Enhancing Functionality of Digital ID Systems: Use Cases Identification and Optimization for the Kaduna State Government (KDSG)

Digital Identity Strategy for the Government and People of Kaduna State

SUBMITTED BY:

Fola Odufuwa
ECA TCND Consultant
Digital ID Operationalization Expert:
Use Cases Identification and Optimization

September 21, 2022

ACRONYMS & ABBREVIATIONS

BVN	Bank Verification Number
CIO	Chief Information Officer
DI	Digital Identities
DPO	Data Protection Officer
ECA	Economic Commission for Africa
EMIS	Education Management Information System
FGN	Federal Government of Nigeria
G2P	Government-to-Person (G2P)
ICT	Information and Communications Technology
ID	Identity
IT	Information Technology
KADRIMA	Kaduna State Residents Identity Management Agency
KDSG	Kaduna State Government
MDA	Ministries, Departments and Agencies
MDM	Master Database Management system of the Kaduna State Government
NDPB	Nigeria Data Protection Bureau
ngCERT	Nigeria Computer Emergency Response Team
NIMC	National Identity Management Commission
NIN	National Identity Number
NITDA	National Information Technology Development Agency
P2G	Person- to-Government (P2G)
PPP	Public Private Partnership
SDG	Sustainable Development Goals
TIN	Tax Identification Number

TABLE OF CONTENTS

1. Introduction 4

2. Rationale for Digital Identity Policy and Strategies 5

3. Policy Objectives 7

3.2 Guiding Principles 7

3.2 Digital ID Policy & Strategy Objectives 7

4. Expected Outcomes of the Digital Identity Strategy 8

5. Strategies Towards Achieving a Digital Identity Ecosystem in Kaduna State 9

5.1 Create a Trust Environment for Digital Identities 9

5.2 Enable Interoperability of Digital Identity Systems 12

5.3 Promote, Implement and Ensure Stakeholder Ownership of Digital Identity Use Cases 14

5.4 Expand the Functionality of the Master Database Management System to Support Digital Identity Implementations 16

5.5 Promote and Pursue the Digital Upskilling of Government Workers 17

6. Implementation Plan 19

6.1 Institutional Arrangements 33

7. Post-Implementation Considerations 34

7.1 Migrating Analog MDAs into the Digital World 34

7.2 Commissioning and Operationalizing the Master Database Management System 34

7.3 Role of the Private Sector 34

8. Monitoring & Evaluation 35

9. Conclusion 36

1. Introduction

The Technology, Climate Change, and Natural Resources Management Division (TCND), Green Technology and Innovation Section (GTIS) of the United Nations Economic Commission for Africa ("ECA"), in close collaboration with the ECA Digital Centre for Excellence ("DCE"), is supporting the office of the Governor of Kaduna State ("KDSG") in the **Identification, Optimization and Operationalization of Digital ID Use Cases** (the "Consultation"). Towards this goal, in June 2022 ECA engaged Fola Odufuwa and Adeola Bojuwoye as the TCND Consultant/Digital ID Operationalization Expert: Use Cases Identification & Optimization and the TCND Consultant/Digital ID Integration & Operationalization Expert respectively (together the "Consultants") to carry out the Consultation.

This Digital Identity Strategy is a comprehensive document that has been developed through a consultative process that incorporates feedback received in structured interviews with 85 senior executives of KDSG across 13 Ministries, Departments and Agencies (MDAs), inclusive of 8 ICT cluster heads responsible for managing the IT infrastructure and process of the public service across all MDAs. In preparing the document, reference was also made to the related strategic plans of KDSG, and comparative digital ID policies of subnational governments in more developed geographies.

The purpose of the **Digital Identity Strategy for the Government and People of Kaduna State** policy is to identify improvements that need to be made to the operational environment currently governing digital identities and data transfers within the public service of Kaduna State for a more transformational change in the quest for a digital government. When fully implemented, the observed result across all variables of measure should be a public sector that is more responsive in meeting the needs and yearnings of the people of Kaduna State within an environment where people's online privacy and rights are well-protected.

The Digital Identity Strategy ties existing digital ID programs into a broad strategy document, complementing and extending other key policies and plans of the Kaduna State Government including the:

1. Kaduna State Development Plan 2021 – 2025,

2. Digital Strategy Policy 2020,

3. Kaduna Open Government Strategic Vision 2021-2023, and the

4. Kaduna State e-Government Strategy 2020.

To summarize, the Digital Identity Strategy should make a modern digital identity ecosystem a reality in the state and make the lives of Kaduna residents safer and easier over the course of its execution.

2. Rationale for Digital Identity Policy and Strategies

This section describes the current environment for the collection, storage and sharing of digital identities in within the public service, out of which we seek to build a new digital identity ecosystem for the state.

