

Digital public infrastructure across Africa: A national identity systems perspective

June 2026, Jonathan Klaaren (Jonathan.klaaren@wits.ac.za)

Abstract

A rising global politics advocates to digitalise national identity systems and link them with payment systems by investing in digital public infrastructure (DPI). The DPI paradigm combines three core elements: digital legal identity systems, national payment systems, and safe and secure data exchange. This study adopts the perspective of the national identity systems and legal identity literatures to assess DPI initiatives across Africa. Based on the three core functions of identity systems as well as their linkage to national payments systems, the study conceptualises four ideal types of national digital identity systems in African countries: identification-led, authentication-led, plural-identification, and payments-led. The study contributes to global DPI debates by emphasising the authentication function, by problematising the relationship between national identity and payment systems and by interrogating a proposed set of global DPI indicators. A qualitative survey of five leading African countries (Ethiopia, Ghana, Kenya, Nigeria, and South Africa), selected by means of this set of indicators, finds empirical support for the utility of the typology in investigating how identity systems are changing across Africa and how value can best be furthered in DPI investments.

Keywords

digital public infrastructure (DPI), legal identity, identity systems, identification systems, digital identity, biometrics, multi-modal authentication, digital verification

1. Introduction and literature review

The promotion of digital public infrastructure (DPI) has been mounting in recent years (Bhattacharya et al., 2023; Eaves et al., 2019; Macdonald, 2023a). Motivation for investment in DPI initiatives are having a particular impact—and draw a degree of their particular politics—from their intersection with national identity and payments systems under the care of African governments. In Africa, DPI initiatives often take the form of public or public-private initiatives to change existing public service delivery systems (Sani, 2025; Mzinyati & Cloete 2025; Sang et al. 2025; Musoni et al. 2026). The value claims of inclusion, security and effective service delivery associated with these DPI initiatives have met with pushback by civil society rights advocates and critical examination from human rights scholars, who have pushed for safeguards including greater data protection and privacy rights (CHRGJ, 2022; Gurusurthy et al., 2025; Manby, 2021; Silva et al., 2023). Drawing on the national identity systems and legal identity literatures, this paper develops a typology of identity systems with which to assess initiatives under the rubric of digital public infrastructure.

Motivations for investment in DPI often refer to a leading global example, the 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 program 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 as “an interesting model to consider for large-scale deployments” (OpenID, 2023, p. 13). Implemented through the modular open-source identity platform (MOSIP), Aadhaar's legitimacy increased during the Covid pandemic (Martin, 2021, p. 105). Aadhaar is the digital identity base for the digital public infrastructure termed India Stack. With biometric data stored in the cloud through Aadhaar, certain application programming interfaces (APIs) of India Stack enable a range of functions including enrolment and identity verification for government services. APIs also provide other forms of digital identity, such as a financial address, enabling the United Payments Interface (UPI), with which digital payment applications can interface, as well as provision of a consent layer allowing for exchange of personal data (Dattani, 2020).

The DPI paradigm is constituted by three interconnected elements at national level—an identity system including electronic verification/authentication, a payments system, and a set of ground rules for personal data exchange. 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 digital public infrastructure—without identity, neither payments nor data exchange would function.¹

The DPI concept has most often referred to the adoption and implementation of infrastructure at country level, due to the national scale of most digital identity systems (Heslop, 2020). With Aadhaar and India Stack in mind, 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 desired to perform) and the infrastructural constituent elements of the DPI, which must be constructed. The conceptual meaning of DPI is tightly bound up with its legitimacy and its justification. However, in many renderings of the concept, the meaning and the call for DPI is 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 was accelerated by the DPI focus of successive G20 agendas, promoted by the DPI-leading nations, namely India, Brazil and South Africa (Shaffer, 2026; le Roux, 2025). Further contributing to, as well as demonstrative of this coherence, a set of indicators allowing for global tracking of DPI has recently been released, namely the Global DPI Tracker (Rao et al., 2025).

The assemblage of various DPIs in African countries poses questions of public value (Eaves et al., 2024; Eaves & Kedia, 2023). Frequently the funding and building of DPI is 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 digital public infrastructure.

