

https://dspace.org/

Digital public infrastructure (DPI) across Africa: A national identity systems perspective

Klaaren, Jonathan

2026-07-17
LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://hdl.handle.net/10539/49981

Downloaded from a DSpace repository. https://dspace.org/

Digital public infrastructure (DPI) across Africa: A national identity systems perspective

Jonathan Klaaren
Professor, School of Law and Wits Institute for Social and Economic Research (WiSER), University of the Witwatersrand, Johannesburg
https://orcid.org/0000-0002-8732-3771

Abstract
A rising global politics advocates for national investments in digital public infrastructure (DPI). The national DPI paradigm combines three core elements: digital national identity systems, digital national payment systems, and safe and secure data exchange. This study, grounded in literature on national identity systems and legal identity, assesses digital national identity systems in several African countries. Based on two of the core functions of identity systems (identification, authentication), as well as identity systems' linkages to national payments systems, the study conceptualises four main types of digital national identity systems present in African countries: identification-led, authentication-led, plural, and payments-led. The study tests the applicability of the typology on a set of 11 African jurisdictions and finds that eight of the jurisdictions fit within the typology: South Africa, Uganda and Zambia (identification-led systems); Ethiopia and Morocco (authentication-led systems); Ghana (plural system); and Kenya and Nigeria (payments-led systems). The study contributes to global DPI debates by emphasising the authentication function in identity systems, by problematising the relationship between national identity systems and payment systems, and by engaging with global DPI indicators.

Keywords
digital public infrastructure (DPI), digital national identity systems, digital national payments systems, identification, authentication, authorisation, identification-led identity system, authentication-led identity system, plural identity system, payments-led identity system, Africa

DOI: https://doi.org/10.23962/ajic.i37.25654

Recommended citation
Klaaren, J. (2026). Digital public infrastructure (DPI) across Africa: A national identity systems perspective. *The African Journal of Information and Communication (AJIC), 37,* 1–16 . https://doi.org/10.23962/ajic.i37.25654

This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:
https://creativecommons.org/licenses/by/4.0

1. Introduction

At global level, the promotion of national digital public infrastructure (DPI) has been mounting in recent years (Bhattacharya et al., 2023; Eaves et al., 2019; Macdonald, 2023a). In the African context, motivations for investment in national DPI initiatives are having a particular impact—and draw a degree of their particular politics—from their intersection with national digital identity and national digital payments systems under the care of governments. African national DPI initiatives have to date tended to take the form of public or public–private initiatives to change existing public service delivery systems (Musoni et al., 2026; Mzinyati & Cloete, 2025; Sang et al., 2025; Sani, 2025). The value claims of inclusion, security, and effective service delivery associated with these DPI initiatives have been met with resistance from certain civil society rights actors and with critical examination by certain human rights scholars—with these actors and scholars advocating for safeguards, including greater data protection and privacy rights (CHRGJ, 2022; Gurumurthy et al., 2025; Manby, 2021; Silva et al., 2023). Drawing on the corpus of literature on national identity systems and on legal identity, this article proposes a four-part typology of ideal digital national identity systems with which to assess African initiatives under the rubric of DPI.

Motivations for investment in DPI often refer to the globally recognised example of India's Aadhaar digital identity system. In terms of individual participants registered and monthly transactions supported, this built-

in-India platform is the largest government-issued identity programme in the world. Since India's Supreme Court judgment of 2018 shored up its formal authorisation, the Aadhaar system has been endorsed by many privacy advocates, with one advocacy body referring to it as "an interesting model to consider for large-scale deployments" (OpenID, 2023, p. 13). Implemented through India's Modular Open Source Identity Platform (MOSIP), Aadhaar's legitimacy was greatly enhanced during the COVID pandemic (Martin, 2021, p. 105). Aadhaar is the digital identity base for the country's India Stack DPI. With biometric data stored in the cloud through Aadhaar, India Stack's application programming interfaces (APIs) enable a range of functions, including enrolment and identity verification for government services. India Stack's APIs also provide other forms of digital identity, such as financial addresses (enabling the United Payments Interface (UPI) with which digital payment applications can interface) and provision of a consent layer allowing for the exchange of personal data (Dattani, 2020).

At national level, the DPI paradigm comprises three interconnected elements: a digital identity system including electronic verification/authentication; a digital payments system; and a set of ground rules for digital exchange of personal data. As Sandman and Eaves (2023) have observed:

> [...] the set of capabilities that enable participation in society is constantly evolving, but over the past two decades, several countries have converged on three capabilities that they manage as digital public infrastructure, specifically the ability to: Digitally verify identities; securely send or receive money; [and] safely exchange personal information.

The digital identity layer is regarded as the foundational layer of DPI. Without identity, neither payments nor data exchange would function.[1]

The DPI concept is most often applied to the adoption and implementation of infrastructure at country level, due to the national scale of most digital identity systems (Heslop, 2020). The example of the India Stack DPI and its Aadhaar digital identity system illustrates that the distinction may be made between: digital platforms that deliver services; and the corresponding technology, data, standards, governance arrangements, and other components that constitute the platform architecture (Roitman, 2023, p. 2). Often passed over in DPI advocacy, this is the difference between the functions that a DPI performs (or is expected to perform) and the constituent infrastructural elements of the DPI, which must be constructed.

Conceptual treatment of DPI is tightly bound up with its legitimacy and its justification. Also, in many renderings of the concept, the meaning of and call for DPI are abstracted from the specific context of the country or countries adopting such infrastructures. In recent years, the DPI paradigm has become increasingly coherent and is now arguably the subject of conceptual agreement (Eaves & Rao, 2025). This coherence has been accelerated by the DPI focus of successive G20 agendas promoted by the DPI-leading nations, namely India, Brazil, and South Africa (Le Roux, 2025; Shaffer, forthcoming). Further contributing to, as well as demonstrative of, this coherence, is the set of indicators allowing for global tracking of DPI that has recently been released as the DPI Map (IIPP, n.d.; Rao et al., 2025).

The assemblage of various DPIs in African countries poses questions of public value (Eaves et al., 2024; Eaves & Kedia, 2023). The funding and building of DPIs are typically conducted, or proposed to be conducted, through the public procurement authority of an African government, often with external assistance. It requires a series of well-resourced operations to obtain and assemble the necessary elements for building the identity, payments, and exchange systems of a country-level DPI.

This article surveys the DPI paradigm through the lens provided by the corpus of literature on national identity systems and legal identity. The article draws on these literatures to propose a four-part typology of African digital national identity systems, to explore the logic of the systems' operationalisation, and to explore the systems power dynamic in relation to payments systems. Eleven African national jurisdictions are identified for review, and eight are found to have national identify systems that correspond to one of the four types of digital national identity systems.

---

1 The DPI terminology is admittedly "somewhat amorphous" (Shaffer, forthcoming, p. 7). In addition, and as a counterpoint to the payments-explicit definition employed here, see the UNDP's definition of DPI as "a combination of (i) networked open technology standards built for public interest, (ii) enabling governance, and (iii) a community of innovative and competitive market players working to drive innovation, especially across public programmes" (Shaffer, forthcoming, p. 7).

2. Digital national identity systems

A digital national identity system encompasses the relevant technology, the rules and processes regarding identity, and the implementation and practice of the rules and processes of the system. The system is embedded within a governance framework, whether explicit or implicit, consisting of the technical and operational specifications for the system and its legal rules (Nyst et al., 2016, p. 37). For digital national identity systems, the legal rules are "a combination of existing public law" that includes identity-specific statutes; generally applicable privacy and data protection law; and competition and consumer protection law, supplementing "contractual agreements between the parties and any standards adopted [usually in such contracts]" (Nyst et al., 2016, pp. 37–38).