Digital Identities offer a safe and secure means of providing reliable authentication for the electronic delivery of G2P and P2G services over contemporary channels such as web and mobile applications.[1] The use of digital identities is veritable proof of a modernized public service as it enables administrative efficiencies, reduces waste, and boosts the convenience of users. In 2021, the provincial government of Ontario found that residents are 1.9 times more likely to use digital ID systems if they trust that the government will protect their information and 14 times less likely if they do not believe it has any benefits.[2]

In the past decade, Nigeria's data ecosystem has undergone rapid transformation with the establishment of a supportive regulatory framework and improvements in broadband data infrastructure. This has ushered the emergence of advanced data start-ups and tech hubs through which innovative solutions are being generated. National schemes such as NIMC's National Identity Database and NITDA's Data Protection Regulations have made Nigeria a continental leader in digital identities and created opportunities for the public and private sectors to work together to implement secure digital IDs solutions that solve real problems within local communities. Furthermore, the increasing availability of broadband mobile and affordable end-user devices has provided fresh prospects for secure digital enrolments with new channels opening up for reaching more communities and vulnerable constituents.

Digital IDs are foundational and can link traditionally separate or independent activities of multiple government agencies in a cross-cutting fashion. This peculiar ability to reuse digital identities can be leveraged upon to create a single, authoritative view of Kaduna citizens and residents that can be shared by numerous processes and applications on a whole-of-government basis, greatly speeding up transaction times at any service interface. This may come under a '***COLLECT ONCE***' policy. That is, once KADRIMA or any other MDA captures the full set of personal information of Kaduna citizens and residents, there would be no further need for any other MDA to collect the same information from the same individual. Digital IDs can ensure that every private individual in Kaduna is proactively and uniquely identified, and that the people who benefit from government are in good standing with the same government. Additionally, the ability of MDAs to, on their own or collaboratively, offer a wide range of applications with the potential for social, financial and digital inclusion will be enhanced through a coherent digital identity policy.

Nonetheless, though Kaduna State seeks to exploit latent opportunities in digital governance founded on digital identities, there are many innate challenges that confront including the following.

[1] McKinsey (2020), How governments can deliver on the promise of digital ID, London.

[2] Govt of Ontario (2022), Digital ID consultations – what we learned, Toronto.

1. **UNDER-DEVELOPED DIGITAL ECOSYSTEM**
While KDSG has made considerable investments in technology in recent years, the deployment and optimization of digital tools is nascent within the public and private sectors, and less than 10% MDAs have been digitally transformed Factors affecting technology implementations within the public sector in particular relate to those challenges associated with the availability and reliability of electricity and connectivity, limited technology literacy of government workers, poor documentation of electronic processes, and a pervasive post-deployment over-dependence on technology vendors and contractors.

2. **ABSENCE OF POLICY TO GOVERN THE EVOLUTION OF DIGITAL IDENTITIES**
KDSG is currently implementing a Residency Card Registration Programme by which every resident of the state is issued a National Identification Number (NIN) in partnership with the National Identity Management Commission (NIMC). However, this digital identity program has been going forward in the absence of an overarching policy document for the state, a scenario which exacerbates risks inherent in collecting, storing, and sharing personally identifiable information through any digital identity implementation. The opportunity for data compromise can be forestalled through a well-executed digital ID policy.

3. **LACK OF A TRUST FRAMEWORK**
The absence of a common trust framework to establish trusted identities across a diverse landscape of online activities prevents public sector agencies from being able to securely share digital identities among themselves or with organisations and enterprises in the private sector. As close collaboration between the public and private sectors is imperative if the government will realize its digital economy ambitions, the trust challenge can be addressed through this Digital ID policy.

4. **LOW STAKEHOLDER & CITIZEN AWARENESS OR INVOLVEMENT**
There is an acutely low awareness of the significant economic and social benefits of digital identities specifically and technology in general both in the public service and the wider public. Low public awareness means that citizens and residents do not understand their need for technology and how digital platforms and solutions can improve personal and community efficiencies. One of the reasons for this is that constituents living in localities that are underserved or unserved by Mobile Network Operators tend to be marginally or completely excluded from any digitally delivered public service of KDSG. Furthermore, it has been difficult convincing service providers to setup infrastructure for digital enrolments in rural areas. While 87% of Kaduna residents have a formal or physical ID[3] (mainly the voters card); only 52% presently possess a digital ID issued by KADRIMA. The target is for near universal digital ID coverage by the end of 2022.

[3] EfFInA (2021), Access to Financial Services in Nigeria 2020 Survey: Kaduna State Deep Dive, Lagos.

3. Policy Objectives

3.2 Guiding Principles

The digital identity strategy of KDSG is anchored on five guiding principles as follows:

1. **GOOD GOVERNANCE**	Compelling digital ID use cases. Electronic delivery of easy-to-use public services.
2. **CITIZEN TRUST**	Privacy and data protection for all. Elimination of distrust for government. Preventing the compromise of the sensitive information of Kaduna residents by cybercriminals.
3. **INCLUSIVENESS**	Increased uptake of government services by all, including vulnerable constituents and the digitally excluded.
4. **INTEROPERABILITY**	Enabling interoperable digital systems. Safe and secure sharing of records.
5. **DIGITAL CAPACITY**	Improved digital skills to support digital ID implementations.

