



Background and Status of the Tanzania National ID System

Coverage

- **INTRODUCTION**
- **IMPLEMENTATION STATUS**
- **KEY TECHNOLOGIES**
- **CHALLENGES**
- **WAY FORWARD**

INTRODUCTION

Introduction- Tanzania at Glance.

- **Total Area:** 947,300 sq km.
- **Population:** 49.2 Million (2012 census)
- **Administratively divisions:** Regions, Districts and Wards
- **Bordering countries(8):** Kenya, Mozambique, Burundi, Malawi, Democratic Republic of Congo, Uganda and Zambia.
- **Main Languages:** Kiswahili and English

Map of Tanzania



Why National ID?

- The concept of national identification in Tanzania aims to answer the following four major fundamental questions:-
 - “Who is who?” -Registration of persons and creation of a family tree
 - “Where does a person live?”- Residential Address including District and Ward
 - “How does a person earn a living?”- *Registration of occupation and major economic activities*

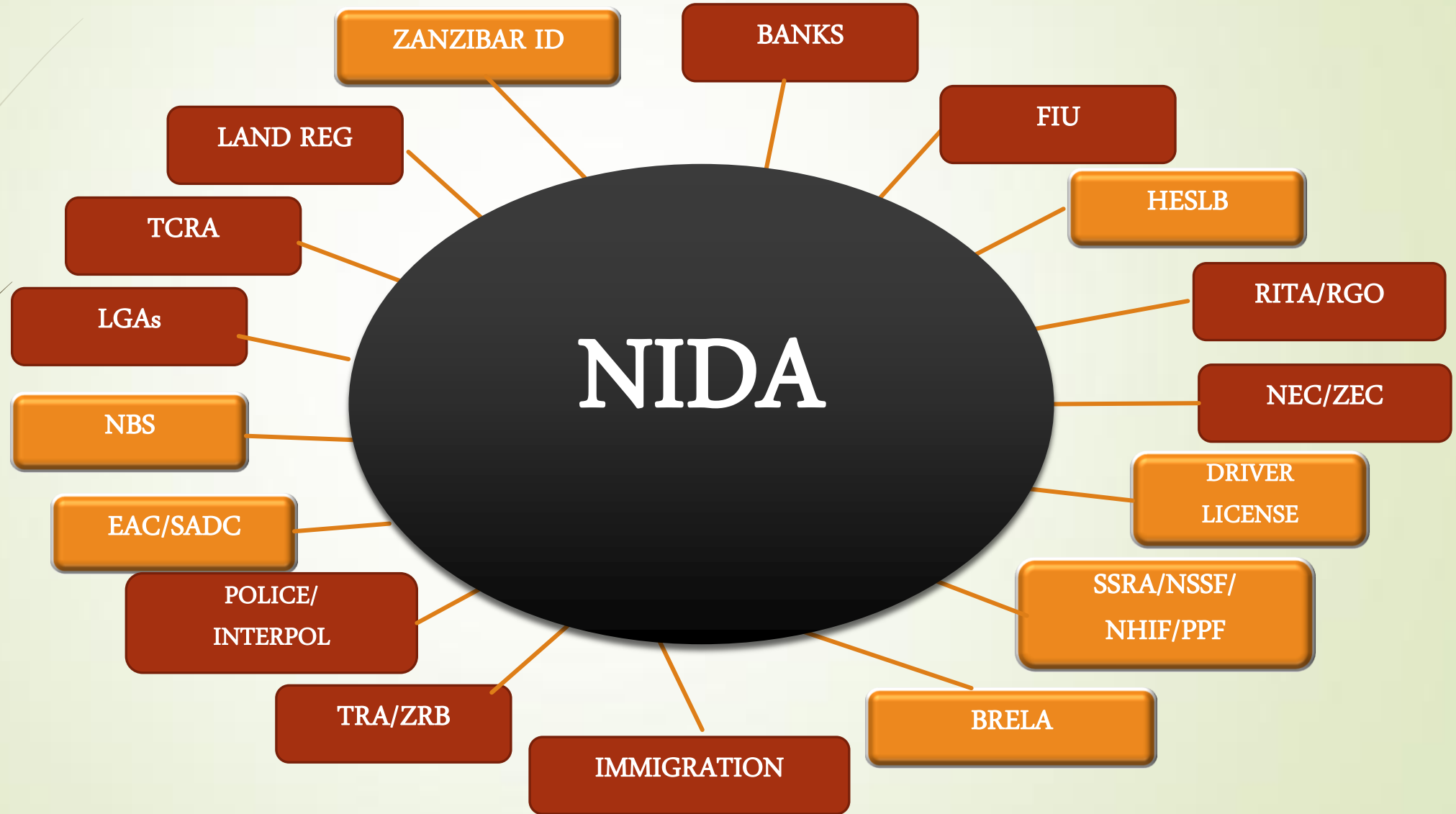
National ID Project Background

- NIDA was established in 2008 with the key mandate to:-
 - Register all **Citizens, Legal residents and Refugees** over the age of **18 years**
 - Mandate: **Register, Issue** National IDs cards and **Manage** national ID program