There are three core functions to an identity system, namely: identification (also known as enrolment, or identity-proofing), authentication; and federation and assertions (functional authorisation) (NIST, 2023). Once enrolled and authenticated, an individual's identity can be further asserted in federated systems, as part of ongoing service delivery or party identification in transactions.[2] According to Nyst et al. (2016, pp. 28–29), identification requires the authorities and the system to establish baseline information unique to the individual or organisation, which involves examining source documents such as birth certificates; corroborating sources of data; and collecting biometric data, referred to as breeder documents. Authentication requires asserting an established identity through presenting and verifying supporting documents already in the system. Authentication can use biometric data for such verification. Authorisation implies determining which services are available to the authenticated person or entity. While Nyst et al. (2016) argue that a digital national identity system must include digital authentication, this study, grounded in the perspective of African identity systems with only partial digitalisation, regards digitalisation of any of the three identification functions—identification, authentication, or authorisation—as evidence of the presence of a digital national identity system, albeit (when not all three of the functions are digitised) one with limitations.

A conceptual distinction widely acknowledged in the field of identity systems is the distinction between foundational identity and functional identity (Gelb & Clark, 2013). An example of foundational identity is a passport or an adult national identity card issued to enrol an individual in the national identity system and to provide proof of legal identity. An example of functional identity is a driver's licence, which provides proof of driving competence and may also serve as a form of legal identification. From this article's perspective, legal identity may best be understood as "that identity that is associated with an individual who it has been formally established has a right to reside in a country, with all of the rights and responsibilities that flow from that" (Nyst et al., 2016, p. 30). In this sense, legal identity may be understood as a right of residence in a particular country, and distinct from and not restricted to citizenship status (Dahan & Gelb, 2015).

Establishment of legal identity is a requirement for authentication and authorisation of digital payments. Accordingly, there is a significant linkage between digital identity systems and the financial sector, specifically to digital national payments systems (Ricks, 2018). In the context of DPI, the linkage between digital identity and digital payments system is enabled both by digital technologies, such as payment platforms, and by supporting legal and regulatory modalities, such as contract law, legal identity, and financial-sector regulation (Carruthers, 2020, p. 152; Pistor, 2019).

3. Categorising digital national identity systems

The relationships among the core functions of identity systems, and the relative prominence of these functions, are central to understanding DPI. Also important is examining the linkages between national identity systems national payments systems. Through focus on these elements, this section constructs a proposed four-part typology of national identity systems present in African jurisdictions.

The primary function of an identity system is identification (also known as enrolment), and the secondary function is authentication. Prior to the adoption of digital systems, identification came sequentially and prominently before authentication. In the pre-digital dispensation, a person was first issued with an identity

2 Thus, one might reserve the term "digital legal identity system" for the set of state agencies that fulfil the enrolment and authentication functions.

document—upon presentation of breeder documents and the capture of biometric data at the primary issuing department. Then the person could use the proof of identity to exercise their right to vote at a polling station or to obtain a driver's licence at a testing station. Here the identification—acquisition and possession of the identity document—was more prominent than the authentication.

In digital national identity systems, the relative prominence of the identification and authentication functions is no longer clear. In the digital space, the two functions are often tightly coupled, as the same organisational entity may now be responsible for both identification and authentication, and may use many of the same processes or personnel for both actions. For example, the Aadhaar system in India is responsible for both the identification of residents of India and the subsequent authentication of their identity. In South Africa, the responsibility for these two functions also currently lies with a single entity, the Department of Home Affairs (DHA). However, the degree of interdependence between these two functions is much greater with Aadhaar, in part because the statutory entity implementing Aadhaar is the Unique Identification Authority of India (UIDAI)—a targeted entity designed to fulfil or ensured fulfilment of these two functions.

In the case of India's Aadhaar system, digitisation has impacted the identification function, but the key impact has been with respect to authentication, which digitisation has revolutionised, both in form and in speed—such that authentication is no longer primarily a decentralised operation at government service desks and is now largely mediated through a nationally centralised website or other electronic channel. Furthermore, this authentication happens instantaneously, providing heightened efficiency (or system failure when internet access or interoperability is disrupted).

It is possible to identify two types of digital national identity systems with respect to the sequencing and systemic coupling of identification and authentication:

- *identification-led systems*, which demonstrate clear sequencing and prominence of the identification function, with relatively loose coupling of the identification and the authentication functions.
- *authentication-led systems*, which demonstrate less-clear sequencing and a greater degree of prominence of authentication, as well as relatively tight coupling of the identification and authentication functions.

The prominence of a function within an identity system indicates its degree of system power (Medaglia et al., 2022). The relative power of the identification and authentication functions is coupled with the relative power of the governance framework of the legal rules (powerful in an identification-led system) or of the technical and operational specifications for the system (powerful in an authentication-led system). Both identification-led and authentication-led identity systems are implemented primarily using a foundational rather than a functional identity. Functional identification can be relatively prominent in national identity systems without prominent foundational identification. This points to a third type of digital national identity system:

- *plural systems*, which do not have prominent implementation of either the identification or the authentication functions.

In plural systems, sector-specific identification arrangements provide identification and authentication (bringing into view the third core function of an identity system, namely authorisation) but do so without any dominant identification or authentication scheme. These are non-dominant identity systems, in which multiple schemes of functional and foundational identification are provided and authenticated. Such identity systems that are characterised by a plurality of functional identities, without the dominance associated with foundational identity systems, are treated, in this study's typology, as examples of plural systems.

National identity systems across Africa tend to vary by virtue of their linkage or absence of linkage to a national payments system. The DPI paradigm envisions such linkage. The payments layer connects to both the digital identity layer and the data exchange layer. Credible and trusted identification is crucial for the authorisation of transactions within a payments system. In most countries, only persons above a legally defined age and with a legally defined citizen/immigration status can hold a bank account or register a mobile subscriber identifier module (SIM) card. Under contemporary regulatory capitalism, the use case

of a national payments system may influence or even drive the technologies, rules, and standards of the identity system with which it is linked. This generates a fourth type of digital national identity system:

- *payments-led systems*, as they are significantly influenced or driven by a national payments system, and by actors and dynamics within that system.

We are thus able to construct a four-part typology of digital national identity systems to use in assessing DPI approaches in African countries:

- An *identification-led* national identity system has a dominant foundational identification scheme that is digitally authenticated and is linked to, but not driven by, a national payments system.
- An *authentication-led* national identity system has a dominant digital authentication scheme, authenticates a foundational identity as well as other functional identities, and is linked to, but not driven by, a national payments system.
- A *plural* national identity system has multiple identification schemes, at least one of which is digitally authenticated but without any being dominant, and is linked to, but not driven by, a national payments system.
- A *payments-led* national identity system has at least one identification scheme that is digitally authenticated and is driven or significantly influenced by its linkage with the national payments system.

4. Identification of African national identity systems for review

This section identifies the African digital national identity schemes that are significant in the DPI context, using data recently collected for the DPI Mapping initiative at the Institute for Innovation and Public Purpose (IIPP) at University College London.[3] The initiative's key output is its DPI Map.[4] The DPI Map should be understood as a guideline or analytical tool for assessing certain DPI-related features, rather than as a definitive authority on DPI status.

In order to collect the base data for this review exercise, the African jurisdictions covered in the DPI Map were selected as the primary database. The DPI Map defines a digital identification system as ranging "from basic identification systems that provide digital authentication for users to more advanced systems that enable citizens to share their credentials with other institutions for a variety of purposes beyond mere self-identification. The Map focuses [on] national or federal-level ID systems that are governed by public institutions" (DPI Map, n.d.).