3.2 Digital ID Policy & Strategy Objectives

Thus, in the light of the foregoing, the primary goal of this Digital Identity Strategy document is:

> *To improve the quality of governance utilizing the unprecedented opportunity offered by the adoption and use of digital identities.*

Recognizing that digital data sovereignty is critical to the shift to a knowledge-based economy as the government seeks:

1. We shall ensure that citizens and residents of Kaduna, irrespective of age, gender, location, physical abilities geographic location or socioeconomic status, are able to securely access any government service, from anywhere, at any time and on any device.

2. We shall create a trust environment for data transfers and the electronic administration of the digital identities of citizens and residents of the state.

3. We shall adopt, implement and strengthen the use of privacy-respecting digital IDs across public and private sector organisations in the state, ensuring needs-only access to the digital records of the citizens and residents of Kaduna State.

4. We shall promote the utilization of digital identity systems for the delivery of public services by implementing compelling use cases driven by fostered and sustained demand and resulting in a positive and consistent user experience.

4. Expected Outcomes of the Digital Identity Strategy

Driven by the five guiding principles of good governance, citizen trust, inclusiveness, interoperability and digital capacity, the Digital Identity Strategy will achieve the following anticipated government-wide outcomes when fully implemented:

1. Acceleration of the digital transformation goals of the Kaduna State Government.
2. Improvements in MDA program quality, service delivery and citizen value addition.
3. Increase in the trust and confidence that citizens and residents have in digital interactions with the government with cybersecurity maximised and fraud minimized.
4. Progress in information-sharing and collaboration across all levels of the government.
5. Cost-reduction for government through (for example) less reliance on paper processes at the points of interface between government and the people.
6. Improved decision-making within the ministries, department and agencies of the government.
7. Digital inclusiveness for Kaduna constituents and the removal of barriers to inclusion.
8. Harness of the social and economic benefits and potential of digital identities and enable the full realisation of the digital economy.

5. Strategies Towards Achieving a Digital Identity Ecosystem in Kaduna State

In this section, we discuss the strategies that we shall apply to develop a modern digital identity ecosystem for the state all founded on the five guiding principles of good governance (section 4), citizen trust, inclusiveness, interoperability and digital capacities.

5.1 Create a Trust Environment for Digital Identities

Beyond the development of a Policy and Strategy document to govern Digital Identities (DI), Kaduna State is in need of a regulatory framework to create a Trust Environment for data governance and digital identities within the public sector. Currently, the regulatory framework to ensure effective use of digital identities is non-existent, the absence of which can only accentuate public concern over data privacy and security and, if unaddressed, will present an almost insurmountable hurdle to widespread adoption. While KADRIMA is the legal body authorized to collect digital identities of constituents, every MDA with citizen-facing processes independently collects, stores and shares the (digital) identities of the members of the public that they serve, resulting in a fragmented, incoherent identification ecosystem.

Trust frameworks have been proven as being able to resolve legal and regulatory uncertainties, security concerns, technological complexities and interoperability challenges of fragmented digital ID networks. However, while it may be possible for the Kaduna State Government to implement a small number of use cases under the existing environment by setting up necessary rules to support those specific use cases through – for instance – executive instruments, the absence of a strong governance framework for the coordinated distribution of digital identities to build trust within the public sector may create opportunities for abuse or misuse of digital IDs which would likely limit the spread and overall benefits of digital identities across the state in general.

It seems quite apparent that the current legislation which has some bearing on digital identities (specifically the KADRIMA Law of 2021) would not be sufficient for Use Case implementations as is being proposed. To reduce systemic risks as they relate to DIs, it may be necessary to anchor the trust framework on a body legally assigned with the responsibility of developing and administering privacy-respecting regulations that can enable secure, interoperable digital identity systems within the public and private sectors of Kaduna State.

5.1.1 Implementation Strategies

1. Adopt and apply a unified, whole-of-government approach to the creation, management and sharing of digital identities of constituents of the state.

2. Create a legal and regulatory framework to govern data transfers and distribution of digital identities in the state.

    a. Establish a regulatory trust framework setting out the rules for the administration of digital identities in the state.

    b. Amend the KADRIMA Law of 2021 to establish KADRIMA as the *de jure* regulator of digital identities in the state and overseer of the proposed trust framework.

   c. Mobilize resources to enable the repurposed KADRIMA to provide oversight for the creation, accessibility, distribution and storage of digital identities within the state.

   d. Enact a data protection law that is consistent with good practices of modern governments.

3. Implement standards, processes and protocols for the secure, seamless and real-time exchange of digital identities across MDAs and with trusted external partners such as financial institutions.

   a. Develop a platform to enable a single trusted sign-in for Kaduna citizens and residents to authenticate and verify their digital identifies whenever they access government services online.

   b. Implement an internal identity and credential management system to authenticate public sector users responsible for accessing digital identities on any digital platform belonging to the state.

   c. Establish an external, state-wide accreditation process (with the level of assurance required for particular processes) to enable secure access to the digital identities of constituents by trusted external partners on a need-*to-know* basis.

   d. Adopt and implement standards (such as encryption, public keys, etc) for the collection, storage and accessibility of digital identities while protecting privacy and personal information.

   e. Monitor, detect, prevent and penalize the unauthorized transfer of the digital identities (and other sensitive information) of the people of Kaduna State.

   f. Ensure that all computer systems and other electronic devices in use for digital identities in the public sector belong to KDSG.