 - Establish a secure **biographical and a biometric databases** of all registered persons in Tanzania (18 years and above)
 - Facilitate sharing of biographical and biometric data with other “**authorized**” Government Institutions and selected private organizations to improve public service delivery

National ID Key Stakeholders

- The key stakeholders have a crucial role of fulfilling the prerequisites for the enrollment and registration into the National ID database.
 - **RITA** for proof of age (must be 18 years or older)
 - **IMMIGRATION** for proof of Citizenship or other status
 - **LGA** for proof of existence (Residential Postal Code address)

National ID Linkages



NATIONAL ID IMPLEMENTATION STATUS

Major Component of National ID System

➤ Key subsystems:-

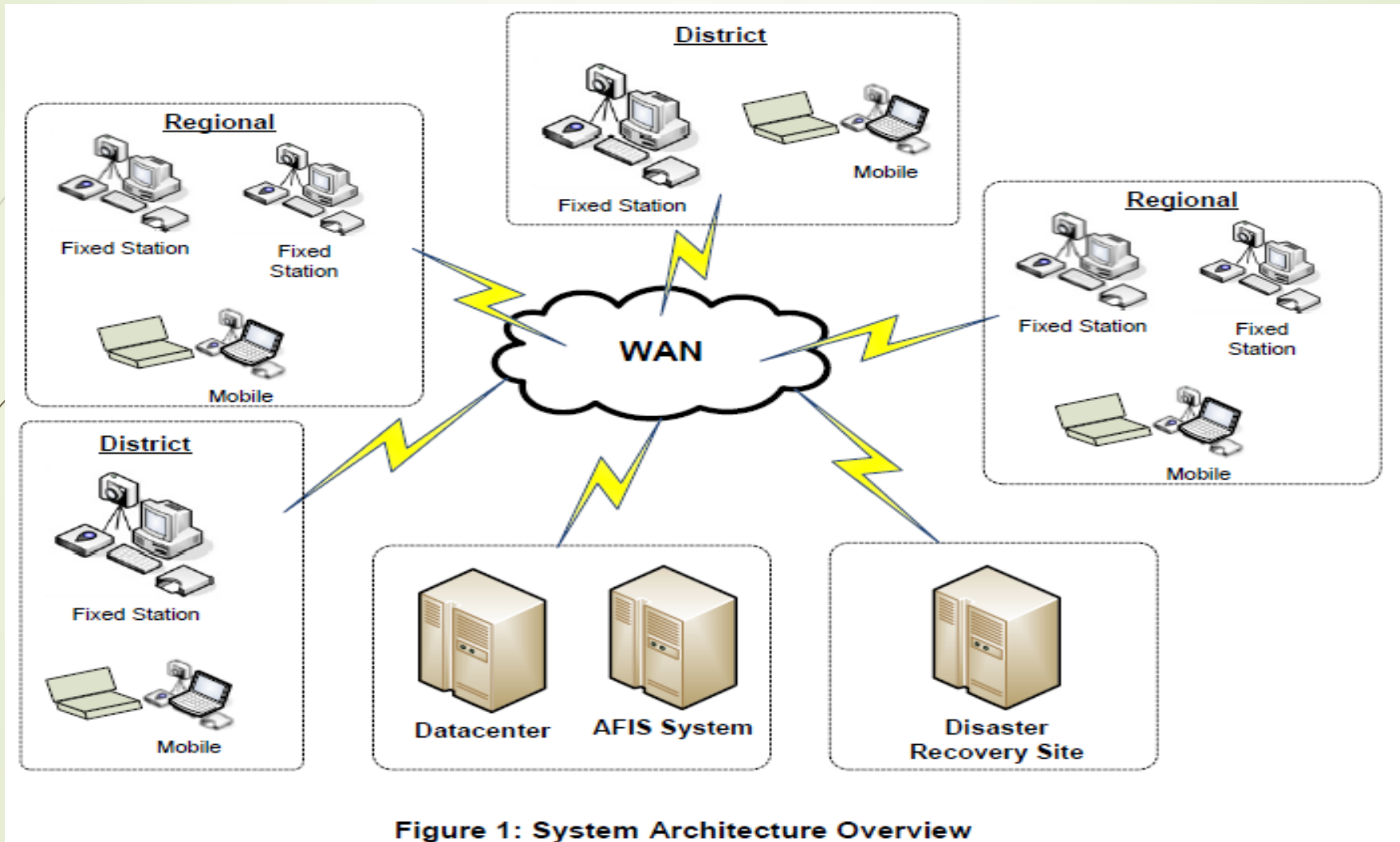
- **Smartcard ID** with photo and fingerprint biometrics
- Central National Identification **Registry** (NIR) or Database
- Automatic Fingerprint Identification System (AFIS)
- National ID **Datacenter** (NIDC)
- **Disaster Recovery Site** (DRS)
- **District Registration Offices** nationwide
- Secure Nationwide **Virtual Private Network** (VPN) to connect remote sites

