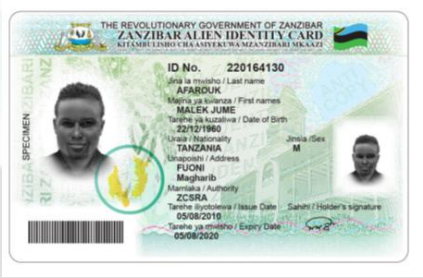
Reliable Identification in Digital Transformation

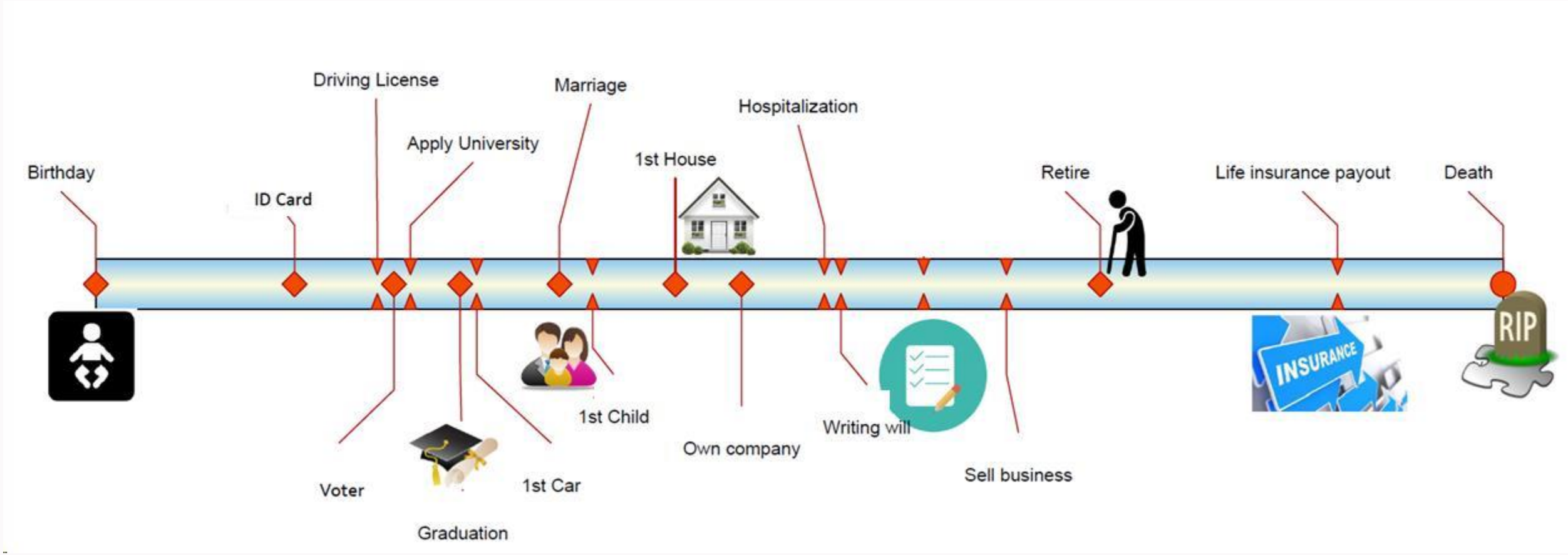


SoftNet
Creativity at Work

Nuru Yakub Othman

Zanzibar ICT Summit- Oct 2022

Significance / Importance



*All phases require reliable identification

RELIABLE IDENTIFICATION

- **Recognition** of individuals and the ability to **verify** that they are who they claim to be
- In a valid and agreed form / type
- Provided by the rightly recognized authority(ies), after following the right process
- Can be trusted; Prevents impersonation and identity fabrication
- Proper usage is enforced
- There are consequences for misuse

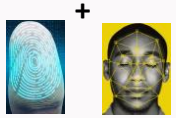
FORMS OF DIGITAL IDENTIFICATION

- In a Digital World, Reliable identification has to be done Digitally, with ability to offer digital verification