4. Improve the capacity, technical reliability and efficiency of existing digital ID infrastructure through new adds and definitive upgrades.

5. Work with related MDAs of the Federal Government (particularly NIMC, NCC, NITDA, ngCERT, NDPB, and the office of the National Security Adviser) to establish and operationalize fundamental protections of privacy and data security and prevent the exposure of the private data of Kaduna citizens and residents to cyberthreats and cybercriminals.

6. Strengthen the anti-fraud and cybercrime capabilities of existing digital identity systems within the public service through software and hardware upgrades.

7. Enshrine the use of unique digital ID identifiers (such as NIN Residency ID number, etc) for public services in a way that aids seamless interactions and minimizes digital/social exclusions.

8. Promote digital identity stewardship by aggressively onboarding MDAs into the trust environment through the leadership and coordination of a dedicated, multi-stakeholder project team consisting of digital identity champions. To achieve this, we shall:

   a. Identify functional positions within the public service that may be assigned (or dedicated) to be responsible for digital identity stewardship.

   b. Define roles and responsibilities for digital identity stewardship.

9. Educate public servants, private citizens and residents on the sensitive nature of digital identity and how to protect their digital identities and data transfers.

5.2 Enable Interoperability of Digital Identity Systems

Digital systems within the public service of Kaduna State are largely inefficient and remain siloed across nearly all MDAs. There is presently a need for KDSG to create an integrated, interoperable ecosystem for digital identities and data transfers within the public sector at the levels of policy and technology. Interoperability at the policy level enables the adoption by public and private sector bodies of common rules, organizational policies and processes governing digital identities and data transfers among themselves; while technical interoperability relates to the standardization of application interfaces, interchange protocols, technical specifications and controls that establish multiple layers of trust for communications between systems. [4] An interoperable system featuring higher-assurance credentials covered by both policy and technology standards will grant MDAs in Kaduna the ability to securely exchange data and databases among themselves through authenticated users, devices, and applications that are privacy-respecting.

In a few words and within our context, digital identity is the fuel for interoperability and horizontal collaboration within the public service. However, interoperability in the envisioned digital identity ecosystem depends on a number of critical factors: the level of digitization and digital readiness or maturity of the MDA, the willingness and eagerness to collaborate with other ministries and departments of government, data governance (especially as they relate to credential management, standardized digital processes and, in another instance, the prevalence of digital identities as a principal conveyor of data exchanges). The availability of digital skills to support digital ID implementations is also imperative.

Positively, on the technology front, the state has taken the first step in developing an enterprise-wide Master Database Management (MDM) system for the use of MDAs. A master database management system consists of the processes, governance, tools, rules and technology needed for the creation and maintenance of consistent and accurate master data.[5] The KDSG MDM is in pole position to become the prime platform for enterprise interoperability in the public sector of Kaduna State when completed. For the moment, only KADRIMA, KADIRS and KADGIS are reported as having achieved MDM connectivity and only about 10 of over 90 MDAs are digitized. The relatively slow rollout of the system and limited uptake of MDAs will be a major limiting factor to full interoperability within the public sector.

There are two other equally important limitations. First, while technical operability may be presently feasible, the absence of a policy or legal/regulatory framework to govern the secure exchange of data and other sensitive information between enterprise systems, departments, governments and the public will patently increase the risk of digital identity solutions. Secondly, the state does not have as yet an enterprise-wide system for verifying the digital (or even physical) identities of residents. The capability to link the digital identities of Kaduna constituents across MDAs with solutions enriched with strong security controls for delivering programs and services to the public will significantly enhance the design and quality of the government's digital services.

[4] USGOV (2011), National Strategy for Trusted Identities in Cyberspace, Washington.
[5] TBCS (2020), Digital Operations Strategic Plan: 2021–2024, Ottawa.

5.2.1 Implementation Strategies

1. Implement a '***COLLECT ONCE***' policy for digital enrolment of Kaduna individuals within the public service.

2. Link together all 'silos' of personal information of Kaduna citizens and residents held by MDAs and eliminate duplicity of digital identities across MDA.

    a. Using digital IDs, synchronize social registries across all government programs such as the Conditional Cash Register, Rapid Response Register, Government Enterprise and Empowerment Programme (GEEP), n-Power and the National Homegrown School Feeding Programme (NHSFP), among others.

3. Make interoperability and seamless integration of systems and processes mandatory for all existing and new digital identity implementations across all MDAs.

    a. Simplify all the processes required in connecting the digital systems of one MDA to another.

    b. Develop an Application Programming Interface (API) strategy to facilitate and structure the sharing of government data and information.

4. Enable remote and round-the-clock electronic verification of digital IDs in the public service.

5. Promote improvements in connectivity infrastructure by engaging with service providers to identify and eliminate geographical 'dark spots' in network provisioning.