Implementation Status to date

- Established:
 - **Data Entry Facility** to deal with the processing and registration of new applicants
 - **Datacenter** where all most all National ID applications are being hosted
 - **Disaster Recovery Site** to ensure business continuity in the event of a major catastrophe – natural or man-made
 - **District/Regional Registration** Offices in selected major population centers
- Registered and issued more than **2M** national ID cards and counting

....Major System Components

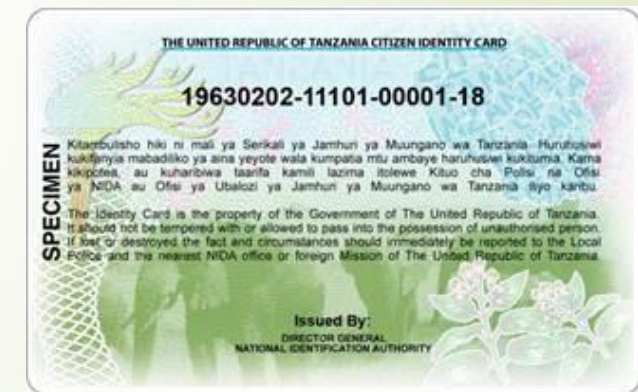
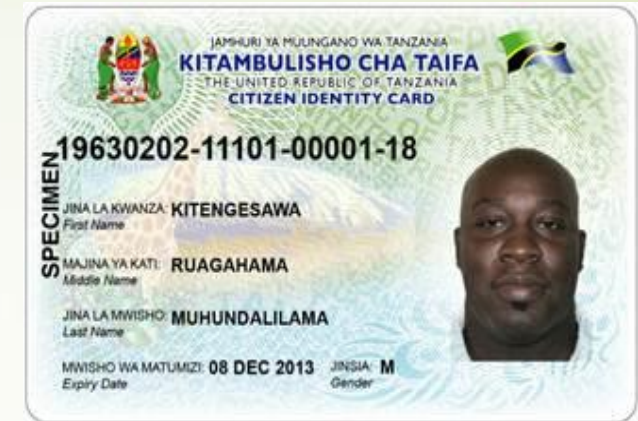
13