This study surveys the DPI paradigm from the perspective of the literatures of legal identity and national identity systems. It draws on these literatures to propose four ideal types of digital identity systems and discusses the logic of their operationalisation within a proposed set of global DPI tracking indicators. It applies this instrument to eleven selected African jurisdictions with DPI-ready national identity systems and uses a case study method to elaborate the four types of evolving African digital identity systems. It discusses the policy and public value implications of this four-part categorisation for investments in DPI across Africa.

2. The perspective of national digital identity systems and legal identity

An identity system encompasses the relevant technology, the rules and processes regarding identity, as well as their implementation and practice as a system. A national identity 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 identity systems, the legal rules are “a combination of existing public law” that includes identity-specific statutes, generally applicable privacy and data protection law, as well as 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 enrolment and identity proofing (identification), 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.

¹ The digital public infrastructure terminology is admittedly “somewhat amorphous”. In addition and as counterpoint to the payments-explicit definition employed here, see the UNDP 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 2026: 7)

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

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 identity system must include digital authentication, from the perspective of African identity systems with only partial digitalisation, this study regards digitalisation of any of the three functions of identification, authentication or authorisation as a digital identity system, albeit one with limitations.

A conceptual distinction widely acknowledged in the field of identity systems is that 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 license which provides proof of driving competence, though its secondary purpose may be to serve as legal identification.

Given its significance, we next explore the linkage of digital identity systems to the financial sector and specifically to the national payments system within that sector (Ricks, 2018). In the context of DPI, the linkage of digital identity to a digital payments system is channelled both through digital technologies such as payment platforms, as well as through supporting laws and legal institutions such as contract law, legal identity and financial sector regulation (Carruthers, 2020, p. 152; Pistor, 2019). 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 in relation to transactions involving payments.

3. Categorising national digital identity systems based on system functions and systems linkages

The relationship among the core functions of identity systems and the relative prominence of these functions is central to understanding DPI. Secondly, the linkage between national identity systems and other systems is necessary to understanding DPI linkages between identity systems and national payment systems. This discussion leads to constructing a hypothesised typology of national identity systems.

The primary function of an identity system is identification (also known as enrolment or identity proofing), and the secondary function is authentication. Prior to adoption of digital systems, identification came sequentially and prominently before authentication. A person is first issued with an identity document upon presentation of breeder documents and capture of biometric data at the primary issuing department. Then the person may 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 acquisition and possession of the identity document is more prominent than authentication or authorisation.

With digital applications, the relative prominence of one or the other of these functions is no longer clear. The two are now often tightly coupled as the same organisational entity may now be responsible for both enrolment and authentication and may use many of the same processes or personnel for both actions. The Aadhaar system in India is responsible for both the enrolment of residents of India and the subsequent authentication of their identity. While the responsibility for these two functions also currently lies with the Department of Home Affairs in South Africa, the degree of interdependence between these two functions is much greater with Aadhaar, in part because the statutory entity implementing Aadhaar. The Unique Identification Authority of India (UIDAI) is an entity designed to either fulfil or oversee fulfilment of these two functions.

As the Aadhaar case shows, while it has impacted the enrolment function, digitisation has revolutionised authentication, both in form and in speed, such that it is no longer a decentralised operation at a government service desk but is often mediated through a nationally centralised website or other electronic channel.³

³ Examples of this impact on the authentication function are visible in South Africa. The initial identification of a person may now be dependent on the successful authentication of the enrollee's parent, as in numerous instances of the South African blocked IDs public interest litigation. (P.P.M and Others v Minister of Home Affairs and Others (14238/21) [2024] ZAGPPHC 2 (16 January 2024)) <https://www.saflii.org/za/cases/ZAGPPHC/2024/2.html>. Thousands of South African permanent resident permit holders should be able to have their identity and immigration status authenticated by the Department of Home Affairs (DHA) but instead

Furthermore, this authentication happens instantaneously, signalling heightened efficiency, or system failure when internet access is disrupted or interoperability is disrupted.

It is therefore possible to identify two ideal types of national identity systems with respect to the significant variable of the sequencing and systemic coupling of identification and authentication. We can characterise the first type as “identification-led” as it demonstrates clear sequencing and prominence of the identification function with relatively loose coupling of the identification and the authentication functions. We can characterise the second type as “authentication-led” as it demonstrates 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 the identity system indicates a degree of power within the system (Medaglia et al., 2022). One indicator of the relative power of the identification or authentication function would be the relative power within the governance framework of the legal rules (identification-led) or the technical and operational specifications for the system (authentication-led). 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 national identity system, those with a plurality of identification schemes without prominent implementation of either the identification or authentication functions. Sector-specific ID systems 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. In these non-dominant identity systems, multiple schemes of functional and foundational identification are provided and authenticated. Identity systems which are characterised by a plurality of functional identities without the dominance associated with foundational identity systems may be characterised as plural national identity systems.