6. Establish a baseline of time-bound standards for the collection, storage, sharing and management of digital identities and data transfers within the public sector including those that require or involve the use of interoperable layers and application programming interfaces.

7. Create state-wide security clearance levels for authorizing access by government workers to the digital identities of Kaduna constituents.

8. Identify and dismantle barriers to collaboration and information sharing within the public service.

    a. Decommission or otherwise digitally link standalone computer systems utilized for any decision-making or collaboration processes.

    b. Eliminate hoarding of information by public servants and the general unwillingness to share useful information between one MDA and another.

5.3 Promote, Implement and Ensure Stakeholder Ownership of Digital Identity Use Cases

As a follow-up to the foregoing, while KDSG is a subnational pacesetter for the digital economy relative to its peers on the African continent, the capabilities and sophistication of the public service may be viewed as digitally nascent. Digital Identity use cases can be implemented in furtherance of the development ambitions of the government for such activities such as the registration of farmers for planning purposes, remote monitoring of pupil attendance in public schools to reduce the high universe of out-of-school children, digital verifications for pensioners, and facilitating G2P cash disbursements to vulnerable segments of the population, among numerous other applications. This would however require government 'ownership' at two rungs: (a) top-level ownership of the executive government as evidenced, in one instance, in the development and planned state-wide implementation of this Digital Identity Strategy document, and (b) ownership of the leadership of the MDA sponsoring a digital identity use case program.

With respect to the latter, there is a present need for individual MDAs to take direct responsibility for 'owning' and developing high value digital identity use cases that would extend the scope, quality and ease of delivery of public services. One way to do this is for MDAs to demonstrate their understanding and eagerness to implement a Use Case by (a) assigning and dedicating a senior executive to oversee the process, (b) listing out linkages with the Development Plan KPIs that would be targeted by a particular Use Case, and (c) operationalizing the Use Case in conformity with any related Implementation Plans. In this respect, the capacity of MDA staff to implement any DI Use Case would need to be significantly enhanced on a wholesale basis. Without Use Case ownership, it would be impossible for MDAs to guarantee a consistently positive user experience or engender a high level of trust post-implementation.

5.3.1 Implementation Strategies

1. Prioritize digital identities as the primary means of solving problems wherever the government interfaces electronically with citizens and residents.

2. Review and reengineer related internal processes prior to the implementation of any digital identity use case by any MDA.

3. Design digital identity use cases with the least connected user in mind by enabling offline and narrowband options of any implementations to eliminate the exclusion of vulnerable and marginalised segments of the population from the collective benefits of a digital ID ecosystem.

4. Mobilize resources and work with development parties and private sector players to initiate and execute digital ID use cases that enable inclusive access and easy-to-use services.

5. Simplify the digital identity authentication process to ensure equitable access for all categories of residents irrespective of age, gender, location, physical abilities geographic location or socioeconomic status.

6. Ensure a consistent and coherent experience ('look and feel') across all the digital service delivery channels of KDSG such as websites, mobile and social media platforms.

7. Analyse and implement lessons learned from digital identity implementations and share identified successes and difficulties across MDAs to improve service delivery of new programs and projects.

8. Periodically rank the potential impact of new digital ID programs prior to their implementation by the responsible MDA.

9. Pursue the digital transformation of MDAs in support of digital identity implementations.

10. Enable inclusion by promoting inclusive and accessible solutions for end-users and encourage citizen access to government information and services.

5.4 Expand the Functionality of the Master Database Management System to Support Digital Identity Implementations

The Master Database Management (MDM) can become the principal source for government-held data as well as the main platform for enterprise interoperability across all MDAs. MDM was designed to integrate all government data registries and has achieved a two-way database integration between the KADRIMA and NIMC databases through an application programming interface. Presently, the enterprise database can be queried by authorized public servants to extract high value information of constituents in designing and implementing any e-government service. The present design of the Master Database Management (MDM) allows for digital exchanges within the public service through a suite of digital exchange tools including the Enterprise Service Bus and the API Gateway. These components may enable the secure exchange of data between MDAs when fully implemented. There is good evidence to demonstrate that MDM will be pivotal to the success of digital identities in the state. Nonetheless, these benefits appear largely dependent on the direction taken in implementing the digital identity components of the system as well as on the policy, technology and standards required in operationalizing a trust environment for digital identities in the state.

5.4.1 Implementation Strategies

1. Identify and extend standard digital identity data elements on MDM that can become authoritative reference points for information sharing and collaboration among MDAs.

2. Enable secure after-hours access by authenticated public workers to the MDM database for government services that require remote verification of digital identities.

3. Expand the current baseline security policies of MDM for the purposes of interoperability.

4. Achieve full integration with other national trust frameworks such as BVN, TIN, etc.

5. Enable the data enrichment capabilities of MDM.

5.5 Promote and Pursue the Digital Upskilling of Government Workers

The digital world is marked by rapid and unprecedented changes in technological innovation and data transformation and it is virtually impossible for government workers at every level to keep up except through constant knowledge exposure. Perpetual disruptions in technology require that government workers acquire new skills and competencies. This is made much more daunting by the high risks that are created in digital identity implementations, in particular, if there is a shallow understanding of what is required to secure and protect data transfers. Even when a public officer becomes digitally literate, the ability to extract high-value insights from existing data of constituents is also tied to the depth of the digital analytic skills that they possess.

