



**ID4AFRICA2026**  
ABIDJAN | CÔTE D'IVOIRE | MAY 12-15



# **The Kenya Digital Identity Playbook: Identity as Foundation of Digital Public Infrastructure**

# CONTENT



**1. WHY DIGITAL IDENTITY MATTERS**

**2. KENYA'S NATIONAL PROBLEM STATEMENT**

**3. ECOSYSTEM MATURITY**

**4. DIGITAL IDENTITY ARCHITECTURE**

**5. DEMAND SIDE: WHO USES IDENTITY AND WHY**

**6. SUPPLY SIDE: ISSUANCE, VERIFICATION & LIFECYCLE MANAGEMENT**

**7. INTEROPERABILITY & DIGITAL INFRASTRUCTURE**

**8. GOVERNANCE & COORDINATION**

**9. SUSTAINABILITY MODEL & LESSONS FOR AFRICA**

**10. KENYA'S VISION FOR TRUSTED DIGITAL IDENTITY**



# BACKGROUND



# WHY DIGITAL IDENTITY MATTERS



Digital identity is the foundational trust layer enabling Kenya's Digital Public Infrastructure ecosystem.

## Kenya's digital identity investments support:

1



Secure and trusted digital government services

4



Fraud reduction and identity assurance

2



Financial and economic inclusion

5



Seamless citizen access to public and private services

3



Efficient service delivery

