East African Communications Organisation

Communications for all in East Africa

STANDARDS ON NATIONAL PUBLIC KEY INFRASTRUCTURE

Prepared by EACO

July 2017

STANDARDS ON NATIONAL PUBLIC KEY INFRASTRUCTURE

A public key infrastructure **(PKI)** is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

I. Current Status in East Africa

	County	Status of Deployment and Legislation on NPKI	Challenges Faced so Far
1.	Rwanda	• Root Certification Authority (RCA) was deployed in 2013; managed by Rwanda Utilities Regulation Authority (RURA). • One government Certification Authority (RGCA) is in place and managed by Rwanda Development Board (RDB) – started issuing digital certificates in e-procurement and over 1000 certificates issued. • The ICT Law 2016. • Draft regulations and guidelines are under review.	• Many of the existing applications are sourced from outside the country therefore difficulties in integration. • No standard APIs have been adopted in the country • Need for govt. (at highest level) to take the lead in adoption of NPKI by both public and private sector. • Awareness creation.
2.	Kenya	• RCA deployed in 2014 and managed by Communications Authority	• Licensing of the first Government Certification Authority (ICTA) has taken too long. • Need for faster adoption of digital certification services by the public

		of Kenya (CA). • In the process of licensing the first Government CA (ICT Authority). • National ICT Sector Policy, 2006 • Kenya Information and Communications Act (KICA) of 1998 • Electronic Certification and Domain Name Administration Regulations, 2010 (under review) • Electronic Certification Service Providers (E-CSP) Licensing Framework • National Cybersecurity Master Plan (NCSP). • Draft regulations and the Kenya ICT Policy 2016 are under review.	and private sectors especially by financial institutions. • Awareness creation.
3.	Uganda	To get a position • Electronic Signatures Act, 2011 • Electronic transactions Act 2011 • E-Transaction Regulations 2011 • Electronic Signatures Regulations, 2013 • Bank of Uganda Mobile	N/A

		Money Guidelines, 2013	
4.	Tanzania	• Under the Ministry of Work, Transport and Communication. • Proposal has been accepted. • Currently in the benchmarking stages. • National ICT Policy 2003 • E-Transactions Act, 2015. • Bank of Tanzania (BOT) have developed a draft for the E transaction	• Bureaucracy in procurement. • Shortage of technical skills and expertise.
5.	Burundi	• Deployment has not commenced • E-Transaction Policy under review under the Central Bank	N/A

II. Cross Certification recommendations.

Necessity for Technical PKI Standards:

- To narrow the implementation scope of the global standard
- To implement PKI interoperability among national accredited CAs
- To protect local company from global IS product and To promote national PKI

1. Objectives for Standard Legislation

- Maintain international interoperability.
- Secure mutual operation for certificate issuance and certificate practices within the digital signature management system based on the Digital Signature Act.

2. **Objectives for Technical Standards**

- Defines the basic field and extension field within the certificate, its objective and its structure.
- Describes all the requirements needed for the root certification authority **(RCA),** accredited certification authority **(CA)** and subscriber's software for certification practices.

3. **Objectives for Industry Standards**

- Defines the certificate profile in domestic digital signature certification management system.
- Contributes to the technical success and related service activation.