National identity systems across Africa 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 and the data exchange layers. Credible and trusted identification is crucial for authorisation of transactions within a payments system. In most countries, only persons above a legally defined age or with a legally defined immigration status can hold a bank account or have a SIM-card registration. 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. A national identity system that is significantly influenced or driven by a national payments system, and by actors and dynamics within that system, may be characterised as a payments-led national identity system.

With the three core functions of identity systems in mind, we can construct a four-part typology of identity systems to use in assessing DPI approaches in African countries. An *identification-led national identity system* has a dominant foundational identity 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 and 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 identification schemes at least one of which is digitally authenticated and is driven or significantly influenced by its linkage with the national payments system.

4. Selecting significant national identity systems across Africa for review

Contemporary calls for the investment in and building of digital public infrastructure draw a degree of their particular politics from their intersection with national payments and identity systems under the care of African governments (discussed further below). In order to begin to take stock of the relative power of these calls, the mapping of digital public infrastructure across Africa has become an urgent and worthwhile effort (Klaaren,

have been directed by the DHA to authenticate the Department’s own issued identification documents with the outsourced digital service, VFS (De Gruchy 2018).

2023). This section identifies the African digital identity schemes that are significant in the DPI context using data recently collected for the Global DPI Tracker project.⁴ The Tracker is part of the DPI Mapping initiative at the University College London Institute for Innovation and Public Purpose (UCL IIPP), found at dpimap.org. The project should be understood as a guideline or analytical tracker for assessing certain DPI-related features, rather than as a definitive authority on DPI status. The compilers of this dataset have done one or two initial probes of its data with an African lens, encouraging further work with and supplementation of their existing data.

In order to collect the base data for this review exercise, the African jurisdictions of the Global DPI Tracker were selected as the primary database. The Global DPI Tracker defines a digital identity 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 DPI Map focuses on national or federal-level ID systems that are governed by public institutions” (DPI Map, n.d.). Of the 52 African jurisdictions in this database, five African jurisdictions are recorded as having digital identity systems, namely Algeria, Ethiopia, Ghana, Seychelles, and Uganda. At first glance, it is surprising that South Africa is not on this list since it has an identification numbering and card system that provides digital authentication for banks and other public and private sector institutions. The reason for its exclusion is that it only scores positively on three of the four required indicators. The four indicators are a digital identity documentation system, a digital authentication system, at least a planned or pilot digital ID, and two implementation use cases. For the fourth element of a digital ID system South Africa is recorded as “no”.

With two indicators used as filters, the data of the Global DPI Tracker can plausibly get us to identifying the set of African identity systems that are significant. The first indicator is identification authentication systems, labelled by the Tracker as digital authentication systems (second on the list of four above). The key aspect of this indicator for our purposes is that these systems operate as part of the national identity system. The list of “authentication methods” that satisfy this indicator in the DPI Tracker are appropriately diverse: “demographic details, biometric data (fingerprints/iris), facial recognition, OTP (one-time password via mobile or email)”. The second indicator to be used is the existence of a real-time payment system. Combined with the first indicator, the existence of a real-time national payments system is both a sign of the significance of the identity system and an integral part of the prospective digital public infrastructure that is the animating vision for these politics, debates, and investments.⁵

Application of these two indicators as filters leads to a set of 11 African jurisdictions from the DPI Tracker, presenting with a combination of digital identity systems and real-time payment systems. As may be expected, five of the leading national identity systems that are discussed in literature are present: Ethiopia, Ghana, Kenya, Nigeria, and South Africa.⁶ The Global DPI Tracker-derived list of significant African national identity systems has the six additional jurisdictions of Egypt, Mauritius, Morocco, Seychelles, Uganda and Zambia.