6

National digital transformation under the Bottom-Up Economic transformation Agenda (BETA)

Identity is no longer only an administrative function; it is national digital infrastructure

## BEGINNING

- ❖ Identity dates back to 1919.
- ❖ National Registration Bureau was established in 1978 vide the Registration of Persons Act, Cap. 107, Laws of Kenya.-
- ❖ The Act provides for mandatory identification, registration, and issuance of identity cards to all persons who are citizens of Kenya and who have attained the age of eighteen years or over.

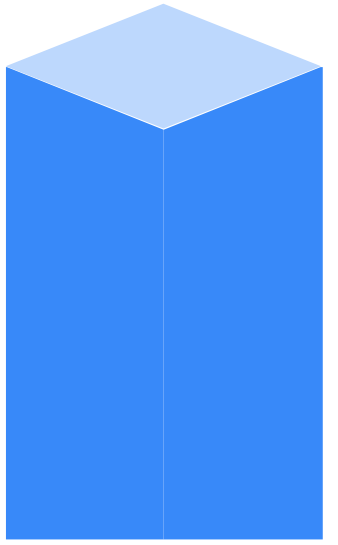
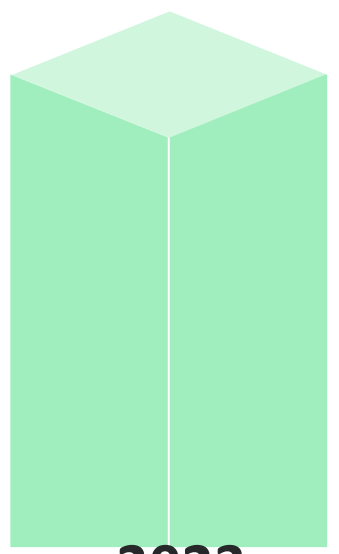
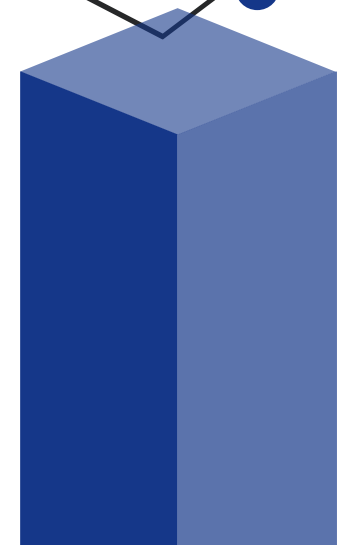
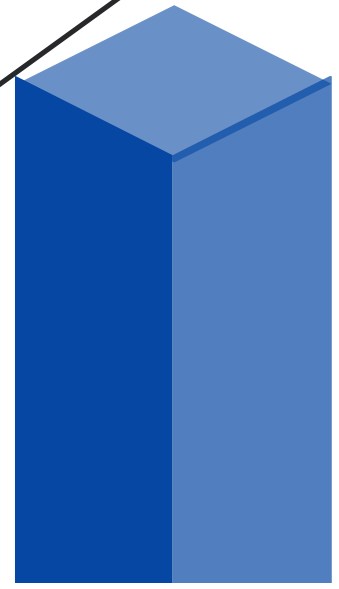
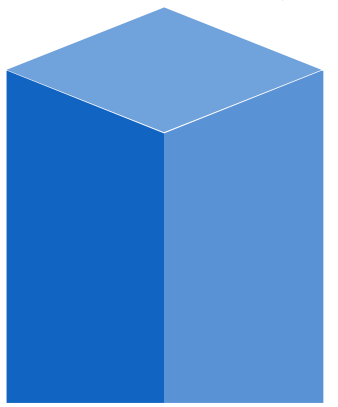
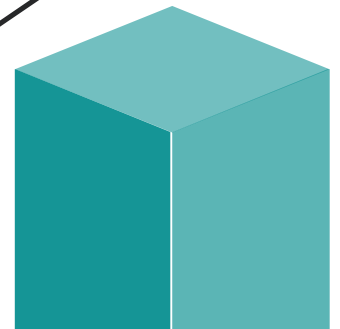
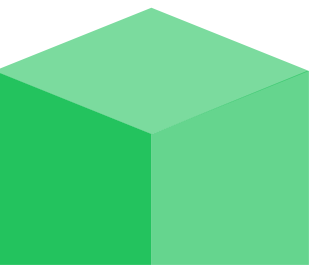
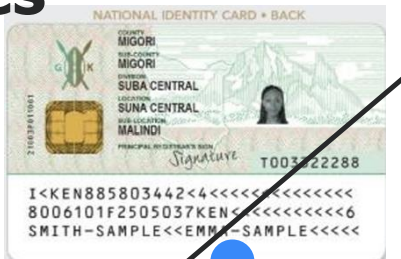
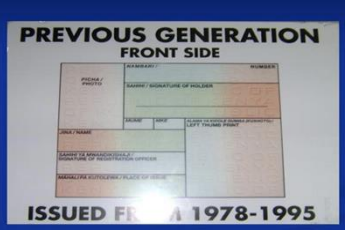
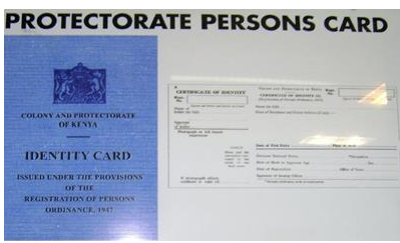
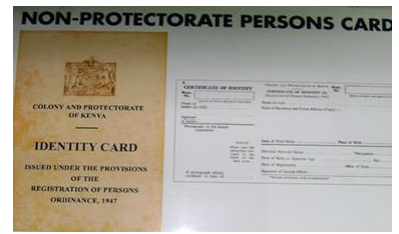
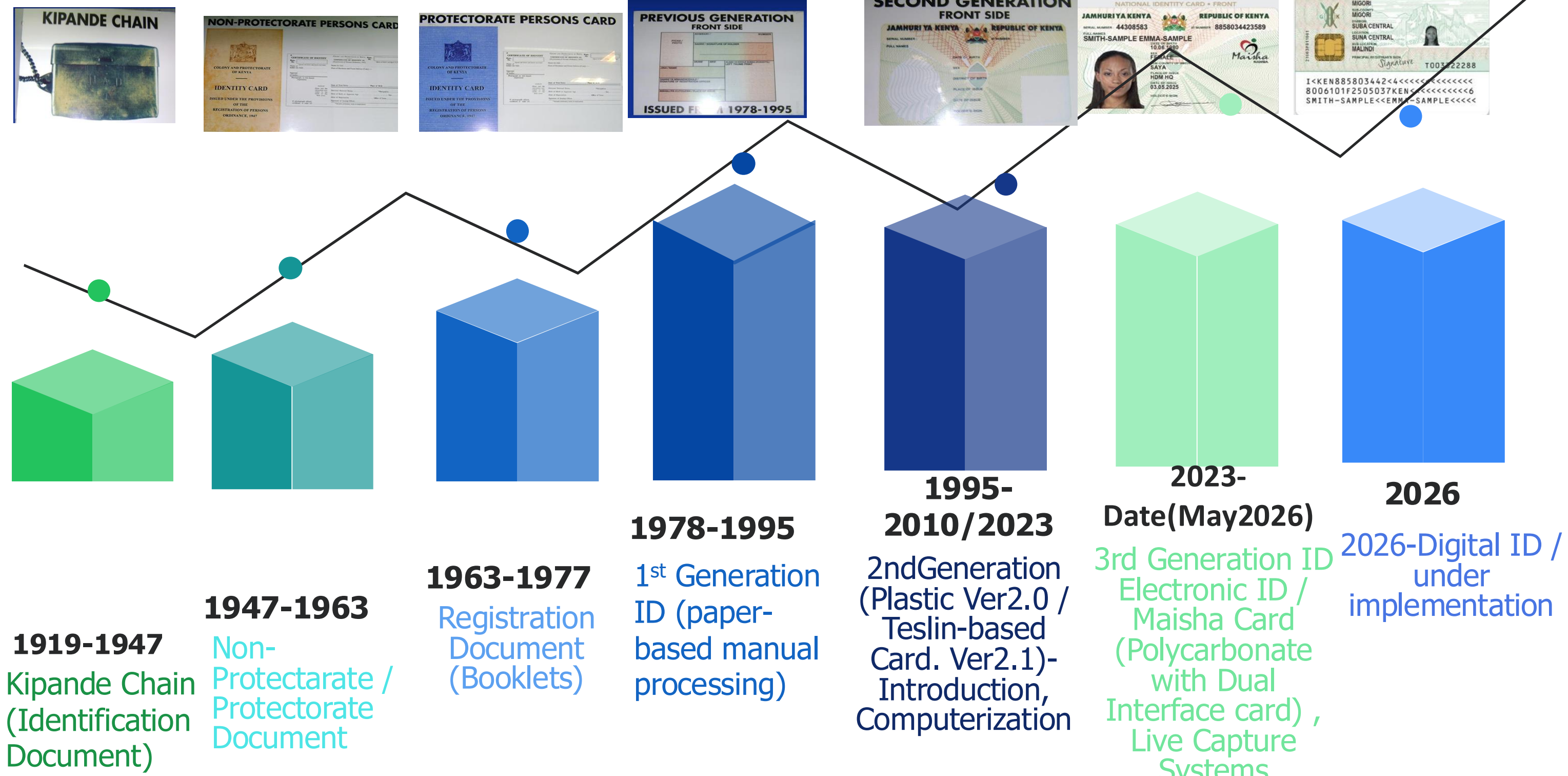
## THE MANDATE