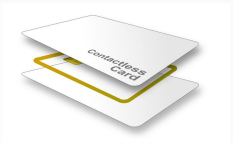
- The most common forms of Digital Ids:
  - Number and Biometrics

123683-56875

+



  - electronic Smart Card

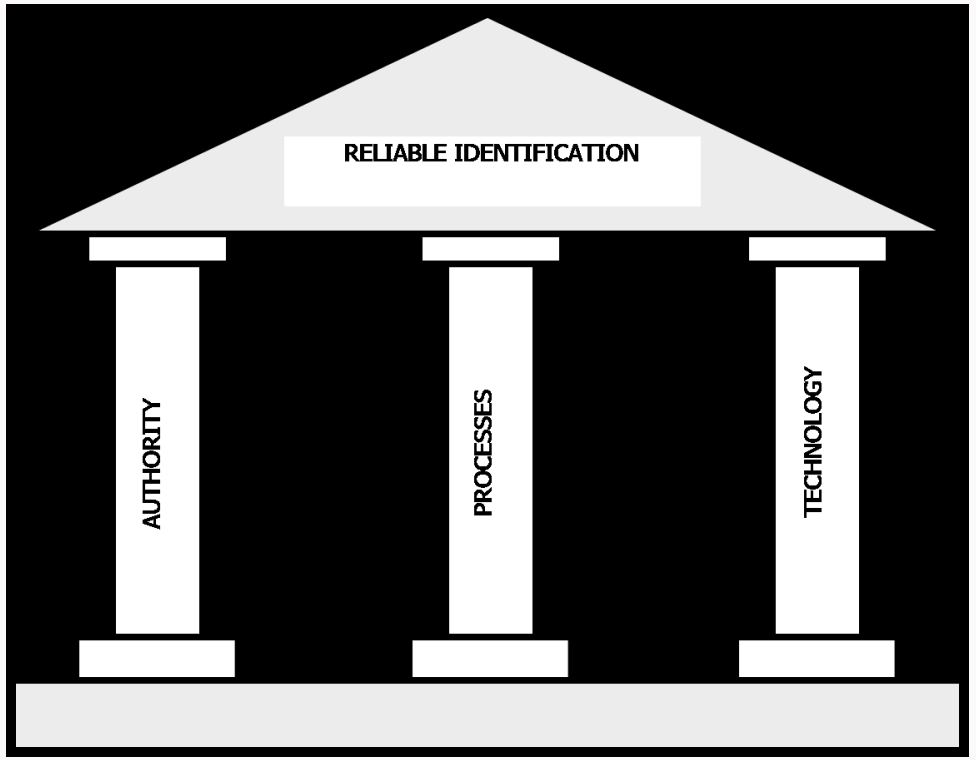


  - Mobile ID

- Backed by a Secure Database for Demographic and Biometric Data, with a stakehold gateway

- Preferably Complemented by PKI Certificates and Digital Signatures

PILLARS FOR RELIABLE IDENTIFICATION



- Reliability through Recognized Identification Authority and Legal Framework
- Reliability through Processes and Procedures
- Reliability through Technology

PILLAR 1: AUTHORITY

- Recognized Identification Authority and Legal Framework to:
  - Make it Mandatory to register, an offence not to register
  - Enforce the Proper Usage
  - Enforce consequence for mis-use
  - Punish impersonators and those who seek multiple identification
  - Punish severely those who knowingly furnishing false information
  - Punish Authority employees responsible for fraudulently issuing Identifications

Pillar 2: Processes

- Proper business processes by the authorities and other stakeholder in proving and issuing identifications

1. Fill application form and Sign
2. Applicant submits documents
3. Preliminary interview
4. Authority verifies Applicant info with 3rd party stakeholders

