National Public Key Infrastructure (NPKI)

Interregional Standardization Forum for PKI & e-Trust

4-5th April 2019

Introduction

The Public key infrastructure (PKI) is the set of hardware, software, policies, processes, and procedures required to create, manage, distribute, use, store, and revoke digital certificates and public-keys.

Digital certificates are the credentials that facilitate the verification of identities between users in a transaction

PKIs help establish the identity of people, devices, and services – enabling controlled access to systems and resources, protection of data, and accountability in transactions.

Public Key Infrastructure (PKI)

Different types of systems in a PKI:

1.**Private and Public Key Systems**: Private systems are symmetric cryptography and a public systems are asymmetric cryptography. Currently, public key systems are the most common.
2.**Symmetric Encryption Systems**: The same key is used for both the processes of encryption and decryption.
3.**Asymmetric Encryption Systems**: A different key is used for each process. One key is the public key and the other key is the private key. If something is encrypted with the public key, then decryption can only be done with the private key. Alternatively, if something is encrypted with the private key, then decryption must be done only with the public key.

National Public Key Infrastructure (NPKI)

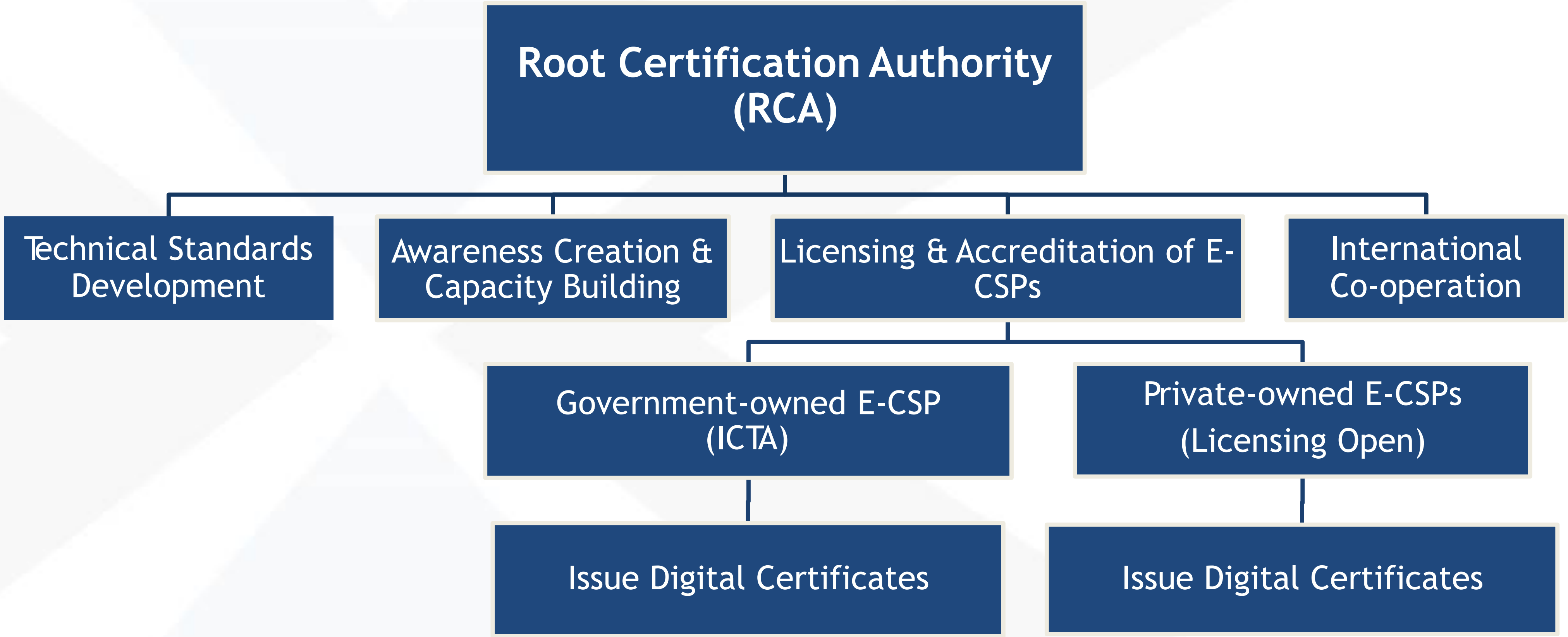
The **National Public Key Infrastructure (NPKI)** project is coordinated by the Ministry of ICT in collaboration with the Communications Authority of Kenya (CA).

Kenya’s National PKI comprises of a Root Certification Authority (RCA), which is managed by the Communication Authority of Kenya (CA), and the Government Certification Authority (GCA), an Electronic Certification Service Provider (E-CSP) which is managed by the ICT Authority (ICTA).

National Public Key Infrastructure (NPKI)

- NPKI launched in 2013
  - Kenya ICT Board
  - Samsung SDS
  - Korea Information Certificate Authority Inc.
    - http://icta.go.ke/the-national-public-key-infrastructure-npki/

NPKI Structure Cont……



Root Certification Authority (RCA)

- Technical Standards Development
- Awareness Creation & Capacity Building
- Licensing & Accreditation of E-CSPs
  - Government-owned E-CSP (ICTA)
    - Issue Digital Certificates
  - Private-owned E-CSPs (Licensing Open)
    - Issue Digital Certificates
- International Co-operation

Why use a Digital certificate ?

- Operates under the Kenyan law
- Ability to digitally **sign** electronic data and information to ensure **integrity** of the data and **non-repudiation**.
- To confirm whether the transaction has been changed or not
- Ability to **encrypt** electronic data and information to ensure **confidentiality**.