- ❖ Identification and Registration of Kenyan Citizens Aged 18 Years and Above.
- ❖ Production and Issuance of Secure Identification Documents.
- ❖ Management of a Comprehensive Database of all Registered Persons.
- ❖ Detection and Prevention of Illegal registration

# IDENTITY EVOLUTION FROM 1919 TO DATE



## Various Identity Documents Issued / Different Registration Regimes



**1919-1947**  
Kipande Chain (Identification Document)

**1947-1963**  
Non-Protectorate / Protectorate Document

**1963-1977**  
Registration Document (Booklets)

**1978-1995**  
1<sup>st</sup> Generation ID (paper-based manual processing)

**1995-2010/2023**  
2nd Generation (Plastic Ver2.0 / Teslin-based Card. Ver2.1)- Introduction, Computerization

**2023-**  
3rd Generation ID Electronic ID / Maisha Card (Polycarbonate with Dual Interface card), Live Capture Systems

**2026**  
2026-Digital ID / under implementation

# KENYA'S NATIONAL PROBLEM STATEMENT



**Before digital identity modernization, Kenya faced several critical challenges:**

**01**

Fragmented identity and civil registration systems

**02**

Manual and paper-based verification processes

**03**

Legal complexity

**04**

Identity fraud and ghost beneficiaries

**05**

Data accuracy across platforms

**06**

The existence of siloed systems

**07**

Resource leakages and high operational costs

**08**

Weak citizen authentication for digital services

**Digital identity addresses these challenges by creating:**

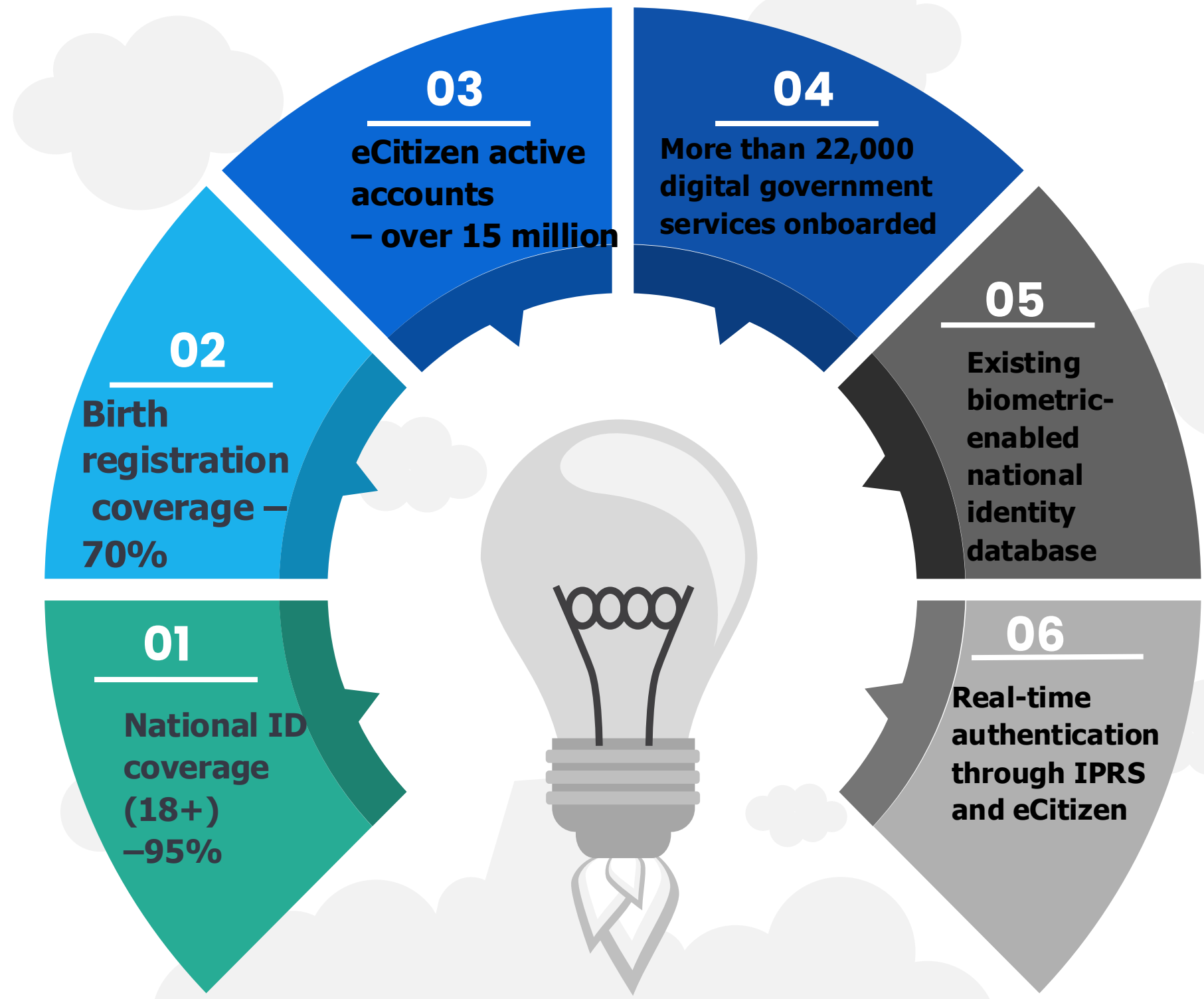
A trusted national identity ecosystem

A unified digital trust framework

Secure digital identification and authentication

- Improved efficiency and accountability
- over 22,000 services are online relying on Digital ID for access

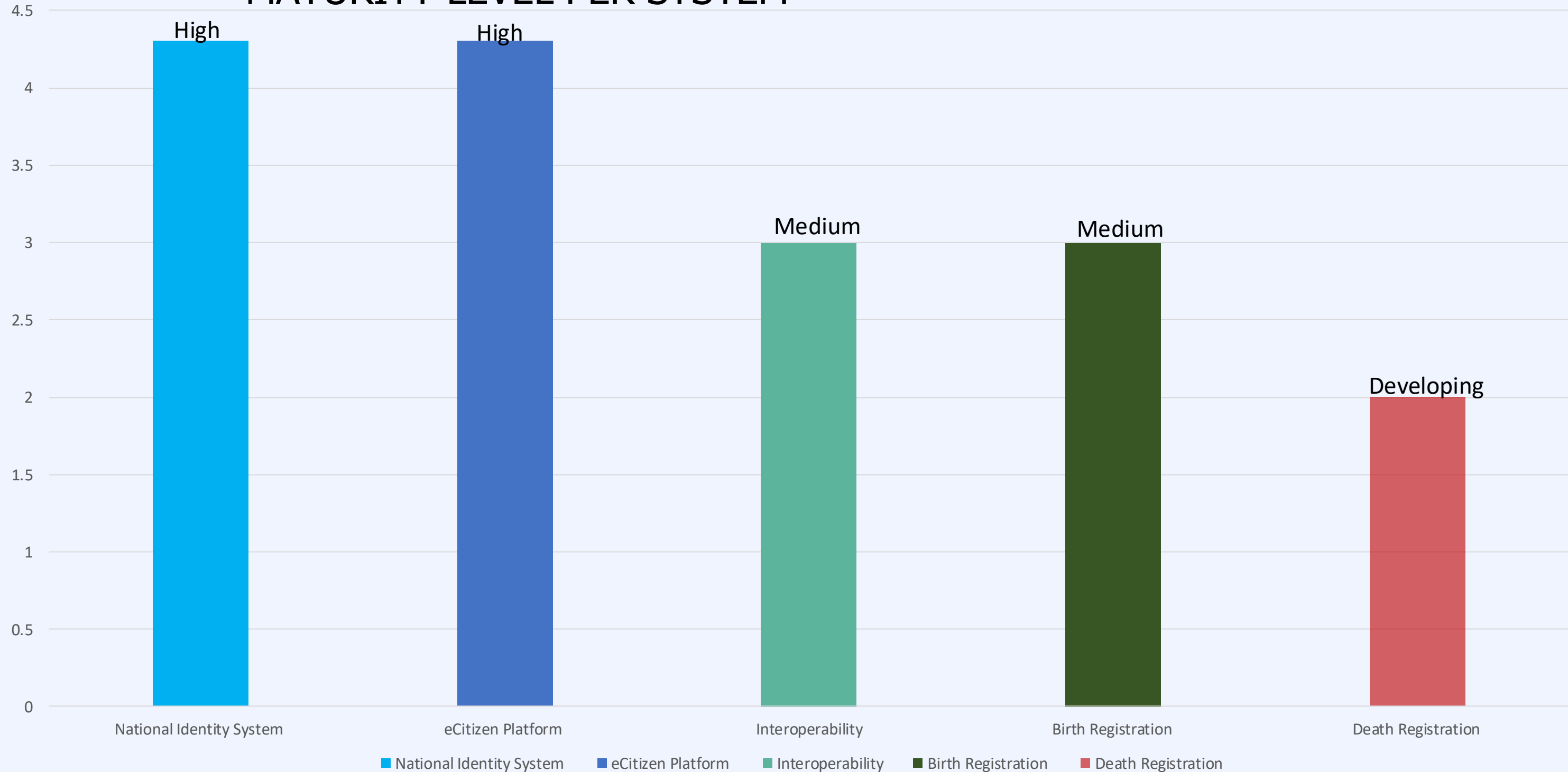
# CURRENT ECOSYSTEM STATUS



# MATURITY ASSESSMENT



## MATURITY LEVEL PER SYSTEM





## KEY OBSERVATION

Kenya already possesses foundational infrastructure upon which advanced Digital Public Infrastructure can scale sustainably.

