JUNE 2022

YIANNIS THEODOROU

On the Road to Digital-ID Success in Africa: Leveraging Global Trends

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

From accessing mobile money to public-health services and promoting financial inclusion, digital-identity (ID) systems can provide individuals with life-enhancing services and benefits while becoming active participants in a digital economy. Despite this, half of the estimated billion people worldwide who have no form of legal identification reside in Africa. While momentum to create such an ecosystem on the continent is building, its leaders have an opportunity to consider several trends from leading digital-transformation strategies globally.

LEVERAGING MOBILE TECHNOLOGY

Mobile technology is a key catalyst and potential gamechanger for driving and advancing digital-ID ecosystems in Africa. Smartphone penetration and mobile-internet coverage are expanding across the continent with estimates suggesting that mobile penetration will rise from 50 per cent to 64 per cent by 2025. With its relatively low costs, ease of use and popularity, mobile technology will be vital in facilitating the creation of digital-ID ecosystems.

During the Covid-19 pandemic, the global response included an acceleration of digital-transformation strategies by governments around the world. Measures included the issuing of digital vaccination passes while in Jordan and Senegal, for instance, government used mobile wallets to deliver aid payments during lockdowns. The rollout of digital-ID and verification systems has been vital to these efforts, with mobile technology at the forefront.

Recently, government policies in combination with public-private partnerships have played a pivotal role in advancing digital-ID ecosystems that harness mobile technology in Africa. For instance, mandating the registration of prepaid mobile SIM cards against users' national ID to drive demand and adoption of new digital-ID credentials. Consequently, there is a strong correlation between having access to an identity credential and having a mobile subscription (SIM card) registered in one's name. A World Bank study found that the primary reason people in developing countries

apply for an ID is to buy a new SIM card or to register their existing SIM card against their ID to avoid having it deactivated by a government-imposed deadline (where mandatory SIM registration is enforced).

In Nigeria and Tanzania, authorities license mobile network operators (MNOs) to act as official ID enrolment partners, effectively leveraging their nationwide presence to accelerate citizen enrolment onto the national digital-ID platform – and therefore supporting the inclusion of several million people who had been previously unregistered.

While digital-ID rollouts increasingly involve the capture of an individual's biometrics (fingerprints, iris, face, voice) to enhance uniqueness and avoid duplication of records, new smartphone technologies can capture individual biometric attributes during ID enrolment. For example, smartphone cameras coupled with machine learning and AI software are being used for identity verification and authentication by companies such as Element.inc and Tech5.

MOBILE IDS AND ID-WALLETS – THE NEW NORM?

A recent report forecasts that more than 3 billion people globally will be equipped with a government-initiated mobile-ID app by 2024. Concurrently, the European Union – through its eIDAS 2.0 framework – aims for every EU citizen to have a reusable ID wallet on a smartphone to present online and offline. A digital-ID wallet app would hold identity documents or attestations such as national ID cards, student IDs, driving licenses, university certificates and permits.

If executed as envisaged, the EU's revised eIDAS Regulation may set the foundations for digital-ID and ID-wallets on a global scale in ways that promote user control and preserve privacy. Countries across Africa with burgeoning digital-ID ecosystems can leapfrog outdated approaches by following this promising EU model – notwithstanding the need to first address infrastructural and capacity gaps.

MAKING OR BREAKING A DIGITAL-ID ECOSYSTEM

While billions of people reap the benefits of convenience, efficiency and security that digital IDs offer, there are also concerns. Digital IDs may increase the risk of exclusion and inequality among marginalised groups who may be unable to register for one, such as those with lower levels of digital literacy, women and children, and those in remote areas with poor internet coverage or without access to mobile devices. In addition, digital-ID holders may face several privacy risks because of sub-standard data-governance frameworks or because their country's digital-ID system creates a power imbalance between the state and its people based on the nature of the personal information collected. Lack of consumer trust in how data will be respected and protected is likely to impact demand for and usage of digital-ID services.