There are 52 African jurisdictions covered in the DPI Map database, and the Map's determination that a country digital national identity system is based on four required indicators:

- a digital identity documentation system;
- a digital authentication system;
- at least a planned or pilot digital ID; and
- two implementation use cases.

For this study, it was decided to focus on two indicators in order to select a set of African digital national identity systems that are significant: one indicator drawn from the four above-listed DPI Map indicators, and a second indicator focussed on national payments systems.

- The first chosen indicator is *existence of a digital authentication system*, labelled by the DPI Mapping initiative "digital authentication systems" (second in the list of four above). The key element of this indicator, for the purposes of this study, is that these systems operate as part of the national identity system. The list of "authentication methods" that satisfy this indicator, according to the DPI Mapping initiative, are appropriately diverse: "demographic details, biometric data (fingerprints/iris), facial recognition, OTP (one-time password via mobile or email)" (IIPP, n.d.).

3 The full method details and the compiled dataset are available at https://osf.io/86xdw/overview.
4 See The Digital Public Infrastructure Map at https://dpimap.org/

- The second chosen indicator is *existence of a digital real-time payments system*. Combined with the first indicator, the existence of a real-time national payments system is a sign of the significance of the identity system as an integral part of the country's DPI. (There appears to be no indicator in the DPI Mapping project that speaks directly to the linkage between the digital identity layer and the digital payments layer.)

It was decided that by using these two indicators, the DPI Map data can plausibly allow us to identify African digital national identity systems that are significant. The application of these two indicators as filters leads to a set of 11 African jurisdictions that each have a combination of a digital authentication system and a digital real-time payments system. Among the 11, five of the jurisdictions with leading national identity systems, which are frequently discussed in the literature, are present: Ethiopia, Ghana, Kenya, Nigeria, and South Africa. The other six jurisdictions are: Egypt, Mauritius, Morocco, Seychelles, Uganda, and Zambia.

5. Categorising African national identity systems

Eight of the 11 African national identity systems selected can be categorised in terms of the four-part typology of digital national identity systems proposed above:

- identification-led systems: South Africa, Uganda and Zambia
- authentication-led systems: Ethiopia and Morocco
- plural system: Ghana
- payments-led systems: Kenya and Nigeria

The three remaining national jurisdictions among the 11 found to be significant—Egypt, Mauritius, and Seychelles—could not be categorised in terms of the proposed four-part typology.

This section now provides short overviews of the digital national identity systems in South Africa, Ethiopia, Ghana, Kenya and Nigeria, thus providing at least one example of each of the four categories in the proposed typology. The overviews consider the key digital identity features, and the power dynamics of the identity systems, in each country.

South Africa: An identification-led system

South Africa's system has identification coupled with a working electronic authentication function as well as a digital national payments system. It is considered one of the world's leading identity systems, particularly for its use (and, under apartheid, abuse) of biometric technology (Breckenridge, 2014a). Albeit with a degree of inefficiency and corruption, South Africa's DHA provides birth registration and adult identification documentation for most citizens, permanent residents, and recognised refugees. In contrast to apartheid's failures in this respect (Breckenridge, 2014b), the post-apartheid government has largely succeeded in rolling out public-sector, biometrically enabled identification (Breckenridge, 2014a).

The foundational identity documents are authenticated in numerous use cases, including citizen identification, bank account verification, credit checks, and social grant distribution. National payments are facilitated through two electronic systems: PayInc (formerly BankServAfrica), which is an interbank system with real-time clearing that is operated by the South African Reserve Bank (SARB) and the commercial banks; and Payshap, a cross-domain digital system which is a collaboration including PayInc (Milne & Lawack, 2024). In May 2026, the DHA called for public comment on a set of draft amendments to Identification Regulations of 1998, with the amendments including provisions tentatively linking the DHA digital identity with the MyMzansi digital government platform, aiming to facilitate citizens' access to public services (DHA, 2026).

The power dynamics present in the implementation of South Africa's identity system, and between it and the payments system, warrant South Africa's classification as an identification-led digital national identity system. Neither the banks nor the telecommunications firms have broken the hegemony of the DHA in identity management (DHA, 2020). Where private firms play a significant role in this sector, they do so on

the specified and regulated terms of the state. For instance, the private service provider for non-citizen visas and immigration control, VFS, operates under the supervision of the DHA (De Gruchy, 2018). In addition, while the digital technology of the authentication function is crucial to the implementation of the system, it does not lead or drive the system's operation. The use cases for information-sharing from the Population Register are, as set out in section 21 of the Identification Act 68 of 1997, firmly within the legal foundation of the identity system. The DHA shares information from the Population Register with insurance businesses and banking institutions.[5]

In July 2025, the system received a major upgrade in its operating business model and increased its rates of cost recovery in order to keep pace with developments in the private-sector use of this service. The DHA negotiated and concluded service-level agreements with a set of trusted financial institutions, facilitating both the existing authentication service and enlisting some banks in the state-controlled identification enrolment function.6

The national payments system does not drive the identity system but is integrated with it under fairly close state supervision. Breckenridge (2019b) has detailed the origins and rise of a maverick firm, Net1, within the payments sector that had the potential to transform the identity system, but that firm's ambitions were ultimately thwarted by the combination of national regulation and existing globally dominant payment firms (Breckenridge, 2019b). South Africa's 2025 Roadmap from the Digital Transformation of Government includes provision for a "Functional Digital Identity for People to Securely and Remotely Access Services", which is planned within central bank regulation of the payments system and is to be integrated with the identity system (MyMzansi, 2025, p. 4).

Ethiopia: An authentication-led system

Ethiopia's National ID Program is coupled with a working electronic authentication function and is linked to a digital national payments system. Envisioned as the country's technology-based foundational identity, the biometric digital ID scheme Fayda, with a 12-digit unique identification number, was launched in 2021 (Sani, 2025, p. 6). By mid-2025, 15 million Ethiopians had enrolled, and the target is 90 million citizens by 2027 (Nkosi, 2025). Fayda replaces the Kebele ID, which is the de facto foundational identity (Ayano, 2018) and the project is intentionally prioritising women in its registration process (World Bank, 2025). Authentication is central to the identity system and is provided both online and offline (National ID, n.d.). Through use of Fayda's authentication function, the National Bank of Ethiopia began in 2023 to fast-track the Fayda ID as the primary ID for banking, demonstrating complementary roles for the identity and payments systems (Radier, 2023).

Fayda is based upon the MOSIP technology associated with India's Aadhaar. Developed, supported, governed, and promoted by India, MOSIP has been marketed, through the success of Aadhaar, as a developmental digital platform for running a national identity system and avoiding vendor lock-in. Seen as a one-stop validation and government services platform (termed MESOB (Modern Ethiopian Service for Organised Benefits)), Fayda uses MOSIP technology with local adaptations for its digital identification (Nkosi, 2025). In the Organisation for Economic Co-operation and Development (OECD) definitional distinction between digital public goods and DPI, MOSIP is a prime example of a digital public good (OECD, 2021).

An examination of the power dynamics in the implementation of Ethiopia's identity system, and between it and the payments system, shows that Ethiopia should be classified as an authentication-led digital identity system. Identity management remains firmly under public control and is regulated at a whole-of-government scale. The Fayda identification scheme is part of a modernisation project launched in 2021 and

5 Identification Act 68 of 1997, section 21. https://www.gov.za/sites/default/files/gcis_document/201409/a68-97.pdf
6 Parliamentary Monitoring Group (2025). *Department of Home Affairs & BMA 2024/25 Annual Reports; DHA ICT rollout of self-service kiosks; One-Stop Border Post Bill; with Minister*. https://pmg.org.za/committee-meeting/41734/?utm_campaign=minute-alert&utm_medium=email&utm_source=transactional

backed by national authorities and international donors (Beny, 2025, p. 166). The adoption was motivated in part by what was seen as Ethiopia's lagging position in the uptake of digital payments services (Alemu et al., 2021). In contrast with South Africa, the digital technology of the Ethiopian system's authentication function is crucial to the implementation of the system; it is central to the system's design and drives its rollout. In July 2025, it was claimed that Fayda had "become the authentication backbone of Ethiopia's digital transformation, serving 55 service providers while cutting service delivery time by 60 percent" (Nkosi, 2025). This configuration of identity systems functions and the relationship to the payments system is acquiesced to by the relatively nascent private financial sector. Fayda's real-time verification function is endorsed by the national banks as part of the National ID Program (Radier, 2023).

