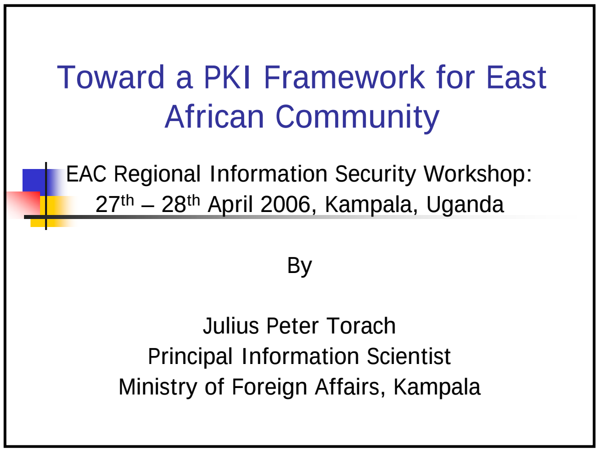
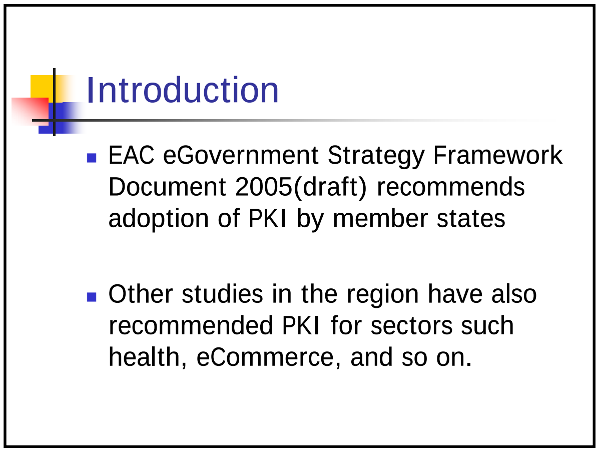


Toward a PKI Framework for East African Community

EAC Regional Information Security Workshop:
27th – 28th April 2006, Kampala, Uganda

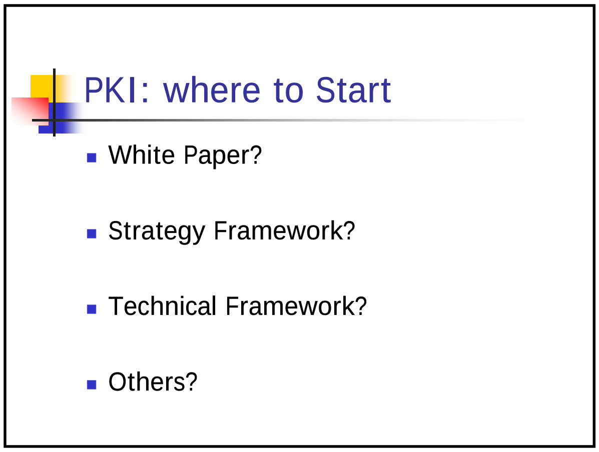
By

Julius Peter Torach
Principal Information Scientist
Ministry of Foreign Affairs, Kampala



Introduction

- EAC eGovernment Strategy Framework Document 2005(draft) recommends adoption of PKI by member states
- Other studies in the region have also recommended PKI for sectors such health, eCommerce, and so on.



PKI: where to Start

- White Paper?
- Strategy Framework?
- Technical Framework?
- Others?

Agenda

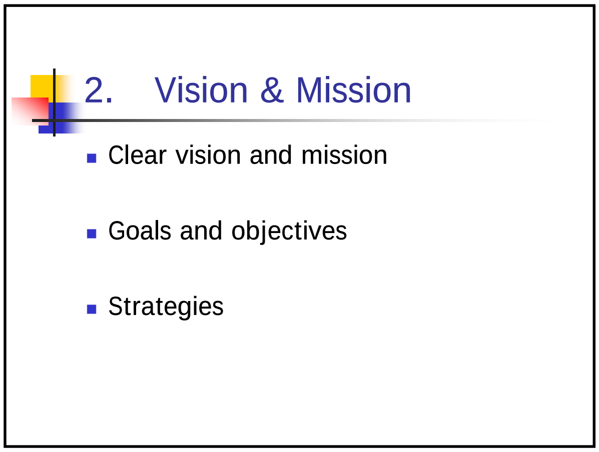
- Proposed sections of a PKI a strategy framework