The evidence shows that the manpower of the Kaduna State public service is not yet empowered to run digital processes. There is currently a preponderance of digital illiteracy among government workers which in turn entrenches a general dependence on paper-based processes and operating systems. Additionally, Nigerian governments in general are poorly branded, widely perceived as technology laggards, bureaucratic, and having limited career development opportunities for developers and other IT professionals, all of which weakens the ability of KDSG to attract and retain top IT talent necessary to support digital identity implementations. On the one hand, governments need to compete with the public sector for IT talent while, on the other, public servants need to be helped to make the necessary shifts to evolving digital realities.

5.5.1 Implementation Strategies

1. Require digital and data literacy from public servants and mobilize resources to ensure government workers are digital citizens in their own right and are able to access, participate and readily work in a digital world.

2. Improve the execution capabilities of digital identity use cases by enabling the acquisition of digital skills by public servants through dedicated training and learning activities in various modes across all staff categories.

    a. Develop an awareness campaign laying out the intricacies and benefits of digital identities.

    b. Assist decision makers within the public service to acquire a deeper appreciation for technology and digital processes.

    c. Collaborate with the private sector to identify competencies for the digital realm and design training programs to fill observed knowledge and capacity gaps.

    d. Train responsible public officers in the use of MDM.

3. Make significant improvements in the work environment through a program of incentives to better attract and retain senior- and mid-level digital talent to internally support digital identity implementations.

    a. Address any talent retention issues as it affects ICTs in general.

4. Incentivize digital literate government workers as a means of encouraging digital inclusiveness within the public service.

5. Encourage early adoption by government employees in executive or leadership positions to encourage their digitally illiterate subordinates to buy-into the digital vision of KDSG.

6. Develop a pipeline of proficient and capable professionals who may be hired at short notice to support digital identity programs and projects.

6. Implementation Plan

This section lays out an implementation roadmap that identifies and assigns responsibility for actions that KDSG intends to take over the next few years in bringing about the goals of this policy.

Government has a paramount role in achieving a privacy-respecting, secure digital identity ecosystem for Kaduna State and the steps to be undertaken must be carefully calibrated as we have outlined in this document. To this end, KDSG will lead the development of the digital identity ecosystem of the state and apply a whole-of-government approach to implementation, fostering cooperation across all levels of government to facilitate the delivery of easy-to-use digital ID programs and services to the general public.

Table 1 below summarizes the strategic action items descried in Section 5 and lays out timelines and parties responsible for policy implementations.

Table 1: Outline of implementation strategies, responsibilities and timings

No.	Policy	Strategies	Responsibilities	Time Target
1.	**Create a Trust Environment for Digital Identities in Kaduna State**	1. Adopt and apply a unified, whole-of-government approach to digital identities.	CIO KADRIMA SSG	2024
		2. Create a legal and regulatory framework. a. Establish a regulatory trust framework. b. Amend the KADRIMA Law of 2021. c. Mobilize resources to enable the repurposed KADRIMA to provide oversight for digital IDs.		

		d. Enact data protection law.		
		3. Implement standards, processes and protocols for real-time exchange of digital identities across MDAs and with trusted external partners. a. Develop a platform to enable a single trusted sign-in for Kaduna citizens and residents. b. Implement an internal identity and credential management system to authenticate public sector users. c. Establish an external, state-wide accreditation process. d. Adopt and implement Digital Identity standards.		

		e. Monitor, detect, prevent and penalize the unauthorized transfer of the digital identities of the people of Kaduna State. f. Ensure that all computer systems and other electronic devices in use for digital identities in the public sector belong to KDSG.		
		4. Improve the capacity, technical reliability and efficiency of existing digital ID infrastructure through new adds and definitive upgrades.		
		5. Work with related MDAs of the Federal Government (particularly NIMC, NCC, NITDA, ngCERT, NDPB, and the office of the National Security Adviser) to establish and operationalize fundamental protections of privacy and data security and prevent the		

		exposure of the private data of Kaduna citizens and residents to cyberthreats and cybercriminals.		
		6. Strengthen the anti-fraud and cybercrime capabilities of existing digital identity systems within the public service through software and hardware upgrades.		
		7. Enshrine the use of unique digital ID identifiers (such as NIN Residency ID number, etc) for public services in a way that aids seamless interactions and minimizes digital/social exclusions.		
		8. Promote digital identity stewardship by aggressively onboarding MDAs into the trust environment through the leadership and coordination of a dedicated, multi-stakeholder project team consisting of digital identity champions. To achieve this, we shall:		