Ghana: A plural system

Ghana's national identification scheme is coupled with a working electronic authentication function and linked to a digital national payments system. Beyond the state-issued Ghana Card, which is held by only a minority of Ghanaians, Ghana uses several functional ID credentials (Thiel, 2020). These include election registration, tax administration, a driver's licence, a SIM card, health insurance, and government payroll credentials (Debrah et al., 2019; Effah & Owusu-Oware, 2021). With respect to authentication, various forms of verifiable identity have been provided by the civil registration agency and by other state institutions, often in alliance with a private firm. From 2001 to 2017, identity verification was fragmented and significantly outsourced, although the state maintained some degree of control over civil registration (Thiel, 2020, pp. 121–130). In recent years, the National Identification Authority's (NIA's) official Identity Verification System Platform (IVSP) has begun to authenticate holders of the Ghana Card. The e-zwich card, a biometrically regulated smartcard that operates through the national payments system, arose out of the failure of a national identity card programme initiated through and driven by the NIA from 2001 (Breckenridge, 2010). A digital wallet (payment) functionality was integrated with the Ghana Card from April 2026 (Africa News Agency, 2026).

Turning to the power dynamics in the implementation of Ghana's identity system as well as between it and the payments system, Ghana's dispensation is best seen as plural, without dominance by either the identification or authentication functions and without a clear driving influence from the payments system. The Ghana Card began using fingerprint biometrics in 2019. In 2023, a digital version of the Ghana Card and the development of a mobile authentication app were introduced, in recognition of the incomplete coverage of the authentication platform, the IVSP, across the country (Macdonald, 2023b). Biometric authentication of the holder of a Ghana Card is promoted by the banking and payments systems, though the payments system does not supplant or dominate the national identity system (Macdonald, 2025a). The e-zwich biometric payment card is used for government payments, and the Ghanaian real-time clearance system enables operation of the card, demonstrating that the identity system is not directly influenced by the payments system (Thiel, 2020).

Kenya: A payments-led system

Kenya is, at the time of writing in mid-2026, in the process of rolling out digital national identification that is coupled with a working electronic authentication function and linked to a digital national payments system. The current official system of identity numbers is the Maisha Namba, launched in October 2023 alongside amendments to the Registration of Persons Regulations in order to provide for both an electronic identification card and an electronic civil register (Ombati, 2023). Maisha Namba replaced an earlier failed scheme of identity numbers, Huduma Namba, which suffered several technical and legal setbacks (Kabata, 2024; Mutung'u & Rutenberg, 2020; Mutung'u et al., 2026). The official authentication function for Kenya's digital identity system is provided by the National Integrated Identity Management System (NIIMS), Kenya's initial large public sector technology project (Caribou Digital, 2019, p. 30; Mutung'u & Rutenberg, 2020). Kenya's payments system has, since the 2010s, been dominated by telecommunications firm Safaricom's mobile money platform M-PESA (Bloomberg, 2020; Tyce, 2020).

The power dynamics in the development, design, and operation of the Kenyan identity system, and between it and the payments system, show that Kenya's digital identity system is best characterised as a payments-led. Indeed, Kenya is the globally paradigmatic case of a dominant firm in the telecommunications sector—in this instance, Safaricom—providing authenticated and verifiable identity in the form of a functional identity (Donovan & Martin, 2017; Martin, 2019). Safaricom has leveraged its dominant market power in telecommunications to expand into banking and credit (Breckenridge, 2019a; Robb & Vilakazi, 2016).

Through creating a distinctive and hugely popular system of mobile money in the 2010s, Safaricom triumphed over the Kenyan banks in a contest for dominance over the national fast-payments system, including through contesting and influencing the legal and institutional arrangements for credit information-sharing (Breckenridge, 2019a; Dafe & Upadhyaya, 2026). As a result of Safaricom's dominance and the state's difficulties in implementing Huduma Namba, there is only a minimal degree of foundational identity function and regulation with respect to the use of identity in the payments system (Upadhyaya et al., 2025). The state's identity authentication service, NIIMS, does nonetheless continue to operate while Maisha Namba is being established.

In Kenya, as distinct from the Nigerian case (see next sub-section), the issuance, authentication, and use of identity within the national payments system is firmly in private hands, rather than in those of a state agency, and is not tightly linked to foundational identity.

Nigeria: A payments-led system

Nigeria's national identification scheme is coupled with a working electronic authentication function and linked to a digital national payments system. Established in 2007, Nigeria's National Identity Management Commission (NIMC) had, by July 2021, enrolled 60 million persons in the country's foundational digital identity scheme (Okunoye, 2022). By March 2025, 118 million persons had identity numbers. The scheme operates with a National Identity Number (NIN) format, but aims to link to other identity systems rather than provide dedicated smart ID cards. It is a harmonisation and linkage programme. As of 2022, the NIN enrolment was roughly equivalent to that of the Bank Verification Number (BVN) population, but less than the populations associated with voter registration (84 million) and SIM card registration (190 million) (Okunoye, 2022). Since 2020, NIN holders have been required to link their NINs with their SIM cards, a requirement that led to an 8% decrease in internet subscriptions (Okunoye, 2022). A fast-payments system, the Nigerian Inter-Bank Settlement System (NIBSS) Instant Payment (NIP) was introduced in 2011 through the efforts of the Central Bank of Nigeria (Okunoye, 2025). The authentication system is an app that individual NIN holders can download from the Google Play Store or Apple App Store (Macdonald, 2025b).

Similar to the dynamics in Kenya—though not demonstrating the dominant power, seen in Kenya in the position of Safaricom, of a single private sector payments firm—the power dynamics in the implementation of Nigeria's digital identity system, and between it and the payments system, show that the Nigerian digital identity system is payments-led. The driving force for the increasing degree of linkage and interoperability within and across the identification and payments systems is the payment functionality.

In the 2010s, this functionality ould be seen in the process of enrolment to the NIN, where the BVN served as a feeder document for the NIN (Monye & de Koker, 2022, p. 5). In the 2020s, the dynamics can be seen through the role of the fast-payments system. By 2025, the NIP had become "the dominant channel for payments in Nigeria, accounting for 70% of all NIBSS payments processing" (Okunoye, 2025, p. 6). The driving role of the payments system with respect to identity is demonstrated by the description of the new general multipurpose ID card rolled out by the NIMC since 2024. According to the NIMC, the card has "multiple use cases: Payments/financial, government intervention/services, travel, etc" and the NIMC is "working with the Central Bank of Nigeria and the Nigerian Interbank Settlement System to deliver the payment and financial use cases" (NIMC, 2024).

6. Towards an explanatory account of African digital identity systems and DPI

The above review of selected African nations' development of digital identity systems and DPI stands to be complemented with an explanatory account of why countries have developed along their different trajectories and to the different end-states identified. Questions of interests, incentives, power, and governance should be central to understanding DPI (Shaffer, forthcoming). Who are the principal actors promoting particular configurations of identity and payments systems? Which coalitions, public agencies, private firms, international organisations, and development partners shape these outcomes? How are competing interests negotiated, and who stands to benefit from particular institutional arrangements? While a full account is beyond the scope of this article,[7] this section provides an initial analysis of the sources of variation among the examples provided in the previous section of the four identified types African digital identity systems—with emphasis on the political, institutional, economic, and historical factors that account for divergent patterns of digital identity system development.