Many African countries still lack data-protection legislation and where it does exist, it is often "vaguely drafted, poorly implemented, or allows for significant executive discretion", according to a Research ICT Africa (RIA) and the Centre for Internet and Society (CIS) report. For example, Kenya's Supreme Court declared the country's national digital-ID scheme illegal in 2021 due to the absence of clearly defined, legal data-governance frameworks. Arguably, this decision helped other countries "by flagging these issues at the outset", with several countries now updating their data-governance frameworks to strengthen data protection and privacy and to engender trust in their digital-ID ecosystems.

STRENGTHENING THE DIGITAL-ID ECOSYSTEM

In response to some of these concerns, the African Union Commission (AUC) is working on a digital-ID policy framework that aims to ensure people can "easily and securely access the public and private services they need, when they need them, and independently of their location". Equally, the Digital Transformation Strategy (DTS) for Africa (2020-2030) stresses the significance of legal digitised-ID mechanisms on the continent, considering them critical for the successful implementation of the African Continental Free Trade Area (AfCFTA).

Given this direction, African governments may wish to consider this (non-exhaustive) list of recommendations when building or strengthening their digital-ID ecosystems:

- **Appoint a champion** within government to lead a consultative, multi-stakeholder effort to articulate a shared vision and achieve buy-in to the collective benefits of a digital-ID ecosystem.
- **Identify relevant and high-value use cases:** When designing digital-ID roadmaps, plan beyond enrolment by developing and offering use cases that offer a value add to governments, the private sector and consumers – especially those at a higher risk of exclusion such as forcibly displaced populations (due to wars or humanitarian disasters for example).
- **Address the underserved:** Maintain offline and analogue options of ID authentication at least during the transition period to avoid exacerbating the risk of exclusion for those already marginalised.
- **Prioritise mobile-based solutions:** Consider policies that make smartphones and mobile internet more affordable to encourage consumer access to digital services and benefits "on the move". For instance, promote healthy competition among (several) commercial mobile network operators to drive prices down for consumers. As mobile digital-ID wallets become available, identity authentication should still be possible even if a user runs out of data on their smartphone. During ID enrolment in areas that lack connectivity, registration agents could use smartphones to capture and store data locally (temporarily) before sending it to secure servers when back online and deleting from those devices.
- **Create conducive policy and regulatory environments**: Identify and mitigate risks of data misuse (privacy, exclusion, discrimination) through appropriate data-governance frameworks and user-centric processes. For example, this could include strengthening data protection and privacy laws by adhering to international norms and best practices to engender trust in digital ecosystems, and applying the "data minimisation" principle whereby only the necessary personal data required for a well-functioning ID ecosystem is collected. Government ID enrolment partners (in the public or private sectors) should not store personal ID data but rather encrypt it and send it to the relevant ID authority's servers as soon as

possible. Where local storage is unavoidable due to lack of internet connectivity, such data should be deleted as soon as possible. The relevant supervisory authorities (data protection commissioner, regulator, auditor, etc.) should also be empowered (in law) to carry out their respective functions independently and without political intervention.

- **Work towards interoperability and globally agreed standards** to ensure mutual recognition of digital-ID across borders. Governments and international trade bodies should proactively be involved in contributing to and shaping developments.
- **Consistently monitor and critically assess the evolution and implementation of the digital-ID ecosystem.** Governments and regional bodies should continually ensure the needs of their citizens and consumers are met (for instance, human rights, safety, cybersecurity needs) while also guaranteeing the fiscal sustainability of the ecosystem's business model to ensure growth and effective provision of services.

Infrastructure and capacity will drive digital transformation in Africa. Yet to sustain it, strategies must be trusted and inclusive. A good starting point is for governments to ensure digital-ID ecosystems are universally accessible. Done right, digital IDs will be key to growth and opportunity on the continent.

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

facebook.com/instituteglobal
x.com/instituteGC
instagram.com/institutegc

General enquiries

info@institute.global

Copyright © May 2025 by the Tony Blair Institute for Global Change

All rights reserved. Citation, reproduction and or translation of this publication, in whole or in part, for educational or other non-commertial purposes is authorised provided the source is fully acknowledged Tony Blair Institute, trading as Tony Blair Institute for Global Change, is a company limited by guarantee registered in England and Wales (registered company number: 10505963) whose registered office is One Bartholomew Close, London, EC1A 7BL.