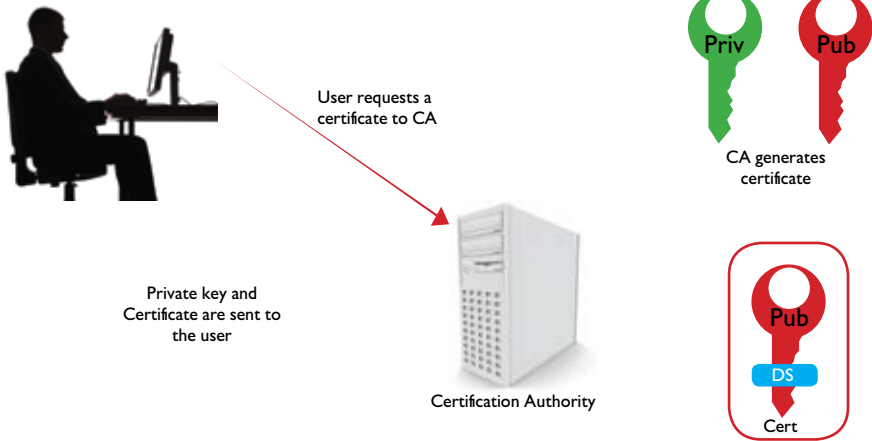
### X.509 Certificate



- When the signature is generated by a Certification Authority (CA), the signature can be viewed as trusted.
- Since the data is signed, it cannot be altered without detection.
- Extensions can be used to tailor certificates to meet the needs of end applications.



## Obtaining a Certificate



## Certificate Storage

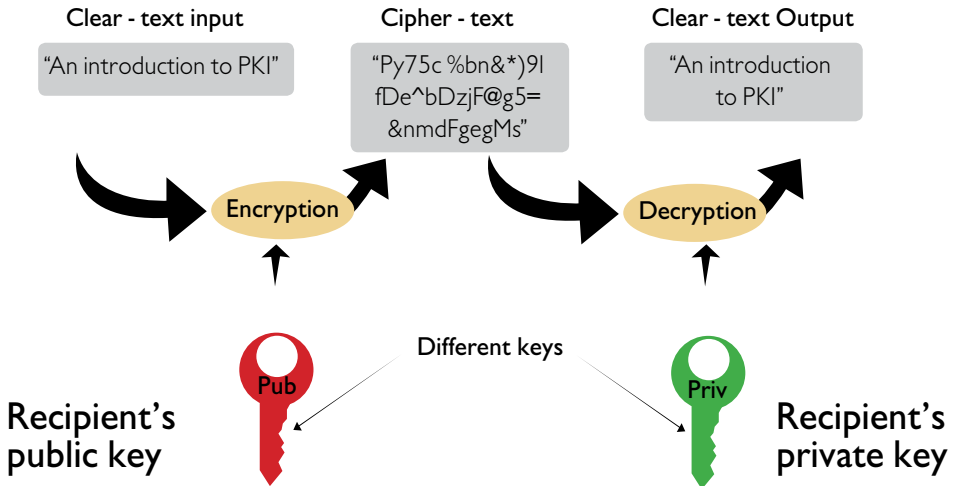
- Typically, private keys and certificates are stored in PC disk memory ("soft certificates") or externally on user-centric hardware such as a smart card device or a USB token ("hardware certificates").
- Mobile phones with PKI enabled SIM.
- Factors to be considered for storage choice:
  - the value and content of the data,
  - usability,
  - compliance needs, and
  - convenience of accessing the private key and certificate.
- The decision about how to store certificates and private keys should reflect a pragmatic balance of these factors.