# DIGITAL IDENTITY ECOSYSTEM ARCHITECTURE



1

## Unique Personal Identifier

- ✓ Implemented and in use by CRS and NRB (integration done.)
- 9-Digit Random Number, generated using a selected data field and hashing.

2

## Electronic Id Card– Maisha Card / 3rd Generation ID Cards- Already in pl

- Smart Electronic ID Card
- Dual interface card (both contact and contactless)
- Storage of civil data/ biographic data and two best fingerprints in the chip.
- International Civil Aviation Organization (ICAO)-compliant travel documents
- 10yearexpiry period with enhanced security features
- Over6million Electronic ID cards have been produced since October 2023 3.

3

## Digital ID Underway

- Digital Identity Management System- core system for management of digital identities
- Identity and Access Management System (IAM)- manage access to digital platforms.
- E-KYC Platform- Verification of Identities
- Digital Signing- secure signing of documents in the public / private sector.
- Infrastructure and connectivity- the supporting infrastructure, including storage, disaster recovery, computing engines, etc.

4

## Master Integrated Database/Integrated Population Registration System

- It consists of a subset of data from foundational databases/ systems, i.e. Civil Registration Services (births and deaths), National Registration Bureau (National ID), Immigration (passports) as well as foreign nationals and refugees data.
- Provides verification for the E-KYC platforms for public and private sector transactions

## How the System Is Structured



**A**

### HYBRID

hybrid architecture model combining **centralized trust** services with **federated** sector implementation



**B**

### FOUNDATIONAL COMPONENTS

- Unique Personal Identifier (UPI) (Maisha Namba)
- E-ID (electronic ID)
- Digital ID (maisha digital)
- National population data management (NPDM)



**C**

### ROLES

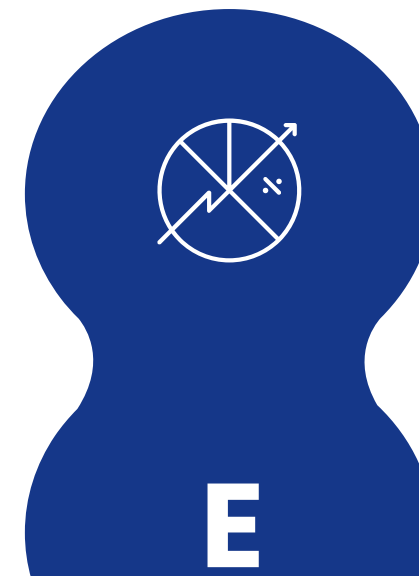
Based on the mandate of each entity in the ecosystem



**D**

### Scale, Resilience, And Evolution

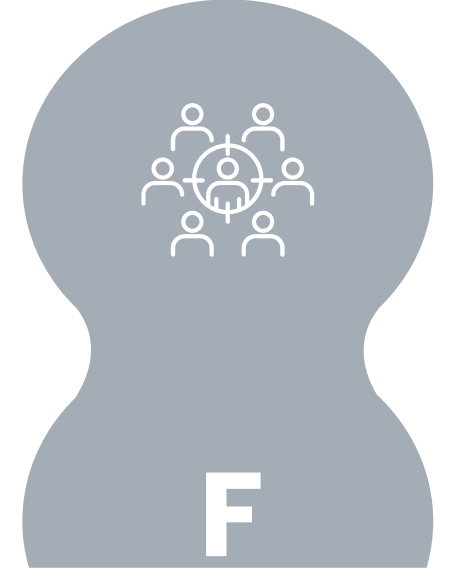
The systems are dynamic and flexible to grow, scale up, and future evolutions..



**E**

### Constraints

New infrastructure setup, technology upgrades, and process reengineering



**F**

### Why this Architecture

- To encourage maturity of systems
- Re-use of Existing databases and systems
- Need for business process reengineering

# CREDENTIALS ARE ISSUED?



## Current documents Issued

## Under reform trajectory:

**A** Physical electronic National ID (biometric , ICAO compliant)

**Digital ID credentials (mobile-accessible)**

**B** Passport (ICAO compliant)

**Biometric-backed digital authentication tokens**

**C** Alien ID

**Derived credentials for specific sector use (finance, health, education)**

**D** Birth Certificate

**Potential wallet-based identity access**

**E** Voter ID (linked to national ID)

**Real time Authentication, digital signature and digital documents  
Access services anywhere anytime**

From static physical ID → to dynamic, portable digital credentials.

## Strategic Design Principles <sup>05</sup>

- Scalability
- Modularity
- Interoperability
- Security-by-design
- Future-readiness

## Service Delivery Ecosystem

- eCitizen
- Banking & e-KYC
- Health systems
- Education systems
- Tax systems
- Social protection

## Trust & Verification Layer

- Biometric verification
- Authentication APIs
- Identity validation services

## Identity Layer

- Maisha Namba (UPI)
- Electronic National ID
- Digital Identity Credentials

## Foundational Registries

- Birth Registration
- Civil Registration
- National Population Database



01



02



03



04



05

# SUPPLY AND DEMAND



## Demand Side: Who Uses Identity and Why

### Primary Users

- Government ministries and agencies
- Financial institutions
- Telecommunications providers
- Health and education sectors
- Social protection programs
- Citizens and businesses

### Problems Solved:

- Identity fraud reduction
- Faster onboarding and authentication
- Improved data quality
- Remote access to services
- Reduced operational costs
- Secure digital transactions

### Why Stakeholders Support

- Improved service delivery
- Economic growth
- Expanded customer reach
- Increased public trust
- Better regulatory compliance