Fitting within a relatively long-standing trend in global public discourse, contemporary calls for investment in, and building of, DPI often take practical form as public or public–private initiatives to change (modernise) existing African public identity systems. From around 2005, mobile-money intellectuals began to draw on Kenya's experience with Safaricom and M-PESA to promote the potential for financial and payments systems to synergise with digital identification schemes operating through mobile phones. This promotion was intended to promote financial inclusion and ultimately address global poverty (Maurer, 2012, p. 301). Centred in the world of finance, the narrative later aligned with the narratives of influential figures in the development sector who came to the position that the digital and biometric identification revolution embodied in India's Aadhaar system could have a significant impact on sustainable development in African national jurisdictions (Gelb & Metz, 2018; Thiel, 2020).

An African perspective would identify at least three sets of actors as promoting a DPI narrative: multilateral institutions, philanthropic foundations, and technology vendor firms (Burke, 2026). These actors are operating within what can be understood as a transnational legal order (Shaffer, forthcoming), and their actions include the sort of G20 agenda-setting action noted above. The African Union has been among the leading actors encouraging African states to develop and adopt mutually recognised digital identity systems, with a particular focus on mutual recognition among states in order to foster intra-African trade (AU, 2022). As Burke (2026) notes: "Large private foundations, especially the Gates Foundation and Omidyar Network, have also been highly influential. They have funded both the technology itself, such as the open-source identity system MOSIP, and the organisations that promote DPI globally […]". As for the technology vendors, Debos (2025) points to the dominance of European companies that sell biometric identification technology to African states—particularly French companies operating in the states of the former French colonial empire—and finds that African states have become increasingly dependent on corporate actors for both election management and citizen identification.

Given that much of the significant action by these actors within the legal order takes place at the national level, how then does one explain the emergence of a particular type of national identity system? A few factors, which also shape the relationship between national identity systems and payment infrastructures, may be provisionally identified. The primary factor appears to be the degree to which the African national state has been able to build and retain power over citizen identification—a strength of the South African state and its DHA. In the South African case, the retention of this power appears to be linked to the continuing power of the DHA over the civil registration function, also housed in the DHA.

7 Such an account should embark upon a comparative study beyond South Africa. In doing so, it might well parallel Breckenridge's *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present* (Breckenridge, 2014a). For work along similar lines exploring the modern history of the state and its identification systems and politics, see Weitzberg (2015; 2020) (Kenya) and Banégas and Cutolo (2024) (Ivory Coast), as well as Sriraman (2018) (India) and Hashmi (2021) (Pakistan). Such an account would align with Frederick Cooper rather than James Scott—seeing the understaffed, underfunded, and often under-interested colonial African state as a consequential gatekeeper rather than as a more powerful classifier (Thornberry, 2015; Weitzberg, 2015, pp. 411, 413, 425–426).

Where such state power does not exist, a further factor explaining variation is the relative power of the telecommunications and banking industries. Specifically, the Kenyan telecommunications sector is more powerful relative to its banking sector than is the case in Nigeria, Meanwhile, in South Africa, the banking actors are more powerful than the telecoms actors with respect to civil identification. Thus, in the trio of South Africa, Kenya and Nigeria, the factors just cited may help to explain the divergent paths taken towards identification-led (South Africa) and payments-led (Kenya and Nigeria) approaches to development of a national digital identity system.

Ghana provides a case where neither the state nor the private sector appears able to achieve dominance in the digital identity environment, thus resulting in a plural system. In Ethiopia, an authentication-led digital identity system is apparently emerging because the citizen identification function is historically, and still is today, firmly state-controlled. The localised and paper-based character of the existing Kebele civil registration system has allowed for, and contributed to, the state's dominance of the authentication function. The state's ambition to digitally link different domains is central to the emergent Fayda system.

7. Conclusions

This study has offered three contributions to the debates around digital national identity systems and DPI in Africa. It has differentiated the general analysis of the digitalisation of government by specifying the distinctive digitising dynamic associated with the authentication function of identity systems. This takes the study of identity systems beyond the distinction between foundational and functional identity. The study has also deepened the study of DPI by problematising the relationship between a country's national identity system and its national payments system, arguing that the nature of this relationship is a crucial feature of the implementation of both these systems. Third, the study has proposed, and partially tested, a four-category typology of digital national identity systems, finding the typology applicable to eight of the 11 African jurisdictions selected for review.

Further research should explore more fully some of the policy implications, including competition economics, of the above analysis of DPI from the perspective of identity systems. It is clear that there can be no one-size-fits-all approach to addressing the policy questions with respect to DPI that are being posed with urgency in national jurisdictions across Africa, including questions around use of public and private resources to build DPI (Eaves et al., 2024; 2025). Other significant policy and regulatory dimensions—including the importance of pursuing privacy rights and data protection principles in an integrated fashion across the digital identity and financial payments sectors, and the fit of particular regulatory strategies to the problematics of digital identity systems— also require further exploration (McCallum & Aziakpono, 2023).

Of particular urgency is the question of public value. Mapping of the sort presented in this article can assist in evaluating the costs and benefits of investments in DPI. Across Africa, nations are compelled to consider whether—and, if yes, how—to use public resources to build a DPI. The issue is, broadly speaking, part of "the policy challenge posed by the rising digital platform economy", and may be approached from "an industrial policy perspective into which competition policy is integrated as a way of refocusing the policy discussion" (Andreoni & Roberts, 2022, p. 1444).

In many African national contexts, infrastructures are inadequate to respond to all the needs of the citizens and residents of the country's various jurisdictions. In the South African case, this stems from both under-investment and lack of maintenance (Watermeyer & Phillips, 2020). The provision of verifiable legal identity deserves both public policy and financial support (Andreoni & Roberts, 2022). Citizen access to verifiable legal identity is fundamental to, inter alia, participation in the formal economy and maintenance of the rule of law, and should be a core DPI provision—with due attention to the risks of error and human-rights harms (Manby, 2021; Roberts & Mare, 2025; Silva et al., 2023). Concerns around panoptic surveillance, privacy violations, and the expansion of state monitoring capabilities must not be downplayed.

The mapping of digital national identity systems, as conducted in this study, has overlaps with, and implications for, questions of belonging, recognition, citizenship, and politics across the continent (Breckenridge, 2014a; Dalberto & Banégas, 2021; Manby, 2013). Of central importance for the continent are the questions related

to the processes and mechanisms of digitalisation that are raised here. What are the politics and incentives driving the adoption and continuation of one or another of the four types of identity systems set out in this article, and what is the true nature of the systems' relationships with national payments systems? More fundamentally, who, in reality, are the actors constructing and negotiating the power dynamics within African national identity systems as they go digital?

Acknowledgements
This work was carried out with the aid of a grant from the International Development Research Centre, Ottawa, Canada. A much earlier version of this research was presented at the WISH seminar at the Wits Institute for Social and Economic Research (WiSER), University of the Witwatersrand, Johannesburg, on 31 July 2023, under the title "Changing digital identity systems across Africa: A sociotechnical and political economy mapping of initiatives for digital public infrastructure". The assistance of seminar participants and colleagues across the University of the Witwatersrand, and especially the Trust Project at WiSER, is gratefully acknowledged.

Data availability
Data used to generate the findings set out in the submission is available at dpimap.org and https://osf.io/86xdw/overview.

AI declaration
The author did not use any AI tools in the research covered in this submission or in the preparation of this submission.