KEY TECHNOLOGIES

Smartcard Feature

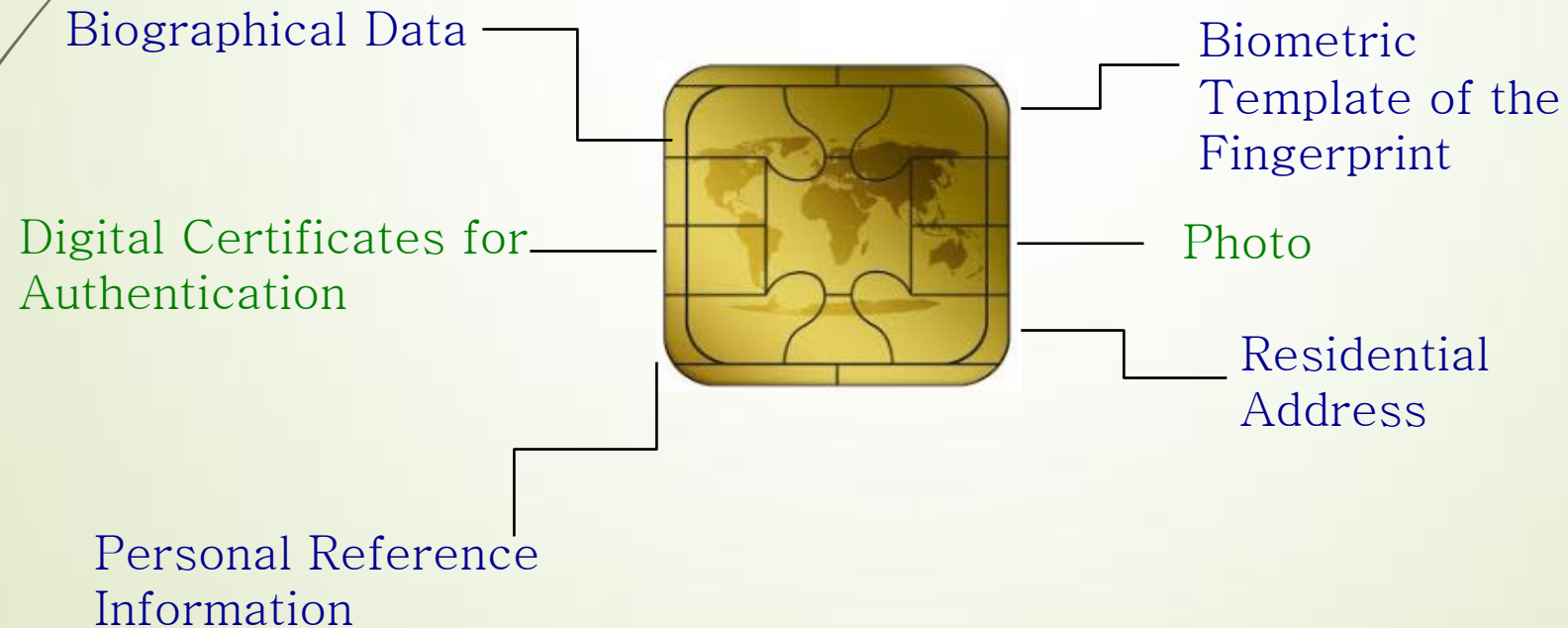
- **Advanced security** features:
 - Hologram; UV ink; Microtext
- **Polycarbonate** material:
 - Higher resistance to damage from heat and UV drastically reducing card replacement costs
- **Multi-application** smartcards ideally suited for diverse uses:
 - health insurance card; voter card



➤ Citizen Identity Card

Smart Card Microchip

- ▶ **Smartcard with a micro-chip** It has the capability to securely store selected data on the microchip



Unimodal Authentication System

- NIDA Biometric authentication is unimodal
 - “single mode” of authentication
- Based on fingerprint biometric authentication supported by smartcard ID technology
- Two modes of authentication are supported:
 1. **Offline authentication** compares a live fingerprint scan against sample stored in the smartcard microchip
 2. **Online authentication** compares a live fingerprint scan against the a sample stored in a secure central database

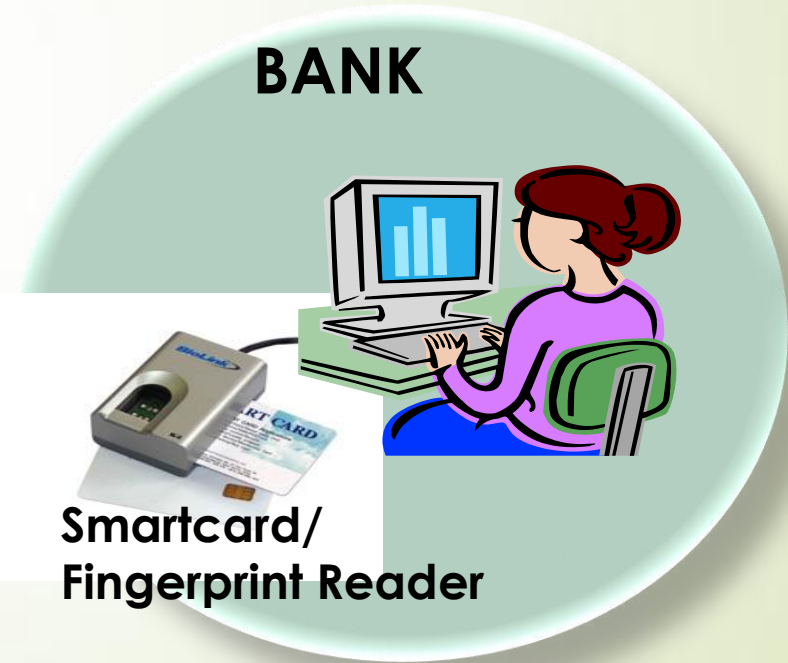
Online/Offline Authentication



**NIDA Datacenter
AFIS System**



INTERNET



BANK

**Smartcard/
Fingerprint Reader**

TECHNOLOGY CHALLENGES

Unimodal Biometric Authentication System Vulnerabilities

- Unimodal authentication schemes have vulnerabilities that include susceptibility to spoof attacks
 - eg: Use of artificial fingers made of materials such as silicone and gelatin