PKI Deployment Framework

- Structure and frame for considering and solving problems
- Should aim at identifying and developing plans, processes, and the documents necessary for successful national/regional PKI
- Will facilitate PKI development, procurement, deployment, or regulation

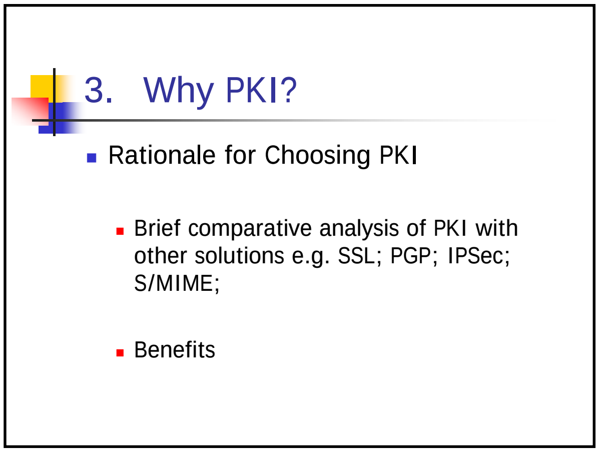
1. Situational Analysis

- Situations in Member States
- Situation at EAC Secretariat (Regional)



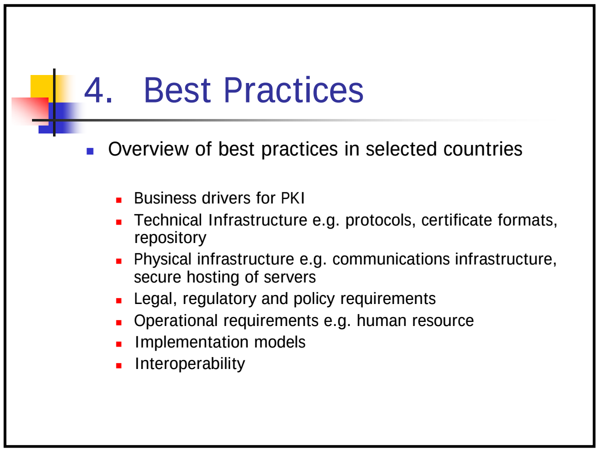
2. Vision & Mission

- Clear vision and mission
- Goals and objectives
- Strategies



3. Why PKI?

- Rationale for Choosing PKI
  - Brief comparative analysis of PKI with other solutions e.g. SSL; PGP; IPSec; S/MIME;
  - Benefits



4. Best Practices

- Overview of best practices in selected countries
  - Business drivers for PKI
  - Technical Infrastructure e.g. protocols, certificate formats, repository
  - Physical infrastructure e.g. communications infrastructure, secure hosting of servers
  - Legal, regulatory and policy requirements
  - Operational requirements e.g. human resource
  - Implementation models
  - Interoperability

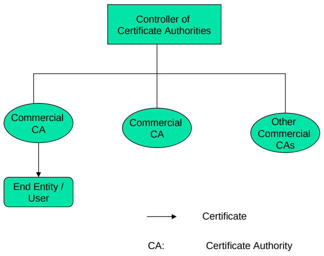
5. Critical Success Factors

- Privacy
- Maintaining trust
- Application development guidelines
- Capacity building
- Awareness
- Interoperability

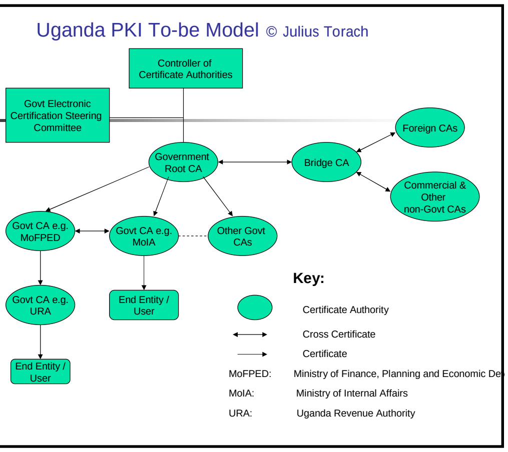
5. Generic PKI Models

- Hierarchical model
  - the root CA of the hierarchy is trusted by all relying parties, i.e., it is the sole trust anchor in the model
- Direct (Peer-to-Peer) Model
  - thereby no root CA and no single trust anchor; any CA can establish a trust relationship to any other peer CA
- Distributed Web-of-trust
  - No trusted third party vouches for the identity or integrity of any end entity e.g. Pretty Good Privacy (PGP)
- Hybrid Trust Model
  - obtained by mixing/combining models
- Bridge CA
  - CA called the Bridge CA acts as a mediator, i.e., it introduces one organization to another instead of bilaterally cross-certifying each other