		a. Identify functional positions within the public service that may be assigned (or dedicated) to be responsible for digital identity stewardship. b. Define roles and responsibilities for digital identity stewardship.		
		9. Educate public servants, private citizens and residents on the sensitive nature of digital identity and how to protect their digital identities and data transfers.		
2.	**Enable Interoperability of Digital Identity Systems**	1. Implement a '***COLLECT ONCE***' policy for digital enrolment of Kaduna individuals within the public service.		
		2. Link together all 'silos' of personal information of Kaduna citizens and residents held by MDAs and eliminate		

		duplicity of digital identities across MDA. a. Using digital IDs, synchronize social registries across all government programs such as the Conditional Cash Register, Rapid Response Register, Government Enterprise and Empowerment Programme (GEEP), n-Power and the National Homegrown School Feeding Programme (NHSFP), among others.		
		3. Make interoperability and seamless integration of systems and processes mandatory for all existing and new digital identity implementations across all MDAs. a. Simplify all the processes required in connecting the		

		digital systems of one MDA to another. b. Develop an Application Programming Interface (API) strategy to facilitate and structure the sharing of government data and information.		
		4. Enable remote and round-the-clock electronic verification of digital IDs in the public service.		
		5. Promote improvements in connectivity infrastructure by engaging with service providers to identify and eliminate geographical 'dark spots' in network provisioning.		
		6. Establish a baseline of time-bound standards for the collection, storage, sharing and management of digital identities and data transfers within the public sector including those that		

		require or involve the use of interoperable layers and application programming interfaces.		
		7. Create state-wide security clearance levels for authorizing access by government workers to the digital identities of Kaduna constituents.		
		8. Identify and dismantle barriers to collaboration and information sharing within the public service. a. Decommission or otherwise digitally link standalone computer systems utilized for any decision-making or collaboration processes.		
		9. Eliminate hoarding of information by public servants and the general unwillingness to share useful information between one MDA and another.		

3.	**Promote, Implement and Ensure Stakeholder Ownership of Digital Identity Use Cases**	1. Prioritize digital identities as the primary means of solving problems wherever the government interfaces electronically with citizens and residents.		
		2. Review and reengineer related internal processes prior to the implementation of any digital identity use case by any MDA.		
		3. Design digital identity use cases with the least connected user in mind by enabling offline and narrowband options of any implementations to eliminate the exclusion of vulnerable and marginalised segments of the population from the collective benefits of a digital ID ecosystem.		
		4. Mobilize resources and work with development parties and private sector players to initiate and execute digital		

		ID use cases that enable inclusive access and easy-to-use services.		
		5. Simplify the digital identity authentication process to ensure equitable access for all categories of residents irrespective of age, gender, location, physical abilities geographic location or socioeconomic status.		
		6. Ensure a consistent and coherent experience ('look and feel') across all the digital service delivery channels of KDSG such as websites, mobile and social media platforms.		
		7. Analyse and implement lessons learned from digital identity implementations and share identified successes and difficulties across MDAs to improve service delivery of new programs and projects.		
		8. Periodically rank the potential impact of new digital ID programs prior to		

		their implementation by the responsible MDA.		
		9. Pursue the digital transformation of MDAs in support of digital identity implementations.		
		10. Enable inclusion by promoting inclusive and accessible solutions for end-users and encourage citizen access to government information and services.		
4.	**Expand the Functionality of the Master Database Management System to Support Digital Identity Implementations**	1. Identify and extend standard digital identity data elements on MDM that can become authoritative reference points for information sharing and collaboration among MDAs.		
		2. Enable secure after-hours access by authenticated public workers to the MDM database for government services that require remote verification of digital identities.		

		3. Expand the current baseline security policies of MDM for the purposes of interoperability.		
		4. Achieve full integration with other national trust frameworks such as BVN, TIN, etc.		
		5. Enable the data enrichment capabilities of MDM.		
5.	**Promote and Pursue the Digital Upskilling of Government Workers**	1. Require digital and data literacy from public servants and mobilize resources to ensure government workers are digital citizens in their own right and are able to access, participate and readily work in a digital world.		
		2. Improve the execution capabilities of digital identity use cases by enabling the acquisition of digital skills by public servants through dedicated training and learning activities in various modes across all staff categories. a. Develop an awareness		

		campaign laying out the intricacies and benefits of digital identities. b. Assist decision makers within the public service to acquire a deeper appreciation for technology and digital processes. c. Collaborate with the private sector to identify competencies for the digital realm and design training programs to fill observed knowledge and capacity gaps. d. Train responsible public officers in the use of MDM.		
		3. Make significant improvements in the work environment through a program of incentives to better		

		attract and retain senior- and mid-level digital talent to internally support digital identity implementations. a. Address any talent retention issues as it affects ICTs in general.		
		4. Incentivize digital literate government workers as a means of encouraging digital inclusiveness within the public service.		
		5. Encourage early adoption by government employees in executive or leadership positions to encourage their digitally illiterate subordinates to buy-into the digital vision of KDSG.		
		6. Develop a pipeline of proficient and capable professionals who may be hired at short notice to support digital identity programs and projects.		