Form Filling, Assessment and Verifications

Proceed for Data Enrolment

1. Application form reviewed
2. Applicant interviewed
3. Officer captures Biographic & Biometric

Enrolment

Proceed for Data Scanning

1. Officer scans the application Forms
2. Officer saves application form

Document Scanning

Optional Data Completion

1. Officer Completes Data entry
2. Officer Saves Application

Data Completion: Branch or Central

Branch Approval

1. Validates scanned application
2. Approves/ Disapproves Application
3. System forwards applications to central

Registration Office Approval

ABIS Adjuducation

ABIS Results

1. Matching and Duplicate check
2. Approve /Reject Application
3. Adjudication processes

Validation

1. Validates application Details
2. Approve/ Reject application

Validation results

Investigation

1. Validates application Details
2. Approve/ Reject application

Proceed to final Approval

Final Approval

1. Validates application Details
2. Final Approve / Reject application

Mobile ID

ID Cards

123683-56875

+

(Number and Biometrics)

PILLAR 3: TECHNOLOGY

- Proven Technology that prevents counterfeits

- Relevant Technologies include:
  - Biometrics
    - Finger Prints, Facial
  - PKI and Key Managemengt Sytems
  - Smart Card with Security Chips and Surface Security Features
  - PKI backed Mobile Applications
  - Secure Database
  - Secure Connectivity

Smart Card ID Composition

Chip

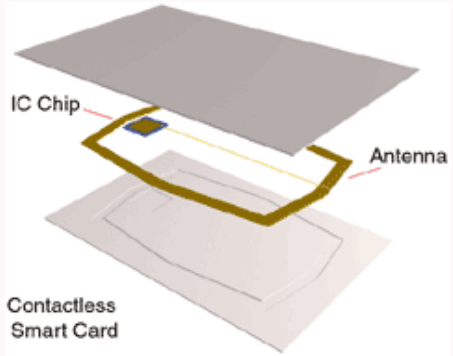
Overlay

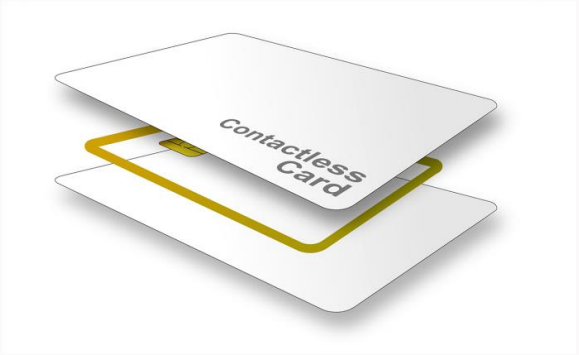
Core

Inlay

Core

Overlay





SoftNet
Creativity at Work

Smart Card ID Security Levels

To ensure the forgery proofing of ID documents advanced printing technologies are used and integrates other security features to the documents.

Security printing classified into three categories:

- **Level 1: Detectable by human eyesight**
- **Level 2: Using simple equipment e.g. magnifying glass, UV**
- **Level 3: Using Electronic Equipment (readers), Forensics etc**

Rainbow Color Print

Coloured fibres

Fluorescent over-print

UV laminate

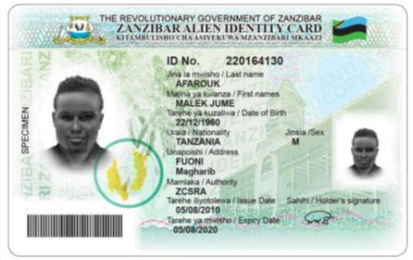
Fluorescent fibres

Color Change Ink

DIGITAL IDENTIFICATION ACHIEVEMEYS IN TANZANIA

- A lot has been achieved in Identity Digitization in Tanzania

- Revolutionary Government of Zanzibar and the Government of the United Republic of Tanzania ALREADY have gone Digital, using Smart Card e-ID
  - => Tanzania National ID is a Smart Card e-ID
  - => ZanID is a Smart Card e-ID
  - => Residence Permit is Smart Card e-ID
  - => Tanzania Passport is e-Passport
  - => Tanzania Visa System and Border Control System is electronic