Uganda PKI AS-IS Model © Julius Torach



Uganda PKI To-be Model © Julius Torach

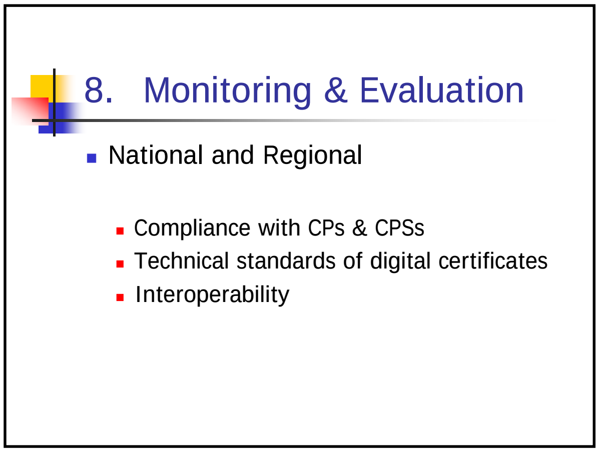

Controller of Certificate Authorities
Govt Electronic Certification Steering Committee
Foreign CAs
Government Root CA
Bridge CA
Commercial & Other non-Govt CAs
Govt CA e.g. MoFPED
Govt CA e.g. MoIA
Other Govt CAs
Govt CA e.g. URA
End Entity / User
End Entity / User
Key:
Certificate Authority
Cross Certificate
Certificate
MoFPED: Ministry of Finance, Planning and Economic De
MoIA: Ministry of Internal Affairs
URA: Uganda Revenue Authority

EAC Model: Key Questions

- Should EAC Secretariat in Arusha act a bridge CA to the member states?
- Should each member state have a bridge CA that cross-certify each other?

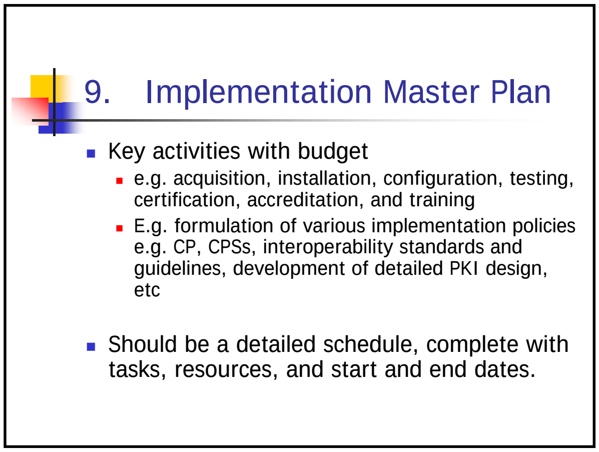
6. Institutional Framework

- EAC PKI Advisory Committee
- National PKI Steering Committees
- Designated national institutions to monitor, regulate and coordinate PKI activities
- Governmental PKI Operators with Governmental Root CA
- EAC & National Bridge CA Operators
- Sector CAs



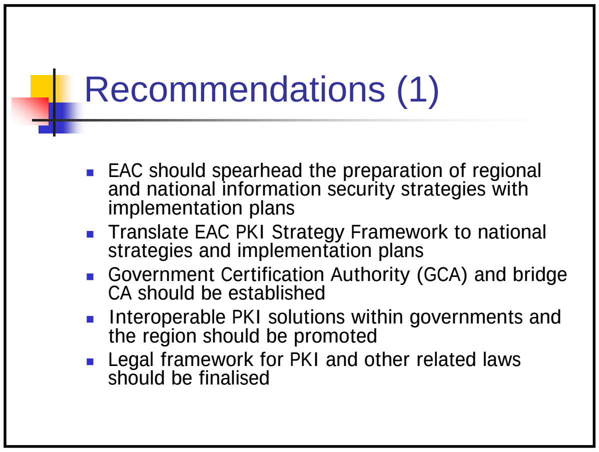
8. Monitoring & Evaluation

- National and Regional
  - Compliance with CPs & CPSs
  - Technical standards of digital certificates
  - Interoperability