The Future is Multi-modal or Multi-factor Biometric Authentication

- ▶ Multimodal/Multifactor authentication overcomes limitations and vulnerabilities of unimodal
 - ▶ Consolidates biometrics from multiple sources
 - ▶ Incorporates anti-spoofing and aliveness detection

Potential Biometric Sources for Multimodal Authentication

- Fingerprint Scan
- Face Recognition
- Voice Recognition
- Iris Scan
- Retina Scan
- Hand Geometry
- DNA (Ultimate)



Hand geometry reader



Fingerprint sensor

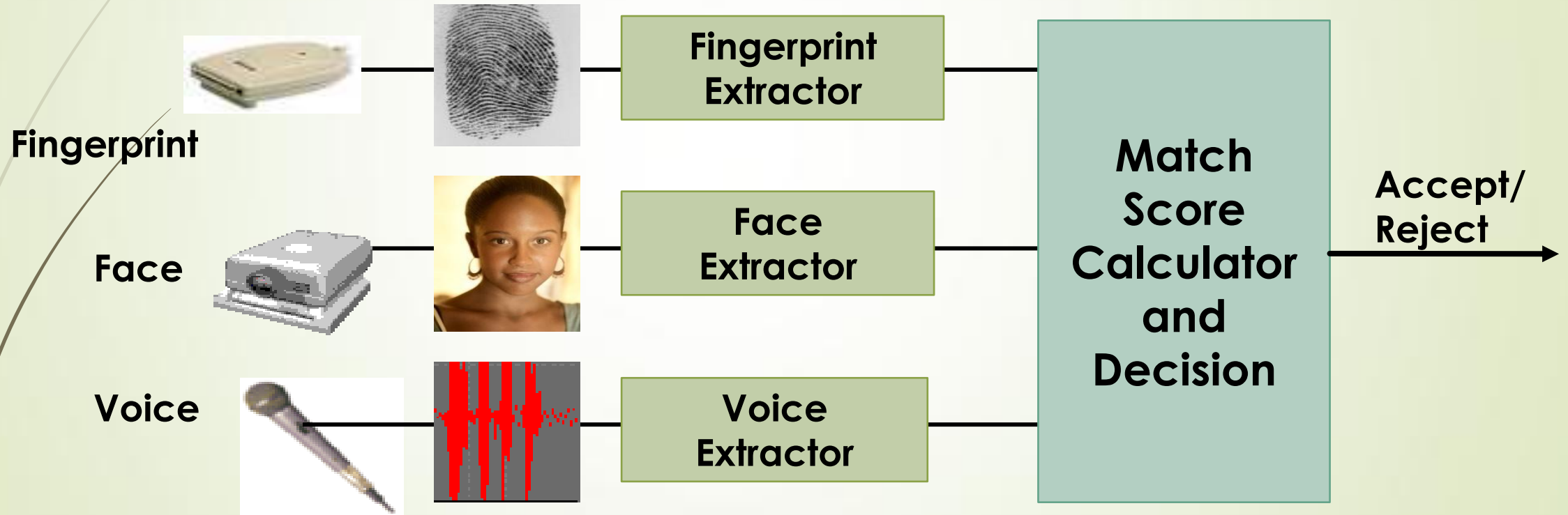


Iris recognition



Face recognition

Example of a Multi-modal/factor Biometric Authentication System



Way Forward – “Applications”

- Targeting to register all 25 million eligible persons the 2016 timeframe
- Commitment to link National ID System with Government Major Systems eg Payroll, Land Registration, e-Government, Police, Immigration, etc
- Currently working with major Banks and Financial institution to facilitate adoption of National ID for Banking and e-Commerce
- Commitment to link National ID with emerging e-Health initiative and National Health Insurance system

Way Forward – “Technology Roadmap”

- Short-term NIDA will deploy only Fingerprint Authentication
- Intermediate/Long-term NIDA is looking to introduce a Multi-modal Authentication System incorporating Fingerprint recognition plus other biometrics, eg
 - Face recognition with lip movement
 - Hand Geometry Scanning
 - Retina Scanning

Thank you!