## PKI Provides Four Security Assurances

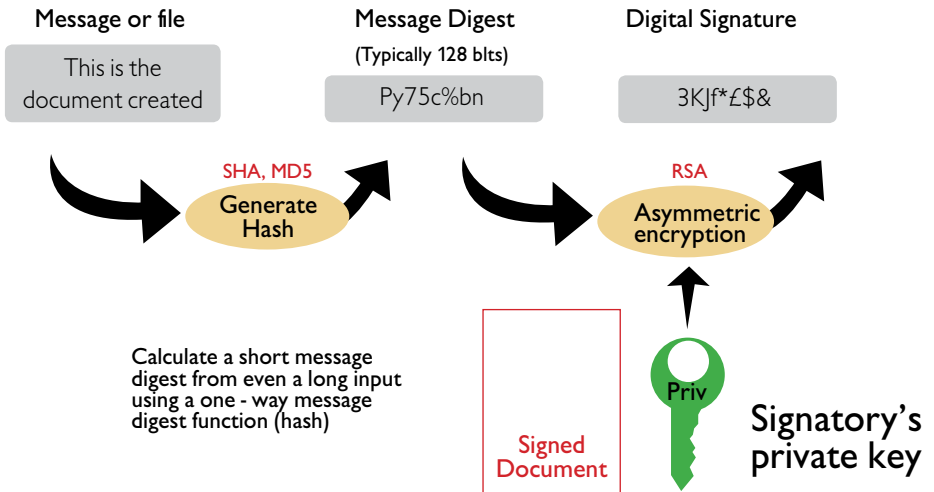
- Confidentiality (The *inability to read* it other than by the sender and addressee)
- Authenticity (Assurance of a message *source*)
- Integrity (Assurance that a message is *unaltered* since sent)
- Non-repudiation (The originator's *inability to deny* having sent the message)

### Confidentiality

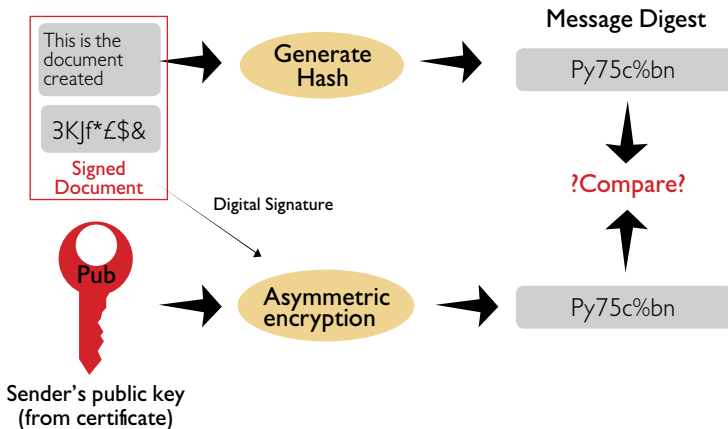
Enabling confidentiality with PKI



## Digital Signature Generation



## Verifying a Digital Signature



## Authenticity, Integrity & Non-repudiation with Certificates

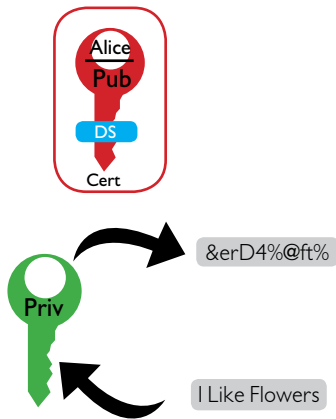


Alice



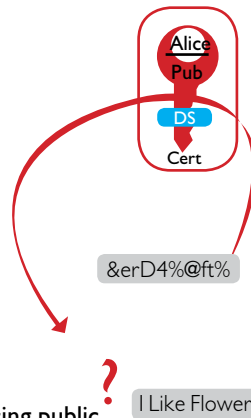
Bob

### Certificate is sent for authentication



Bob verifies the digital signature on the certificate

He can trust that the public key really belongs to Alice, but is it Alice standing in front of him ?