Competing interests declaration
The author has no competing interests to declare.

References

Africa News Agency. (2026, April 8). *Ghana: National ID becomes digital wallet, transforming payments.* https://africa-news-agency.com/ghana-national-id-becomes-digital-wallet-transforming-payments

African Union (AU). (2022). AU Interoperability Framework for Digital ID. https://au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf.

Alemu, G., Ferede, T., & Fiorito, A. (2021). *Identifying binding constraints on digital payment services in Ethiopia: An application of a decision tree framework*. Center for Global Development. https://elibrary.acbfpact.org/demo/collect/acbf/index/assoc/HASH3ff9/a452c815/5369b70b/31.dir/Ethiopia%20decision%20tree.pdf

Andreoni, A, & Roberts, S. (2022). Governing digital platform power for industrial development: Towards an entrepreneurial–regulatory state. *Cambridge Journal of Economics, 46(6), 1431–54.* https://doi.org/10.1093/cje/beac055

Ayano, M. F. (2018). Rural land registration in Ethiopia: Myths and realities. *Law & Society Review*, *52*(4), 1060–1097. https://doi.org/10.1111/lasr.12369

Banégas, R., & Cutolo, A. (2024). *ID wars in Côte d'Ivoire: A political ethnography of identification and citizenship (1st ed). Oxford University Press.* https://doi.org/10.1093/oso/9780192870476.001.0001

Beny, H. (2025). Digital-ID in Ethiopia: Country report. In G. Sesan & T. Roberts (Eds.), *Biometric digital-ID in Africa: Progress and challenges to date – Ten country case studies* (pp. 163–185). Institute of Development Studies. https://doi.org/10.19088/IDS.2025.051

Bhattacharya, A., Biggs, M., Bishop, M., Grown, C., Ingram, G., Kharas, H., McArthur, J. W., Mendelson, S. E., Nelson, J., Pipa, T., Sarabi, N., Taylor, J., Vora, P., & Winthrop, R. (2023). *The SDG second half: Ideas for doing things differently*. Brookings. https://www.brookings.edu/wp-content/uploads/2023/04/The-SDG-Second-Half_Final.pdf

Bloomberg. (2020, February 19). Safaricom likely to borrow to fund Ethiopia Telecom bid. *Daily Maverick*. https://www.dailymaverick.co.za/article/2020-02-19-safaricom-likely-to-borrow-to-fund-ethiopia-telecom-bid

Breckenridge, K. (2010). The world's first biometric money: Ghana e-zwich and the contemporary influence of South African biometrics. *Africa*, *80*(4), 642–662. https://doi.org/10.3366/afr.2010.0406

Breckenridge, K. (2014a). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. Cambridge University Press.

Breckenridge, K. (2014b). The book of life: The South African population register and the invention of racial descent, 1950–1980. *Kronos*, *40*(1), 225–240. http://www.jstor.org/stable/24341941

Breckenridge, K. (2019a). The failure of the 'single source of truth about Kenyans': The NDRS, collateral mysteries and the Safaricom monopoly. *African Studies*, *78*(1), 91–111. https://doi.org/10.1080/00020184.2018.1540515

Breckenridge, K. (2019b). The global ambitions of the biometric anti-bank: Net1, lockin and the technologies of African financialisation. *International Review of Applied Economics*, *33*(1), 93–118. https://doi.org/10.1080/02692171.2019.1523836

Burke, M. (2026, May 8). *The political economy of digital public infrastructure adoption in digital identity systems*. DIGI-GOV-South Africa. https://digigovsa.substack.com/p/the-political-economy-of-digital

Caribou Digital. (2019). *Kenya's identity ecosystem*. Commonwealth Digital ID Initiative. https://caribou.global/publications/kenyas-identity-ecosystem

Carruthers, B. G. (2020). Law, governance, and finance: Introduction to the Theory and Society special issue. *Theory and Society*, *49*(2), 151–164. https://doi.org/10.1007/s11186-020-09390-5

Center for Human Rights & Global Justice (CHRGJ). (2022). *Paving a digital road to hell? A primer on the role of the World Bank and global networks in promoting digital ID*. New York University. https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf

Dafe, F., & Upadhyaya, R. (2026). Digital empowerment: Banks and the rise of FinTechs in Kenya and Nigeria. *Competition & Change, 10245294261426516.* https://doi.org/10.1177/10245294261426516

Dahan, M., & Gelb, A. (2015, April 28). Reflections on the future of legal identity. Digital Transformation: World Bank blog. https://blogs.worldbank.org/en/digital-development/reflections-future-legal-identity

Dalberto, S. A., & Banégas, R. (Eds). (2021). *Identification and citizenship in Africa: Biometrics, the documentary state and bureaucratic writings of the self* (1st ed). Routledge. https://doi.org/10.4324/9781003053293

Dattani, K. (2020). "Governtrepreneurism" for good governance: The case of Aadhaar and the India Stack. *Area*, *52*(2), 411–419. https://doi.org/10.1111/area.12579

De Gruchy, T. (2018). 'Every Tom, Dick and Harry': Understanding the changing role of the South African immigration industry. In T. Lacroix & A. Desille (Eds.), *International migrations and local governance: A global perspective* (pp. 151–167). Springer International Publishing. https://doi.org/10.1007/978-3-319-65996-1_9

Debos, M. (2025). A postcolonial card cartel: How European companies sold biometric voting in Africa. *Development and Change*, *56*(3), 457–483. https://doi.org/10.1111/dech.70000

Debos, M., & Desgranges, G. (2023). L'invention d'un marché: Économie politique de la biométrie électorale en Afrique. *Critique Internationale*, *98*(1), 117–139. https://doi.org/10.3917/crii.098.0117

Debrah, E., Effah, J., & Owusu-Mensah, I. (2019). Does the use of a biometric system guarantee an acceptable election's outcome? Evidence from Ghana's 2012 election. *African Studies*, *78*(3), 347–369. https://doi.org/10.1080/00020184.2018.1519335

Department of Home Affairs (DHA). (2020). Draft Official Identity Management Policy: Public Consultation Version. *Government Gazette* No. 44048, 31 December. Government of South Africa. https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf

DHA. (2026). [Draft] Amendment of Identification Regulations, 1998. *Government Gazette* No. 54610, 4 May. Government of South Africa. https://www.dha.gov.za/images/gazettes/54610_4-5_HomeAffairs.pdf

Donovan, K., & Martin, A. (2017). *The rise of African SIM registration: The emerging dynamics of regulatory change*. SocArXiv. https://doi.org/10.31235/osf.io/qgfhd

Eaves, D., Coyle, D., Vasconcellos, B., & Deshmukh, S. (2025). *The economics of shared digital infrastructures: A framework for assessing societal value*. Institute for Innovation and Public Purpose (IIPP), University College London, and Bennett Institute for Public Policy. https://www.ucl.ac.uk/bartlett/sites/bartlett/files/2025-04/the_economics_of_shared_digital_infrastructures.pdf

Eaves, D., & Kedia, M. (2023). *Exploring different financing models for digital public infrastructure and why they matter*. Observer Research Foundation. https://www.orfonline.org/wp-content/uploads/2023/06/T20_PolicyBrief_TF2_213_FinancingModels-DPI.pdf

Eaves, D., Mazzucato, M., & Vasconcellos, B. (2024). *Digital public infrastructure and public value: What is 'public' about DPI?* Institute for Innovation and Public Purpose (IIPP), University College London. https://www.ucl.ac.uk/bartlett/sites/bartlett/files/2025-06/Digital_Public_Infrastructure_and_Public_Value.pdf