## Supply Side: Issuance, Verification & Lifecycle Management

### Identity Lifecycle:

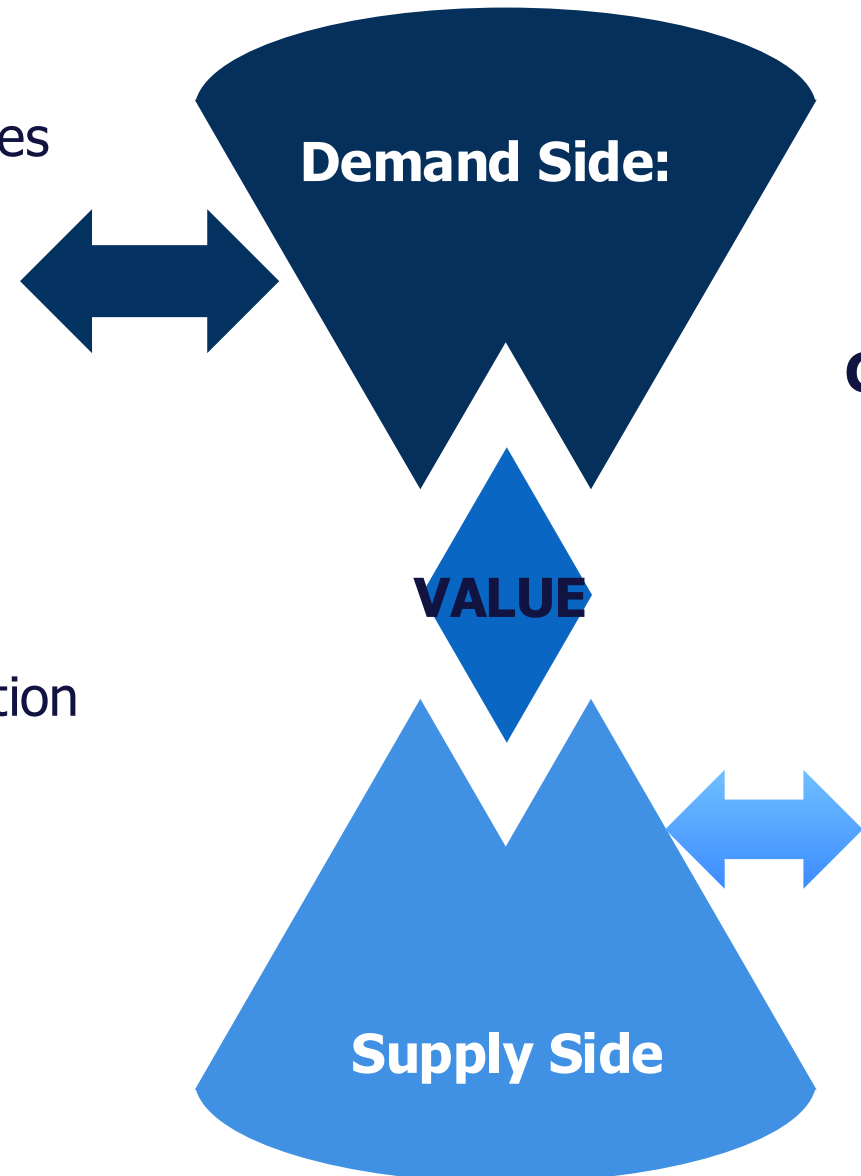
- Birth Registration → UPI Issuance → National ID → Digital Credentials → Service Access

### Core Infrastructure

- Biometric enrollment systems
- AFIS deduplication infrastructure
- Authentication APIs
- SIM registration integration
- Mobile-enabled verification systems

### Identity Lifecycle Management

- Birth registration
- Unique Personal Identifier issuance
- National ID enrollment
- Digital credential issuance
- Authentication and verification
- Status updates and synchronization
- Revocation and reissuance
- Death registration integration

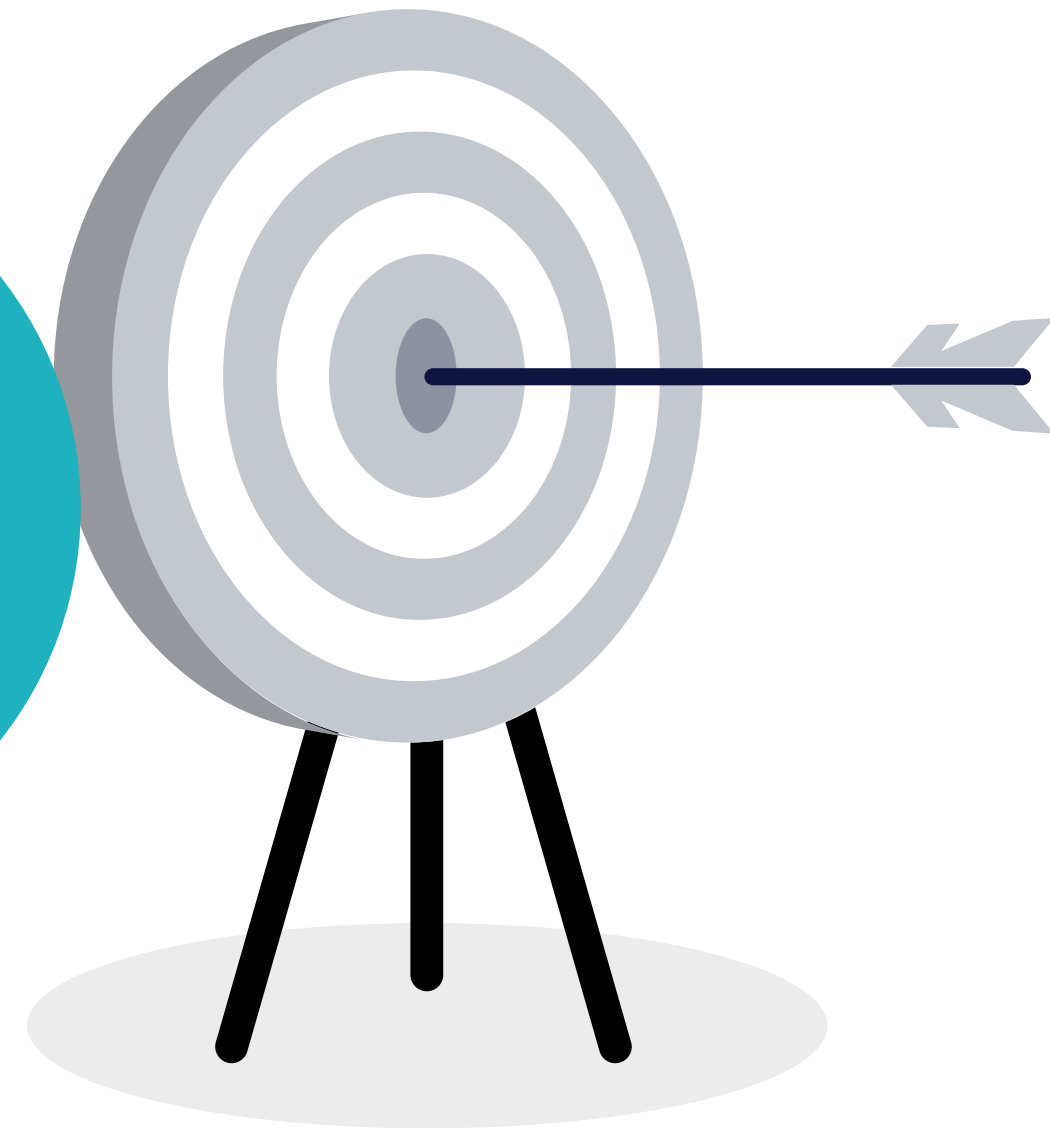


***Identity is not a static credential; it is a continuously managed trust relationship.***

## INTEROPERABILITY & DIGITAL PUBLIC INFRASTRUCTURE



Identity functions as Kenya's common trust layer across government and private sector ecosystems.