Bob challenges Alice to encrypt for him a random phrase he generated

Decrypt using public key in certificate and compare

## PKI - Based Applications

### Signed and Encrypted Email - S/MIME

- S/MIME – Secure Multipurpose Internet Mail Extensions
- Prevent email spoofing
  - Helps preventing forged email
  - Helps preventing spam
- Protect sensitive messages & documents
- Secure business processes
  - Signed messages
  - S/MIME-based applications

### Securing online applications with Digital Certificates

#### Typical scenario



Citizen connects to server (thru' SSL)

Client component is downloaded to the citizen's machine

Citizen fills form & clicks submit button

Citizen uses her private key to sign the data

Signed data is encrypted with server public key & sent

Server decrypts signed data and performs verification and validation checks

Successful check will result in server generating and sending a receipt

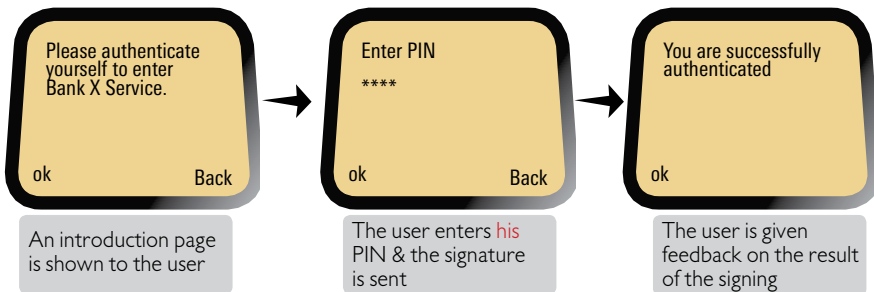


Following Validation done

- Date integrity verification
- Signer certificate is expired?
- Signer certificate is trusted?
- Signer certificate is compromised?

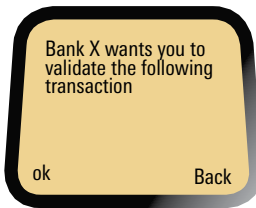
## mBanking Authentication

1. End user accesses bank website with his mobile phone with **PKI** based SIM Card
2. Bank system sends authentication request to Operator's WPKI server, based on user credentials (phone number)
3. Users enters his authentication PIN
4. Access to the bank service is allowed

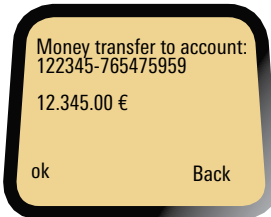


## mBanking: Transaction Validation

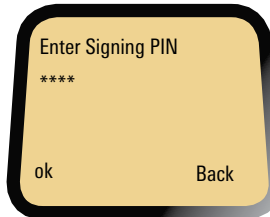
An introduction page is shown to the user



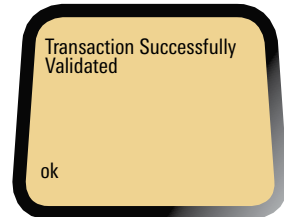
1. Bank sends validation request to Operator's WPKI service
2. The signature process is WYSIWYS (what you see is what you sign)



The text to be signed by the users is displayed



The user enters his PIN and the signature is sent



The user is given feedback on the result of the signing

## Conclusion

The purpose of this guide is to give an insight into the PKI. Definitions of terms commonly employed have been defined in simple terms. The salient features of the laws related to the PKI are presented. The operating mechanics including typical examples depicting the illustrative uses of PKI have been presented.

Please feel free to visit the website of the CCA of Mauritius on <http://www.cca.mu> for more detailed information on the PKI framework in Mauritius. A Discussion Forum has also been created on the website inviting any views and suggestions that you may have.









**ICTA**

INFORMATION & COMMUNICATION  
TECHNOLOGIES AUTHORITY

Email: [icta@intnet.mu](mailto:icta@intnet.mu)

Website: <http://www.icta.mu>



**CCA**

CONTROLLER OF CERTIFICATION  
AUTHORITIES OF MAURITIUS

Email: [info@cca.mu](mailto:info@cca.mu)

Website: <http://www.cca.mu>

Level 12 - the Celicourt - 6, Sir Celicourt Antelme Street - Port Louis - Mauritius  
Tel: (230) 211 5333/4 Fax: (230) 211 9444