6.1 Institutional Arrangements

To ensure the coordinated implementation of this Digital Identity Strategy, and subject to the findings of an ongoing Data Protection Impact Assessment being undertaken by KDSG in conjunction with the United Nations Economic Commission for Africa (ECA), the government may, on an interim or permanent basis, direct four tiers of organization to create and maintain the digital identity ecosystem of the state. These layers are as follows:

1. **RESPONSIBILITY**: Direct responsibility for the *Digital Identity Strategy for the Government and People of Kaduna State* policy may be formally issued and delegated to the Chief Information Officer of the Kaduna State Government who shall have the authority to ensure the full implementation of the goals, strategies, standards, and other procedures related to this policy. However, the office of the CIO does not presently have the institutional resources to support digital identity programs specifically and technology operations in general and, as a result, ICTs at a majority of MDAs are, for the most part, internally unsupported. This lacuna needs to be permanently filled by the mandating of an entity by the executive arm of government for the support of technology assets and processes within the public service, possibly on a Public Private Partnership (PPP) basis.

2. **REGULATION**: Custodianship and regulations of digital identities may rest with the Kaduna State Residents Identity Management Agency (KADRIMA). KADRIMA has developed and currently manages the state's functional ID system and database with the collaborative support of NIMC.

3. **DATA PROTECTION**: Within the next 12 months, KDSG may consider recruiting and appointing a Data Protection Officer (DPO) for the state who shall be directly responsible for the fuller development and implementation of the data protection & privacy framework, regulations and legislation of the state in close collaboration or under the supervision of the Ministry of Justice. The DPO shall also monitor the compliance of MDAs to their data protection obligations under state and federal laws and regulations, among other responsibilities.

4. **MONITORING**: Independent monitoring board consisting of senior government executives, representatives of the private sector, academia and civil society.

7. Post-Implementation Considerations

7.1 Migrating Analog MDAs into the Digital World

The success of the Digital Identity Strategy is directly tied to the extent to which we reform and digitally transform MDAs that are struggling to exit out of the former ways of doing government business. These MDAs exist at two levels: those that were previously digitized but are saddled with legacy systems and out-dated technology infrastructure, and those that barely have any technology assets in the first place. As a result of these challenges, the state does not presently have sufficient infrastructure to support digital identities. Even a piecemeal approach to digital ID use case implementations may not suffice as each new program will require its own systems, processes and people and interoperability if *real* success would be attained.

Thus, it would not be enough to simply adopt a digital identity strategy without making critical changes to our digital governance, management practices and operations across all ministries as we continue to build on the foundation for a digital government. Towards this, we shall work relentlessly to eliminate all legacy barriers and institutional resistance to digital transformation and digital identity implementations in the state. We shall continually track, consistently monitor and critically evaluate the implementation of the digital identity ecosystem to ensure full compliance with the aims of policy.

The momentum being gradually generated through the process of prioritizing and implementing Digital ID Use Cases needs to be grown and sustained by making key stakeholders (and even the general public) aware of the potential and benefits of these use cases and digital identities in general. This would likely aid the acceptance, usage and end-user trust of any proposed DI solution.

7.2 Commissioning and Operationalizing the Master Database Management System

MDM is currently in the last stages of development and has not yet been handed over to KDSG by the contractor. As such, the database is not yet in use and the server is being turned off frequently to save on costs. We recognize that if any of the goals and broad ambitions of this Digital Identity policy would be achieved, it would be imperative to fully implement and commission MDM.

7.3 Role of the Private Sector

We also recognise that unless direct linkages are made between the state, private sector and civil society, this Digital Identity Strategy may not succeed. While the public sector must retain leadership, accountability and oversight capabilities for digital identity systems, the role of the private sector in the building, operations and use of these systems is large. The involvement of civil society in working with the government to monitor the way these systems are utilised cannot also be understated. Crucially, this Digital Identity Strategy can only succeed if the enabling environment for the digital ecosystem is self-sustaining and is not an onerous burden on the government. This will require innovative funding models to incentivize actors at all levels to play their expected roles in the development of the ecosystem.

8. Monitoring & Evaluation

We shall measure the progress of the implementation of this policy using the following parameters:

1. Percentage of Kaduna citizens and residents with unique digital ID identifiers.

2. Percentage of Kaduna citizens and residents who are being served receiving government services through the use of digital IDs.

3. Percentage of Kaduna citizens and residents who are confident that their personal information and sensitive data is secure.

4. Percentage completion of the MDM system.

5. Percentage of MDAs that have been connected to the MDM.

6. Percentage of government services equipped to offer and support digital identities.

7. Percentage of MDAs that are collaborating with each other using the digital identities of Kaduna citizens and residents.

8. Level of usage of digital identity components of MDM.

9. Increase in the number of government employees benefitting directly from any digital identity training programs.

9. Conclusion

This first-ever **Digital Identity Strategy for the Government and People of Kaduna State** creates a comprehensive framework for the management of privacy-respecting digital identities in the state. It will enhance the government's determination towards a digital and data driven economy and help ensure that government services are more convenient, reliable and digitally accessible by every segment of the population. The document will also serve to guide and shape all future public and private sector digital identity initiatives in the state.