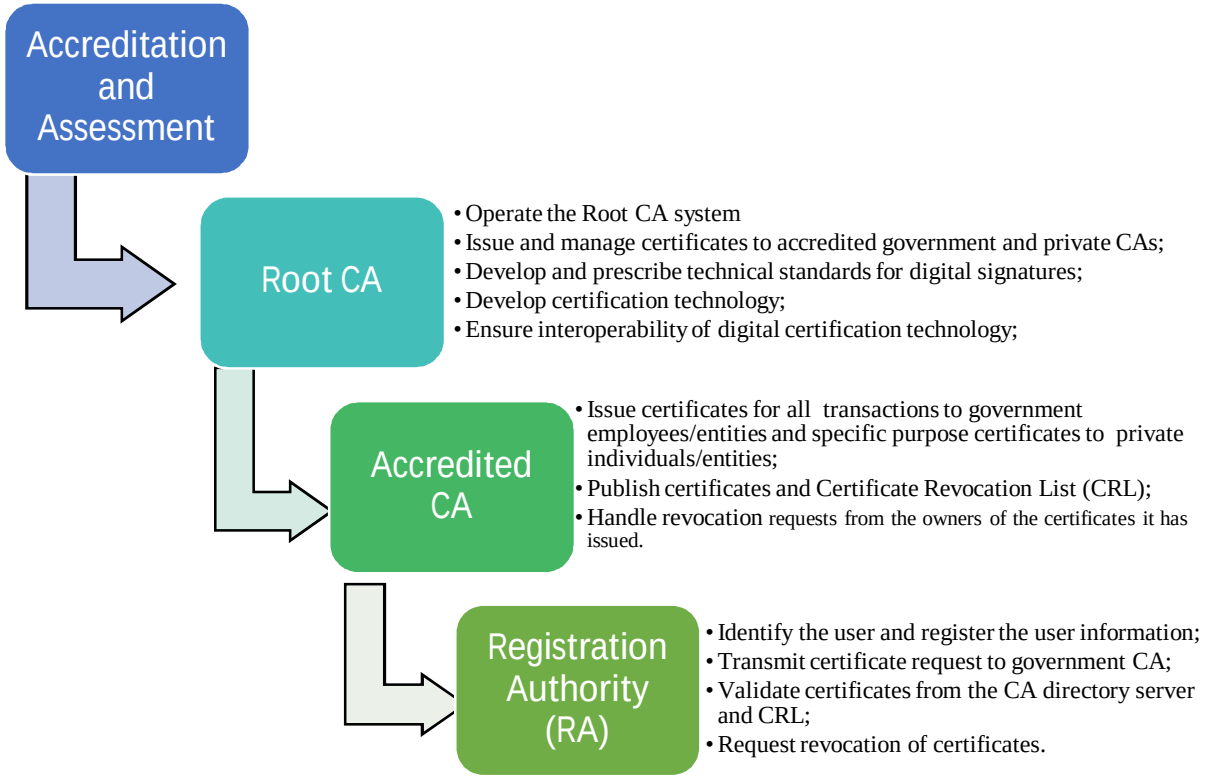
4. **Design of International Cross Certification Model using Cross Certificate**

- Cross Recognition (CR): This is an interoperability arrangement in which a corresponding party in one PKI domain can use authority in another domain to authenticate a subject in the other PKI domain, and vice versa.
- Certificate Trust List (CTL): A CTL is a signed Public Key Cryptography Standards (PKCS) data structure that can contain, among other things, a list of "trusted CAs". A "trusted CA" is identified with the CTL by a hash of the public key certificate of the subject CA.
- Cross Certification (CC): A certification authority may be the subject of a certificate issued by another certificate authority (CA).

Among EAC members, Kenya and Rwanda has already implement the NPKI and they learned the best practice from the NKPI of South Korea. For a successful implementation of the NPKI a nation should follow the scope of PKI model:

- *PKI Scheme: PKI Organization and Hierarchy*
- *Law & Regulation: CP/CPS Guidelines; Facilities and equipment guidelines, accreditation and auditing criteria*
- PKI Center :Root CA, Accredited CA, Facilities & Equipment, Operational guidelines
- Technical Standards: PKI International Standards

1. **PKI Scheme: PKI Organization and Hierarchy**



2. Law & Regulation

It is recommended that the accredited CA shall carry out accreditation and distribute relevant evaluation criteria including PKI system requirements, facilities and equipment requirements and technical standards. Therefore EAC members must have more detailed regulations for operation, for example the following should be considered while designing regulations for NPKI:

Index	Contents
Identification	User information and methods for new issuance, renewal, re-issuance,

	suspension and revocation application
Operational Requirements/ Certification Service	- Reasonable methods to identify the certificate applicants - Technical procedure and subscriber obligation for new issuance, renewal, re-issuance, suspension and revocation application
Facilities & Equipment	- To protect against all physical attacks, relevant procedures should be included - In the case of the termination of CA's operations, CA should notify it to subscribers and users and then notify it to Root CA
Technical Security Management	- Information on public key generation and private key management - The key size and hash value should be determined in according to used digital signature algorithm - Information and methods for system security control, operational control and network security control
Accredited Certificate, CRL profile	- Detailed information on certificate profile, CRL profile
Audit & Regular Maintenance Check about Certification Service	- CA should be annually audited by Root CA to check facilities and equipment secure operation - Information on Identification and qualifications of the auditor
Business and Relevant Laws	- CA's warranty should be stated in the relevant law - Information on compliance with the relevant law

KEY PERFORMANCE INDICATORS FOR THE STRATEGIES DEVELOPED BY THE MEMBERS

ToR: Strategies on ICT Service Transactions and Applications

To devise strategies for stimulation of demand and uptake of ICT enabled services and applications.

The ITU developed Key telecommunication/ICT monitoring and performance indices in the mobile, fixed and mobile broadband services, home ICT access, and more.(EGH ITU Expert Group on Household) EGTI (ITU Expert Group on Telecommunication Indicators)

ICT related services and applications today include and are not limited to;

1. E-governance applications
2. E-Agriculture
3. E-learning
4. E-Health
5. E-Commerce

Access and Usage surveys must be done to obtain monitoring information for the demand and uptake of these services to determine the Indicators of Demand and uptake.

S.No	ICT Service	Indicators of growth In demand
1.	**E-Learning** This happening mostly in academic institutions like, Primary, Secondary and Tertiary institutions. In Uganda's case, we have applications and activities enabling E-learning; (Community Training, Teacher retooling, and Cyber School Technology Solutions).	1. Number of education Institutions with Computers 2. Number of Computers in the education Institution 3. Number of education Institutions subscribing for Internet 4. Bandwidth Usage 5. Total Enrollment for ICT-related courses at Tertiary level 6. Enrollment for Online Courses 7. Number of candidates (Primary and Secondary) registered for National Examinations 8. Enrollment for Science subjects in Schools. 9. Frequency of community training requests from local leadership 10. Number of ICT cafes and training facilities in the community as a result of the training 11. Number of teachers that have been trained by retooled teachers

2.	**E- governance** Applications have been putting place for Business License registration, utility payment, e-visa application, e-tax	1. Number of Tax transactions online 2. Number of Online registered tax payers 3. Number of E-Visa Applications 4. Number of local businesses registered 5. Number of government offices with computers 6. Number of government offices subscribing to Internet 7. Bandwidth Usage
3.	**E-Health** Applications have been designed for birth registration, Health Management Information Systems have been put in place	1. Number of Health facilities with HMIS 2. Number of Health facilities with computers 3. Internet subscriptions 4. Online Registered births in the country 5. Number of online health insurance records
4.	**E-Agriculture and E-Commerce**	1. Number of persons with computers 2. Number of persons using the online payment platforms (pay way etc) 3. Mobile Money subscriptions 4. Volume of Mobile Money Transactions 5. Number of online utility payments (Water, Electricity,etc) 6. Online bank transactions 7. Number of mobile money agents
5.	**General ICT Related services** A survey can be done at the following levels; Individual or Household but using the same Indicators	**For both households and Individuals (ITU);** 1. Proportion with a computer 2. Proportion with Internet subscription 3. Proportion using internet by type of activity 4. Proportion using internet by type of activity 5. Barriers to Internet Access 6. Proportion with a mobile phone 7. Subscriber Numbers for Voice and Mobile Data 8. Internet Bandwidth Usage (Trends) 9. Voice traffic (Minutes)