## 1. Reduces Duplication & cost

- one credential, many services

## 2. Enables cross border use

- travel, trade, refugee access

## 3. Promotes financial inclusion

- unbanked can open accounts with verified ID

## 4. Strengthens data protection

- data stays in one place; only attributes are shared

**Interoperability turns a static ID into a dynamic, reusable credential.**



**DPI = shared, publicly governed digital platforms that enable core economic functions**

Single source of truth, reduces fraud

**For identity, DPI includes**

2

**Foundational ID system (Maisha Namba)**



**Authentication & consent layer (eKYC, biometric verification)**

3

Real-time verification without exposing raw data

Citizen controls who sees what, for how long

4

**Interoperability gateway (APIs & standards)**



**Data protection & audit layer**

5

Use same ID across sectors (health, tax, voting)

# WHO GOVERNS ACCESS?

- Data sharing controlled to safeguard personal data and prevent unauthorized access.
- Information through IPRS is on a view-only basis. **Secure communication channels** protects data in transit.

Central ID authority

Ministry of ICT

**Access is:  
Controlled,  
audited,  
and legally  
anchored.**

Data Protection Commissioner

Sector regulators  
(CBK, CAK, etc.)

# INTEROPERABILITY ENABLERS



## INTEROPERABILITY ARCHITECTURE

  
**Interoperability standards**


**Enterprise Service Bus (GIF)** with  
Tokenized verification requests

  
**Secure APIs & data formats**

  
**Data governance frameworks**

**GEA**  
**Mutual recognition & legal frameworks**  
➤ Data Protection Act (2019)  
➤ Central ID authority governance

  
**Data minimization protocols**

  
**Consent and audit mechanisms**

**Upholds the Once-only principle – Citizens provide information once and government systems should securely reuse it responsibly across government systems.**

## Connected Systems

E-Citizen  
E-Government  
platform



CIVIL REGISTRATON  
IPRS



KRA-TAX



SHA/SHIF



Financial  
Sector e-KYC



Immigration  
systems



Education  
systems



SIM  
registration



Social protection  
systems



01



## DPI provides the infrastructure

- Unique ID,
- authentication,
- consent,
- single source of truth.

02






## Interoperability enables scaling

- Turns truth into a universally accepted, reusable credential
- Same ID works for healthcare, banking, trade, voting.

03

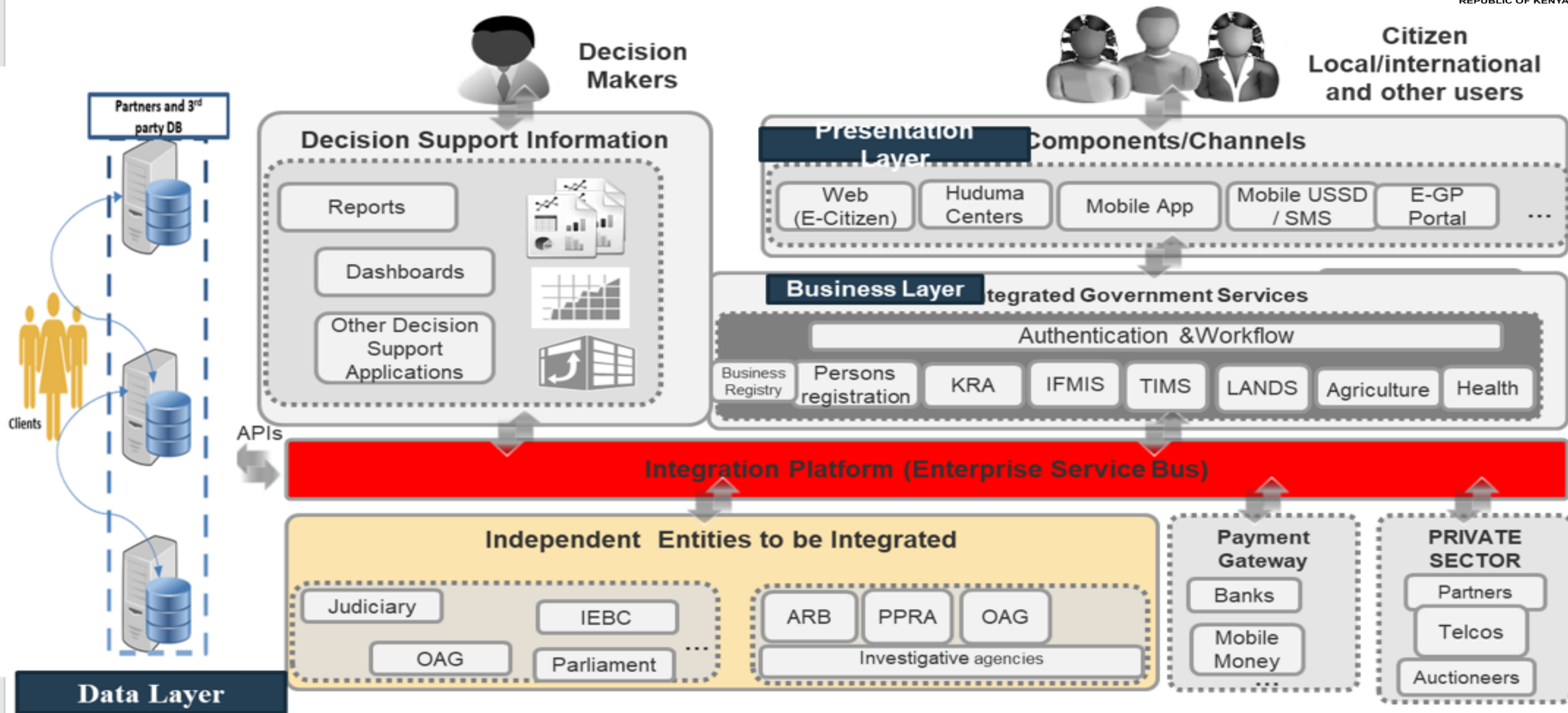


## Result

-  Trusted credentials – accepted anywhere, anytime, without repeated KYC.
-  Secure Digital Public Infrastructure
-  Inclusive digital economies (national & cross border)

**DPI without interoperability is a silo. Interoperability without DPI is insecure point to point connections. Together, they unlock value.**