- NID, ZanID and Immigration Systems have Stakeholder Gateway for Online Verification

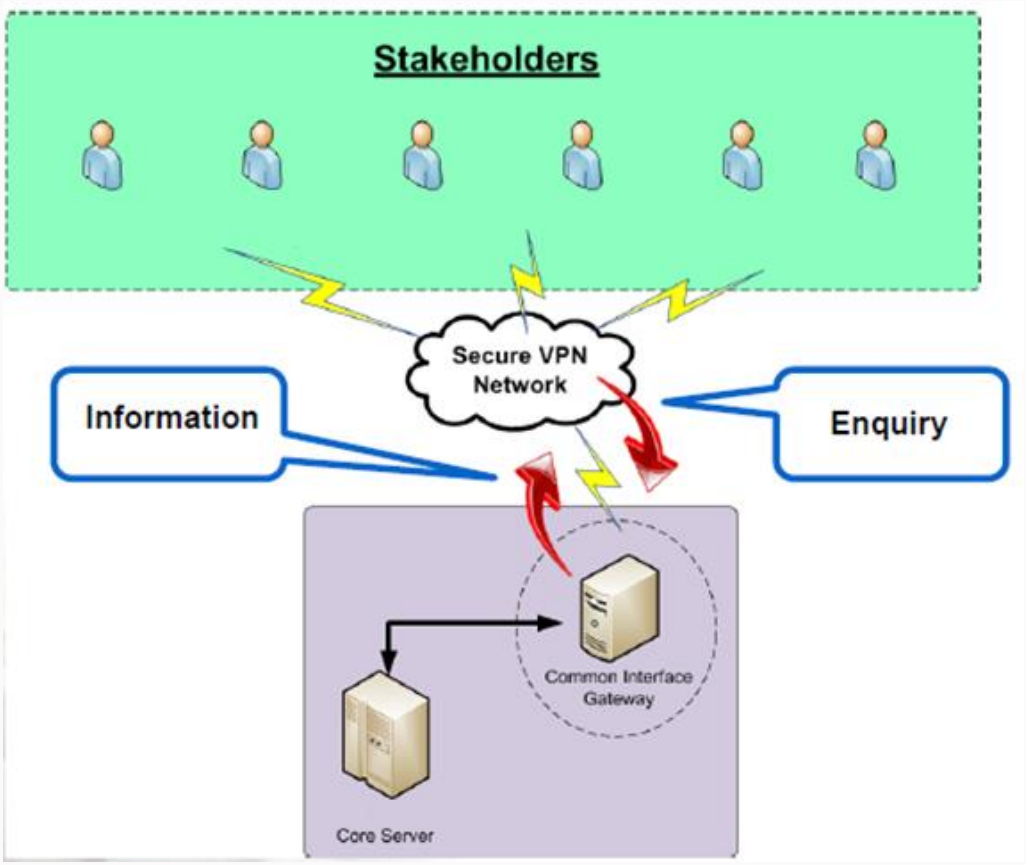
- Missing: Common/National PKI System to help with online

Means of Usage of Identification Data

Desktop Software uses Card Reader to Read and Verify data

Software in Mobile Reader is used to Read and Verify data

Offline Usage



Stakeholders Query and Verify applicant's data Online in Real-time from the Database, securely

Online

SoftNet
Creativity at Work

Sample Usage of Digital IDs in Tanzania

- eKYC Mobile Phone Registration
  - NIN + Biometrics
- eKYC in Banks and Other Financial Institutions
- Company Incorporation with BRELA/ZBPRA
- Coming Soon=> Linking TIN numbers with National ID numbers
- ..... A lot more can be done to improve Digital Services in Tanzania
- ..... Need innovative applications to make use ID data in solving common problems

Conclusion and Recommendations

- Tanzania is already doing very well in Digital Identifications
- A lot more can be done to improve Digital Services in Tanzania
- It’s time for more innovative applications to make use of ID data in improving service delivery and solving Identification related problems