emudhra
Trust Delivered

CASE STUDY

Mauritius Government goes Digital using PKI

Mauritius Government goes Digital using PKI

eMudhra helps Mauritius Government to implement a National PKI infrastructure

Industry
Government

e-Governance Initiative
The Government of Mauritius laid out a comprehensive strategy for Digital Transformation. In 2012, one of the key initiatives was to implement a National PKI infrastructure to facilitate secure electronic commerce using Digital Signatures based on UNCITRAL Model Law for usage of e-Signatures.

Government Need
Setup Root Certifying Authority infrastructure and issue licenses to licensed Certifying Authorities for digital signature issuance.

Approach
Deploy an integrated approach for setup of data centre, procurement of hardware, setup of necessary CA software for Certificate Lifecycle Management and create the trust chain for Certifying Authorities to operate in Mauritius.

Background
The ICTA agency in Mauritius being keen on promoting e-Governance and Digital Transformation wanted to implement a National PKI infrastructure to facilitate secure electronic commerce using Digital Signatures based on UNCITRAL Model Law on Electronic Signatures. There was an increased global adoption of Digital Signatures for Government to Citizen services and Banking Systems as a result of several countries having established PKI infrastructure and licensed Certifying Authorities issuing Digital Signatures for use in online commerce.

Implementing the National PKI infrastructure gradually enhanced the security of online transactions and electronic payment systems. Over time, increased global adoption promoted the use of digital signatures in Government to Citizen services and Banking to enhance security and enable digital transformation into a completely paperless environment. This significantly reduced operational costs, improved customer experience and improved convenience for citizens of Mauritius.

Digital Signature Technology

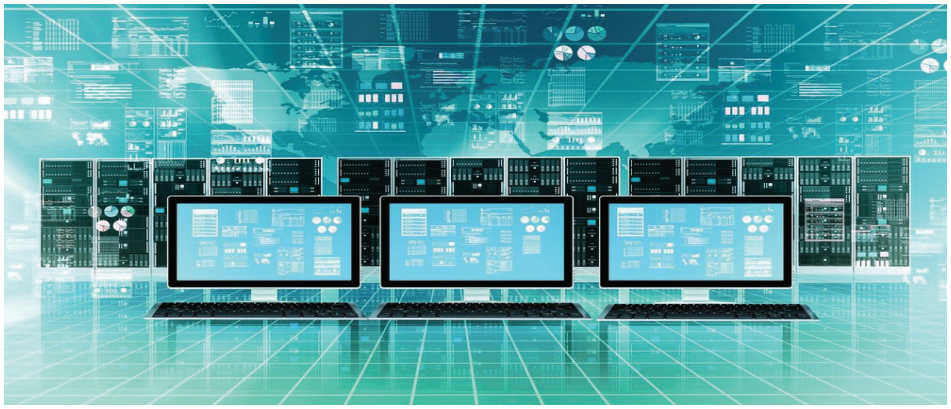
The Digital Signature Technology works on the Public Key Infrastructure framework which uses a Cryptographic Key Pair – Private and Public Key for secure access and transmission of Information using advanced encryption standards that are global.

The PKI framework has been adopted as law in several countries worldwide hence providing Digital Signatures the same legal validity as wet signatures.

Outcome

ICTA, Mauritius was able to implement Root CA infrastructure in a quick timeframe.

- eMudhra became the first licensed Certifying Authority to issue Digital Signatures to citizens of Mauritius
- ICTA, Mauritius has been able to successfully complete Microsoft Root CA audit for being trusted as part of the Microsoft list of trusted Certifying Authorities
- Public Procurement Office has been the first department to go LIVE with the usage of digital signatures
- eMudhra is working closely with the ICTA and Government of Mauritius to enable large scale Digital Transformation using digital signatures



Solution

eMudhra, India worked closely with the ICTA in Mauritius to setup the Root CA infrastructure and become the first licensed CA to operate in Mauritius by using Digital Signatures in PDF/XML documents.The solution was able to validate the signer and contents of the document before accepting submission. This ensured error free filing of documents with the department.

This included:

- **Consulting** – Provide detailed training sessions, workshops, consulting on the policies, audit procedures, system, data centre and hosting architecture for ICTA to operate the root CA infrastructure
- **Implementation** – Advise on the procurement of necessary hardware including Hardware Security Module and software (both System software and application) for Certificate Lifecycle Management
- **Rollout** – Hardware and software configuration, key ceremony for issuance of Certificates to first Licensed Certifying Authority
- **Hosting of Licensed CA Infrastructure** – Included partnering with National Computer Board to host eMudhra CA infrastructure
- **Certificate Lifecycle Management** – Implementation of emCA for Certificate lifecycle management (issuance, revocation, CRL/OCSP management, time stamping)

The emCA solution comprises of the following broad modules:

- **eMudhra Authentication Server** – To authenticate, verify digital signature certificates on real time basis
- **Configuration Module** – Signature, Encryption & HSM
- **CRL** – Ability to publish Certificate Revocation List
- **OCSP (Server and Client)** – Online Certificate Status Protocol to check status of Certificates
- **Time Stamping Server** – Ability to provide a reliable time source for Digital Signatures
- **Hardware Security Module** – FIPS 140-2 level 3 certified physical computing devices that safeguards and manages digital keys for strong authentication and provides crypto processing
- **Certificate Lifecycle Management Module** –
  - **Certificate Issuance** – To manage the issuance, revocation of Digital Signature certificates
  - **Certificate Download** – For downloading Digital Certificates from Certifying Authority (CA) as a soft or crypto token
  - **Certificate Registration** – To allow the customer to register their digital signature on the Banking application

About eMudhra:

Much like the name, which is an embodiment of the seal of authenticity in the electronic or digital world, eMudhra is a cyber security solutions company and a trust service provider that is focused on accelerating the world's transition to a secure integrated digital society. With presence in 5 continents and a global delivery center in Bengaluru, India, eMudhra is empowering secure digital transformation of over 45 global banks, several Fortune 100 customers and thousands of SMEs.