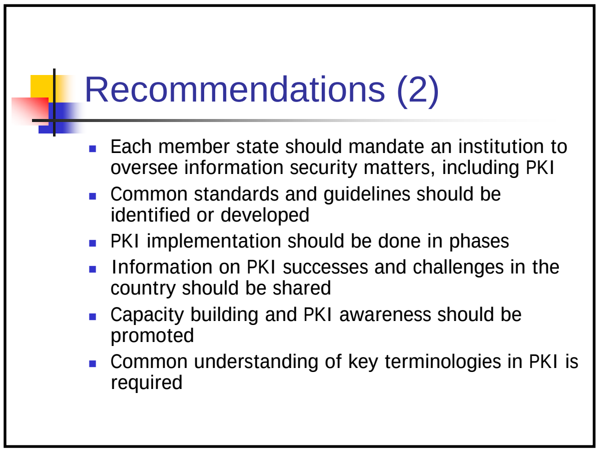
9. Implementation Master Plan

- Key activities with budget
  - e.g. acquisition, installation, configuration, testing, certification, accreditation, and training
  - E.g. formulation of various implementation policies e.g. CP, CPSs, interoperability standards and guidelines, development of detailed PKI design, etc
- Should be a detailed schedule, complete with tasks, resources, and start and end dates.



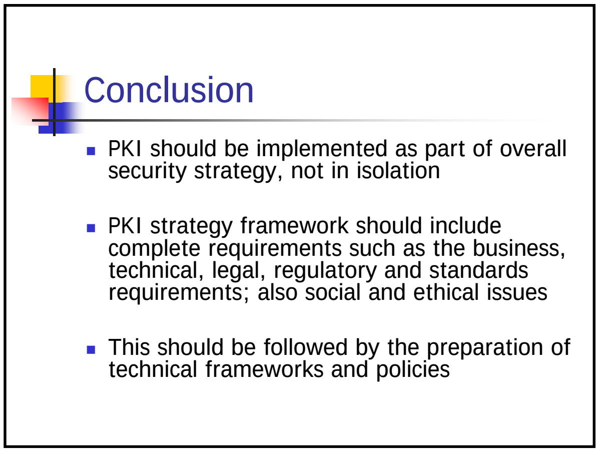
Recommendations (1)

- EAC should spearhead the preparation of regional and national information security strategies with implementation plans
- Translate EAC PKI Strategy Framework to national strategies and implementation plans
- Government Certification Authority (GCA) and bridge CA should be established
- Interoperable PKI solutions within governments and the region should be promoted
- Legal framework for PKI and other related laws should be finalised



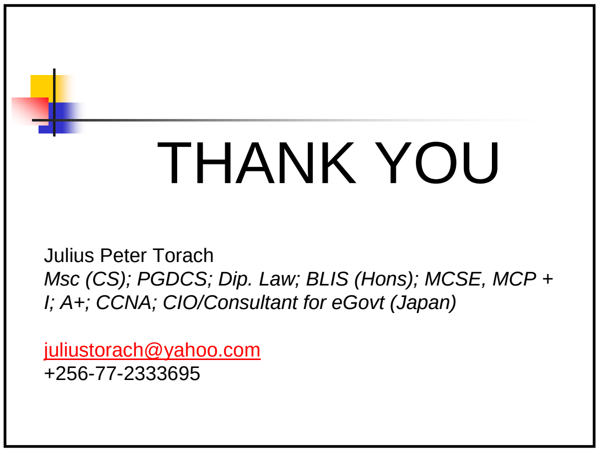
Recommendations (2)

- Each member state should mandate an institution to oversee information security matters, including PKI
- Common standards and guidelines should be identified or developed
- PKI implementation should be done in phases
- Information on PKI successes and challenges in the country should be shared
- Capacity building and PKI awareness should be promoted
- Common understanding of key terminologies in PKI is required



Conclusion

- PKI should be implemented as part of overall security strategy, not in isolation
- PKI strategy framework should include complete requirements such as the business, technical, legal, regulatory and standards requirements; also social and ethical issues
- This should be followed by the preparation of technical frameworks and policies



THANK YOU

Julius Peter Torach
Msc (CS); PGDCS; Dip. Law; BLIS (Hons); MCSE, MCP + I; A+; CCNA; CIO/Consultant for eGovt (Japan)

juliustorach@yahoo.com
+256-77-2333695