# GOVERNMENT INTEROPERABILITY FRAMEWORK



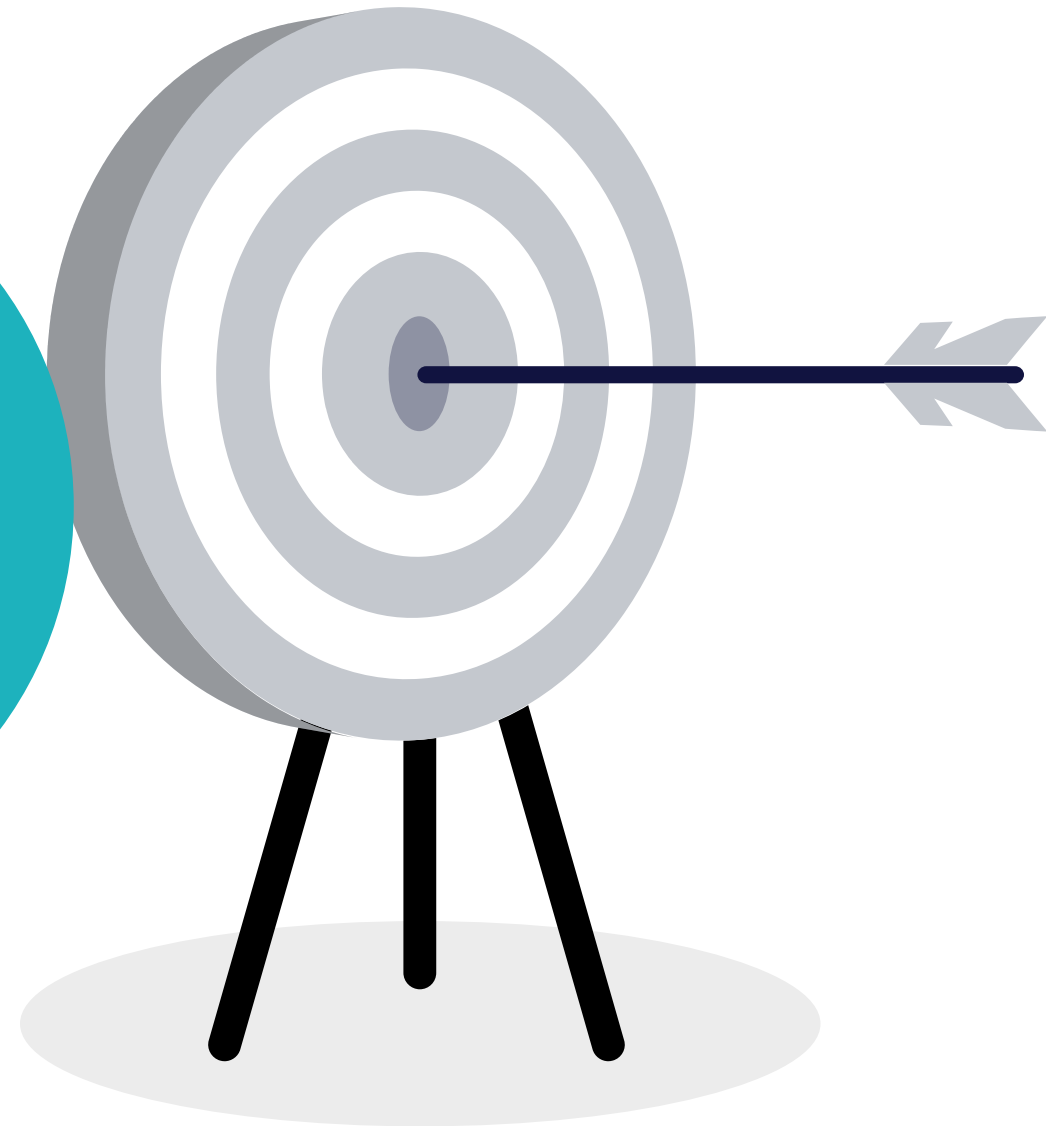
ICT SKILLS, OPERATIONS STANDARDS AND COMMUNICATION

LEGAL & GOVERNANCE FRAMEWORK

SECURITY



# GOVERNANCE



# GOVERNANCE OBJECTIVES:



POLICY  
COHERENCE

STANDARDS  
ENFORCEMENT

TRUSTED  
INTEROPERABI  
LITY

CITIZEN TRUST  
AND  
ACCOUNTABILITY



Ultimately it is the Citizen trust  
Cybersecurity and resilience

## The Ministry of ICT acts as the orchestrator of Kenya's Digital Public Infrastructure ecosystem.

### Strategic Leadership:

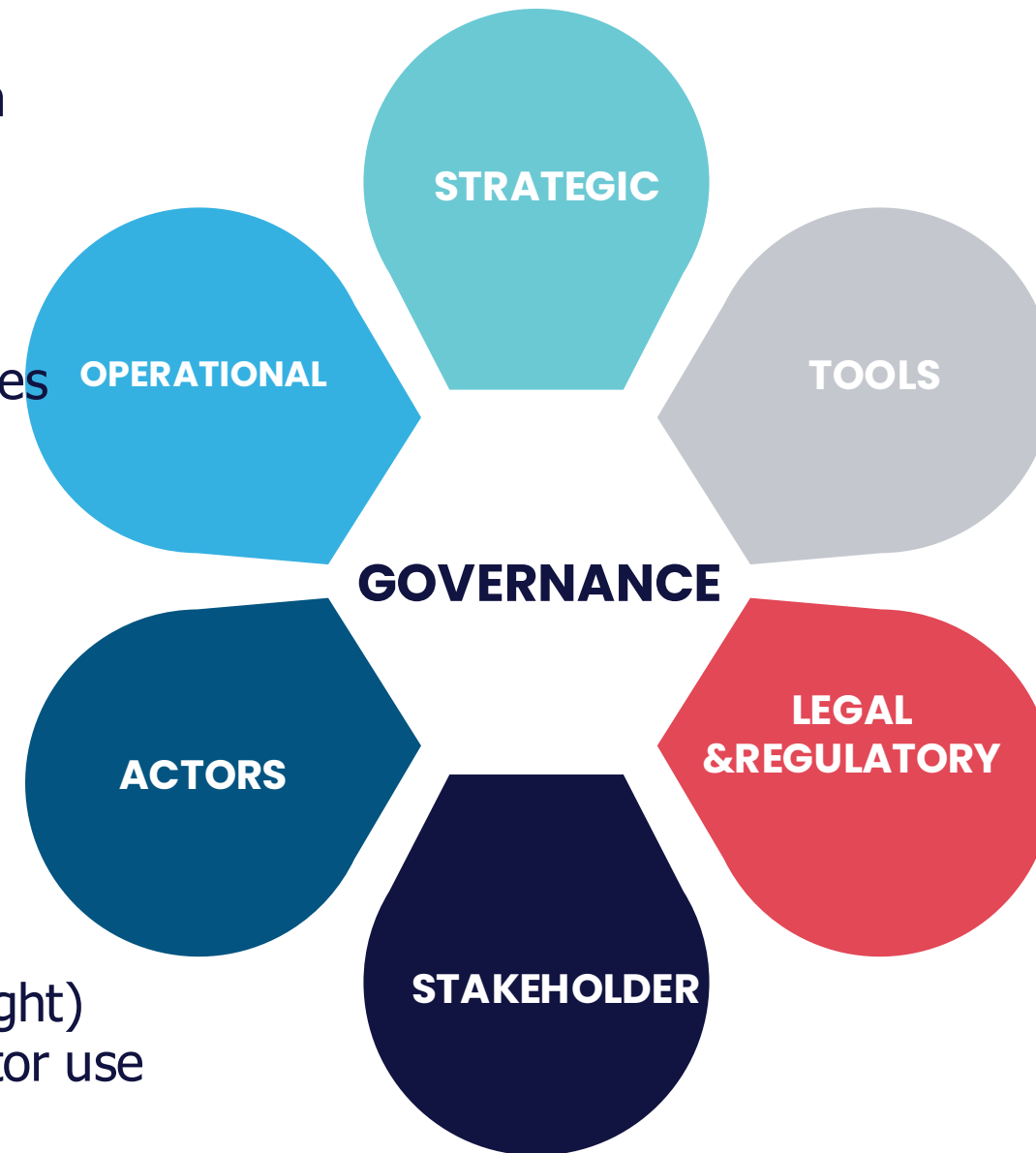
- Cabinet-level digital transformation oversight
- Ministry of Interior and National Coordination
- Ministry of ICT Leadership
- Inter-ministerial steering committees

