

## ***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 trustworthiness of its personnel.

## ***Licensing Scheme*** (*sec 5 – sec 7 of Reg.*)

- The licensing of a CA by the Controller is an indication that the CA has met the stringent regulatory requirements established.
- It is thus an indication to the public that the CA is trustworthy and deserving of consumer confidence.
- 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. (*3<sup>rd</sup> schedule of Reg. – sec 1*)

## ***Operational Criteria*** *(3<sup>rd</sup> Schedule of Reg. – Sec 2)*

- 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). *(sec 26 of Act & sec 29 of Reg.)*
- 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.

## ***Security Guidelines***

*(sec 30 of Reg.- Will be issued as 'IT Security Directives' & 'Security Directives for CA')*

- The Controller will issue a set of security guidelines as Directives as and when required and CAs will be audited against.
- These security guidelines are specially tailored for CA operations.
- In addition to general security requirements, there are specific requirements governing CA operations such as certificate and key management.

## ***Requirements on Record Keeping*** *(sec 22 of Reg.)*

- Licensed CAs must have reliable records and logs for activities that are core to the CA's operations.
- These activities include
  - certificate management,
  - key generation and
  - administration of its computing facilities.
  - To enable verification of past transactions, licensed CAs have to archive certificates for a minimum of ten years.

## ***Management of Certificates***

*(sec 23 of Reg. & as per conditions specified in the CPS)*

- 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 *(sec 31 of Act & sec 26 of Reg.)*
  - revocation immediately after receiving an authorised request for a certificate suspension or revocation *(sec 32 of Act & sec 27 of Reg.)*

## ***Confidentiality Requirements*** *(sec 32 of Reg.)*

- Licensed CAs have to ensure confidentiality of subscriber information.
- This is to prevent abuse of the subscriber's trust in providing potentially private subscriber information to the CA when applying for a certificate.

## **Government CAs** (sec 14 of Reg.)

- 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*** *(sec 9 of Reg.)*

- 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 also apply to both foreign and recognised CAs

## ***Conclusion***

The Act and the Regulations aim to provide a legal framework that will establish trusted CA services in Mauritius, serving both the domestic and international markets.