Eaves, D., Pope, R., & McGuire, B. (2019). Government as a platform: How policy makers should think about the foundations of digital public infrastructure. *Kennedy School Review*, *19*, 126–131. https://www.proquest.com/docview/2316725327/abstract/9AA0BC9657604890PQ/1

Eaves, D., & Rao, K. (2025). *Digital public infrastructure: A framework for conceptualisation and measurement*. Working Paper WP 2025-01. Institute for Innovation and Public Purpose (IIPP), University College London. https://www.ucl.ac.uk/bartlett/sites/bartlett/files/dpi_conceptualisation_and_measurement.pdf

Effah, J., & Owusu-Oware, E. (2021). From national to sector level biometric systems: The case of Ghana. *Information Technology for Development*, *27*(1), 91–110. https://doi.org/10.1080/02681102.2020.1818543

Gelb, A., & Clark, J. (2013). *Identification for development: The biometrics revolution*. SSRN Scholarly Paper No. 2226594. https://doi.org/10.2139/ssrn.2226594

Gelb, A., & Metz, A. D. (2018). *Identification revolution: Can digital ID be harnessed for development?* Brookings Institution Press and Centre for Global Development. https://www.jstor.org/stable/10.7864/j.ctt21c4t40

Gurumurthy, A., Chami, N., Sanjay, S., Lakra, R., & Vaidya, E. (2025). *Recovering the 'public' in India's digital public infrastructure strategy*. SSRN Scholarly Paper No. 5515958. https://doi.org/10.2139/ssrn.5515958

Hashmi, Z. (2021). *Identifying kin biometric belonging and databased governance in colonial South Asia and postcolonial Pakistan*. [PhD thesis, University of Michigan]. https://doi.org/10.7302/3875

Heslop, L. A. (2020). A journey through 'infraspace': The financial architecture of infrastructure. *Economy and Society*, *49*(3), 364–381. https://doi.org/10.1080/03085147.2020.1733843

Institute for Innovation and Public Purpose (IIPP). (n.d.). *The digital public infrastructure map (DPI map): Codebook*. University College London. Retrieved July 1, 2026, from https://dpimap.org/codebook

Kabata, V. (2024). An assessment of the legal and regulatory framework supporting the implementation of the National Integrated Identity Management System (NIIMS) in Kenya. *Data & Policy*, *6*, e7. https://doi.org/10.1017/dap.2023.36

Khan, M., & Roy, P. (2019). *Digital identities: A political settlements analysis of asymmetric power and information*. Anti-Corruption Evidence (ACE) Working Paper 15. https://ace.soas.ac.uk/wp-content/uploads/2022/05/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

Klaaren, J. (2017). *From prohibited immigrants to citizens: The origins of citizenship and nationality in South Africa*. UCT Press. https://doi.org/10.58331/UCTPRESS.35

Klaaren, J. (2023, July 31). Changing digital identity systems across Africa: A sociotechnical and political economy mapping of initiatives for digital public infrastructure. Paper presented at WISH seminar, Wits Institute for Social and Economic Research (WiSER), University of the Witwatersrand, Johannesburg. https://wiser.wits.ac.za/system/files/seminar/Klaaren2023.pdf

Le Roux, K. (2025, November 4). World Bank and Google activate partnership to reach 100 million with AI-driven public services. *Daily Maverick*. https://www.dailymaverick.co.za/article/2025-11-04-world-bank-and-google-activate-partnership-to-reach-100-million-with-ai-driven-public-services

Macdonald, A. (2023a, April 21). *Stakeholders examine benefits of digital public infrastructure at IMF meeting*. Biometric Update. https://www.biometricupdate.com/202304/stakeholders-examine-benefits-of-digital-public-infrastructure-at-imf-meeting

Macdonald, A. (2023b, December 14). *Ghana plans digital version of national ID card to simplify authentication.* Biometric Update. https://www.biometricupdate.com/202312/ghana-plans-digital-version-of-national-id-card-to-simplify-authentication

Macdonald, A. (2025a, March 4). *Ghana's banking industry emphasizes biometric verification for secure transactions.* Biometric Update. https://www.biometricupdate.com/202503/ghanas-banking-industry-emphasizes-biometric-verification-for-secure-transactions

Macdonald, A. (2025b, May 7). *Nigeria unveils platform to streamline national ID authentication, verification.* Biometric Update.https://www.biometricupdate.com/202505/nigeria-unveils-platform-to-streamline-national-id-authentication-verification

Manby, B. (2013). *Struggles for citizenship in Africa*. Zed Books. https://doi.org/10.47622/9781936133291

Manby, B. (2021). The Sustainable Development Goals and 'legal identity for all': 'First, do no harm'. *World Development*, *139*, 105343. https://doi.org/10.1016/j.worlddev.2020.105343

Mann, L. (2018). Left to other peoples' devices? A political economy perspective on the big data revolution in development. *Development and Change*, *49*(1), 3–36. https://doi.org/10.1111/dech.12347

Martin, A. (2019). Mobile money platform surveillance. *Surveillance & Society*, *17*(1/2), 213–222. https://doi.org/10.24908/ss.v17i1/2.12924

Martin, A. (2021). Aadhaar in a box? Legitimizing digital identity in times of crisis. *Surveillance & Society*, *19*(1), 104–108. https://doi.org/10.24908/ss.v19i1.14547

Maurer, B. (2012). Regulation as retrospective ethnography: Mobile money and the arts of cash. *Banking & Finance Law Review*, *27*(2), 299–313. https://www.proquest.com/docview/916627632/abstract/769BEDAE27D74CDAPQ/1

McCallum, W., & Aziakpono, M. J. (2023). Regulatory sandbox for FinTech regulation: Do the conditions for effective adoption exist in South Africa? *Development Southern Africa*, *40*(5), 1100–1116. https://doi.org/10.1080/0376835X.2023.2182759

Medaglia, R., Eaton, B., Hedman, J., & Whitley, E. A. (2022). Mechanisms of power inscription into IT governance: Lessons from two national digital identity systems. *Information Systems Journal*, *32*(2), 242–277. https://doi.org/10.1111/isj.12325

Milne, A. K. L., & Lawack, V. (2024). *Digital assets in payments and transaction banking*. South African Reserve Bank Working Paper Series WP/24/20. https://www.resbank.co.za/content/dam/sarb/publications/working-papers/2024/digital-assets-in-payments-and-transaction-banking.pdf

Monye, O., & de Koker, L. (2022). Strengthening financial integrity in Nigeria: The national identification harmonization project. *Journal of Financial Crime*, *29*(4), 1137–1154. https://doi.org/10.1108/JFC-05-2022-0104

Musoni, M., Domingo, E., & Ogah, E. (2023). *Digital ID systems in Africa: Challenges, risks and opportunities*. ECDPM. https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-in-Africa-ECDPM-Discussion-Paper-360-2023.pdf

Musoni, M., Pouyé, R., & Odhiambo, S. (2026). *Digital public infrastructure in the East African Community*. ECDPM Discussion Paper No. 404. https://ecdpm.org/application/files/5217/7685/8488/Digital-public-infrastructure-East-African-Community-ECDPM-Discussion-Paper-404-2026.pdf

Mutung'u, G. (2023). Checking the power of technology business in public roles through strategic litigation: Case examples from Kenya. *Javnost - The Public*, *30*(2), 236–252. https://doi.org/10.1080/13183222.2023.2201796

Mutung'u, G., Martin, A., & Brewczyńska, M. (2026). Regulatory entrepreneurship's threat to digital sovereignty: The case of Worldcoin in Kenya. *Science and Public Policy*, *53*(2), 289–299. https://doi.org/10.1093/scipol/scag010

Mutung'u, G., & Rutenberg, I. (2020). Digital ID and risk of statelessness. *Statelessness and Citizenship Review*, *2*(2), 348–354. https://doi.org/10.35715/SCR2002.1111