### Operational Decisions:

- Technical agencies under IC
- National Registration Authority
- ICT Authority Standards Enforcement

### Key Actors

- Interior (Registration)
- ICT (Digital Transformation)
- Treasury (Funding & Fiscal Oversight)
- Health, Education, Transport (sector use cases)
- Communications Authority
- Central Bank



### Coordination Tools:

- Joint Working Groups (multi-Sectoral Committees)
- Shared Digital Roadmap
- Cabinet Approval Processes

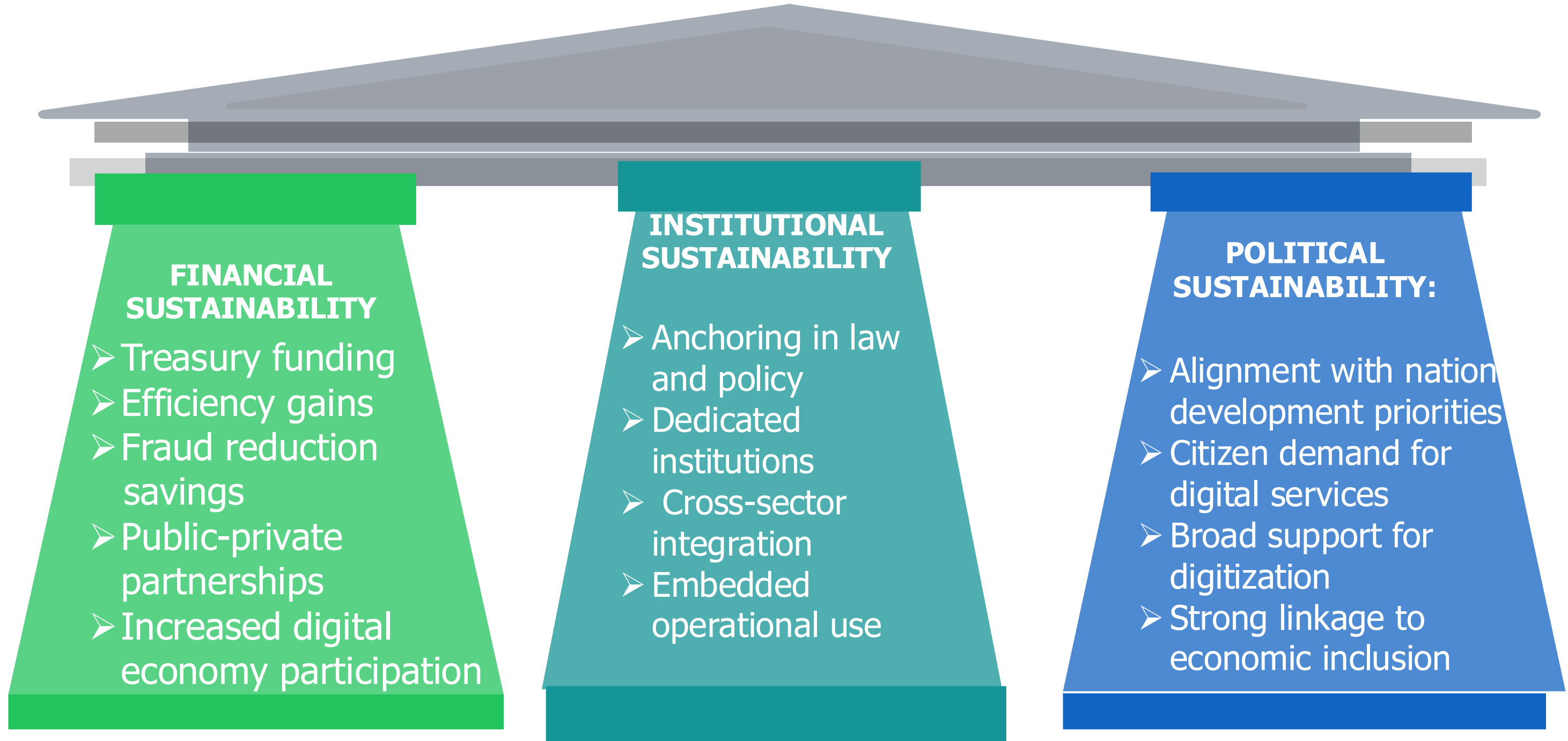
### Legal & Regulatory Anchors

- Registration of Persons Act
- Kenya Information & Communications Act
- Financial sector KYC Guidelines
- SIM registration regulations

### Multi-Stakeholder Forums

- ID working groups
- Financial sector forums
- ICT roundtables
- Private sector consultations
- ID4Africa participation

# SUSTAINABILITY MODEL



**Digital identity is now operationally embedded into Kenya's digital transformation journey**

# KEY LESSONS FOR AFRICA FROM KENYA'S JOURNEY



**1. Treat digital identity as national infrastructure**

**2. Build strong legal and governance frameworks early**

**3. Prioritize interoperability from the beginning**

**4. Anchor identity in service delivery**

**5. Prioritize citizen trust and inclusion continuously**

**6. Avoid fragmented systems**

**7. Invest in local institutional capacity**

**8. Avoid vendor lock-in**

**9. Strong political leadership is essential**

- **Ensure strong public engagement**
- **Digital identity is not an IT project It is the trust foundation of the digital state.**

Thank you for your  
attention.