Mzinyati, L., & Cloete, D. (2025). *Digital public infrastructure futures: Charting inclusive and secure transformation in the SADC region. Policy Insights No. 171. South African Institute of International Affairs (SAIIA).* https://saiia.org.za/wp-content/uploads/2025/12/SAIIA_PI_171_DPI-FUTURES.pdf

MyMzansi. (2025). *South Africa's roadmap for the digital transformation of South African government*. https://www.gov.za/sites/default/files/gcis_document/202505/south-africas-roadmap-digital-transformation-government.pdf

National ID. (n.d.). *Authentication*. https://id.gov.et/authentication

National Identity Management Commission (NIMC). (2024, April 15). *The e-ID Card*. https://nimc.gov.ng/e-id-card

National Institute of Standards and Technology (NIST). (2023). *NIST SP 800-63 digital identity guidelines*. https://pages.nist.gov/800-63-4

Nkosi, M. (2025, July 12). *How Fayda digital ID powers Ethiopia's ambitious one-stop government service platform*. IT News Africa. https://www.itnewsafrica.com/2025/07/how-fayda-digital-id-powers-ethiopias-ambitious-one-stop-government-service-platform

Nyst, C., Pannifer, S., Whitley, E. A., & Makin, P. (2016). *Digital identity: Issue analysis*. Consult Hyperion. https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

Okunoye, B. (2022). Mistrust of government within authoritarian states hindering user acceptance and adoption of digital IDs in Africa: The Nigerian context. *Data & Policy*, *4*, e37. https://doi.org/10.1017/dap.2022.29

Okunoye, B. (2025). *Understanding digital public infrastructure (DPI) through Nigeria's NIBSS NIP real time payments layer*. Paper presented to TRUST seminar, Wits Institute for Social and Economic Research (WiSER), University of the Witwatersrand, Johannesburg. https://wiser.wits.ac.za/content/understanding-digital-public-infrastructure-dpi-through-nigerias-nibss-nip-real-time-0

Ombati, C. (2023, October 26). Digital ID regulations out as piloting set to start. *The Star*. https://www.the-star.co.ke/news/2023-10-26-digital-id-regulations-out-as-piloting-set-to-start

OpenID. (2023). *Draft report: Government-issued digital credentials and the privacy landscape*. https://openid.net/wordpress-content/uploads/2023/04/DRAFT-Government-issued-Digital-Credentials-and-the-Privacy-Landscape-publiccomment.pdf

Organisation for Economic Co-operation and Development (OECD). (2021). *Development co-operation report 2021: Shaping a just digital transformation*. https://doi.org/10.1787/ce08832f-en

Pistor, K. (2019). *The code of capital: How the law creates wealth and inequality*. Princeton University Press. https://doi.org/10.1515/9780691189437

Radier, T. (2023, July 20). *NBE to make digital ID primary for use by banks*. FSD Africa. https://fsdafrica.org/nbe-to-make-digital-id-primary-for-use-by-banks

Rao, K., Fetter, J., & Eaves, D. (2025). *2025 state of digital public infrastructure report: A look at measurement and prevalence as DPI transitions from experiment to scale*. Institute for Innovation and Public Purpose (IIPP), University College London. https://dpimap.org/iipp-state-of-dpi-report-2025.pdf

Ricks, M. (2018). Money as infrastructure. *Columbia Business Law Review*, *2018*(3), 757–851. https://heinonline.org/HOL/P?h=hein.journals/colb2018&i=775

Robb, G., & Vilakazi, T. (2016). Mobile payments markets in Kenya, Tanzania and Zimbabwe: A comparative study of competitive dynamics and outcomes. *The African Journal of Information and Communication (AJIC)*, *17*, 9–37. https://doi.org/10.23962/10539/21630

Roberts, T., & Mare, A. (Eds.) (2025). *Digital surveillance in Africa: Power, agency, and rights. Bloomsbury Academic.* https://doi.org/10.5040/9781350422117

Roitman, J. (2023). Platform economies: Beyond the North-South divide. *Finance and Society*, *9*(1), 1–13. https://doi.org/10.2218/finsoc.8089

Sandman, J., & Eaves, D. (2023, April 5). *What is digital public infrastructure?* UCL IIPP Blog. https://medium.com/iipp-blog/what-is-digital-public-infrastructure-6fbfa74f2f8c

Sang, D., Munga, J., & Sambuli, N. (2025). *Digital public infrastructure: A practical approach for Africa*. Carnegie Endowment for International Peace. https://assets.carnegieendowment.org/static/files/Munga%20et%20al_A%20Practical%20Approach%20for%20DPI%20in%20Africa-1.pdf

Sani, S. (2025). *Biometrics and digital identification systems in Africa: Assessment of governance, vendors, and human rights*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2025/11/Biometrics-and-digital-identity-in-Africa.pdf

Shaffer, G. (forthcoming). The transnational legal ordering of digital economies: Opportunities and constraints for a development focus. In G. Dimitropoulos & N. Mishra (Eds.), *Reorienting international economic law for the digital economy: From addressing the digital divide to enabling digital development?* Hart Publishing.

Silva, R., Breckenridge, K., Gruskin, S., & Klaaren, J. (2023). *Rights and ethics in biometric population registration: Mapping the limits of digital recognition and the drivers of exclusion*. https://doi.org/10.2139/ssrn.4647719

Sriraman, T. (2018). *In pursuit of proof: A history of identification documents in India*. Oxford University Press. https://doi.org/10.1093/oso/9780199463510.001.0001

Thiel, A. (2020). Biometric identification technologies and the Ghanaian 'data revolution'. *The Journal of Modern African Studies*, *58*(1), 115–136. https://doi.org/10.1017/S0022278X19000600

Thornberry, E. (2015). Keith Breckenridge. *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present* (book review). *International Feminist Journal of Politics*, *17*(3), 517–519. https://doi.org/10.1080/14616742.2015.1055142

Tyce, M. (2020). Beyond the neoliberal-statist divide on the drivers of innovation: A political settlements reading of Kenya's M-Pesa success story. *World Development*, *125*, 104621. https://doi.org/10.1016/j.worlddev.2019.104621

Upadhyaya, R., Weitzberg, K., & Bonyo, L. (2025). Digital credit providers, regulatory frameworks, and structural power: A case study of digital microcredit regulation in Kenya. *Finance and Society*, *11*(2), 1–23. https://doi.org/10.1017/fas.2025.4

Watermeyer, R, & Phillips, S. (2020). *Public infrastructure delivery and construction sector dynamism in the South African economy*. Final Report. National Planning Commission. https://www.nationalplanningcommission.org.za/assets/Documents/Public%20infrastructure%20delivery%20and%20construction%20sector%20dynamism%20in%20the%20South%20African%20economy.pdf

Weitzberg, K. (2015). The unaccountable census: Colonial enumeration and its implications for the Somali people of Kenya. *The Journal of African History*, *56*(3), 409–428. https://doi.org/10.1017/S002185371500033X

Weitzberg, K. (2020). Biometrics, race making, and white exceptionalism: The controversy over universal fingerprinting in Kenya. *The Journal of African History*, *61*(1), 23–43. https://doi.org/10.1017/S002185372000002X

Whitley, E. A., & Schoemaker, E. (2022). On the socio-political configurations of digital identity principles. *Data & Policy*, *4*, e38. https://doi.org/10.1017/dap.2022.30

World Bank. (2025, February 27). *The transformative power of Ethiopia's digital ID: Unlocking a better future for all*. https://www.worldbank.org/en/news/feature/2025/02/27/the-transformative-power-of-ethiopia-afe-digital-id-unlocking-a-better-future-for-all