5. Categorising African identity systems

Deploying and elaborating upon the four-part typology, this section provides short overviews of a selection of the 11 digital identity systems identified above. In addition to outlining the power dynamics within these systems, this includes a partial testing of the utility of the four categorisations proposed in Part Four. The South African and Zambian systems are characterised as identification-led national identity systems. Ethiopia and Morocco may be characterised as authentication-led systems and Ghana is characterised as a plural identity system. Kenya and Nigeria are examples of payments-led systems. Yet to be classified but regarded as significant by our application of the Global DPI Tracker indicators are Egypt and the two island nations, Mauritius and The Seychelles. The following overviews consider the key digital identity features, using at

⁴ The full method details and the compiled dataset are available at [anonymised/redacted].

⁵ There appears to be no indicator in the Global DPI Tracker that speaks directly to the linkage between the digital identity layer and the digital payments layer.

⁶ It is interesting that some jurisdictions – such as Rwanda – do not figure on this list. Rwanda apparently has no identification authentication system, though it does have a real-time national payment system.

least one case study for each of these four categories, supplementing them with insight into the power dynamics of their identity systems.

South Africa: An identification-led system

South Africa has identification coupled with a working electronic authentication function as well as a digital national payments system, thus qualifying as a significant African digital identity system. Indeed, it is a leading identity system in the world, particularly for its use (and, under apartheid, abuse) of biometric technology (Breckenridge, 2014a). Albeit with a degree of inefficiency and corruption, the Department of Home Affairs 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, banking account verification, credit checks and social grant distribution. National payments are facilitated through two electronic systems: an interbank system with real-time clearing, PayInc (formerly BankServAfrica) 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, Home Affairs called for comment on a set of draft digital identification regulations, which included provisions tentatively linking the DHA digital identity with the MyMzansi platform, aiming to facilitate citizens' access to public services (Department of Home Affairs, 2026).

The power dynamics in the implementation of the identity system, and between it and the payments system, warrants South Africa's classification as an identification-led digital identity system. First, neither the banks nor the telecommunications firms have broken the hegemony of the Department of Home Affairs (DHA) on identity management (Department of Home Affairs, 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 Department of Home Affairs (De Gruchy, 2018). Second, 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 rooted firmly within the legal foundation of the identity system, the Identification Act 68 of 1997 (section 21). The DHA shares information from the population register with insurance businesses and banking institutions.⁷

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 the developments in 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 function⁸. Thirdly, the national payments system does not drive the identity system but is integrated with it under fairly close state supervision. Breckenridge has detailed the origins and rise of a maverick firm 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). The "Functional Digital Identity for People to Securely and Remotely Access Services" is planned within the South African Reserve Bank (SARB) regulation of the payments system and integrated with the identity system as part of South Africa's Digital Transformation Roadmap (Mymzansi, 2025, p. 4).

Ethiopia: An authentication-led identity system

Ethiopia has a national identification scheme coupled with a working electronic authentication function and linked to a digital national payments system, thus qualifying as a significant African digital identity 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

⁷ Identification Act 68 of 1997, Pub. L. No. 68 of 1997, Act 68 of 1997, § 21, accessed March 20, 2019, https://www.gov.za/sites/default/files/gcis_document/201409/a68-97.pdf.

⁸ *Department of Home Affairs & BMA 2024/25 Annual Reports; DHA ICT rollout of self-service kiosks; One-Stop Border Post Bill; with Minister | PMG*, accessed October 15, 2025, https://pmg.org.za/committee-meeting/41734/?utm_campaign=minute-alert&utm_medium=email&utm_source=transactional.

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 Program, n.d.). Utilising the 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 payment systems (Radier, 2023).

Ethiopia is one of several African countries that have begun or are on the cusp of substantial long-term investment in digital systems to fulfil authentication and identification functions. The leading global technology in this category is the Modular Open-Source Identification Platform (MOSIP) associated with Aadhaar. In the OECD definitional distinction between digital public goods and digital public infrastructure, MOSIP is a prime example of a digital public good (OECD, 2021). Developed, supported, governed and promoted by India, MOSIP has been marketed, in the wake of Aadhaar, as a developmental digital platform for running a national identity system and further justified as avoiding vendor lock-in. In Africa, technologies associated with the Pakistani digital identity system, compete (and in some instances inter-operate) with MOSIP. NADRA Technologies Limited (NTL) is the commercial, for-profit arm of the Pakistani identification agency that develops and exports Pakistani digital ID technologies (*Pakistan Today*, 2023). Fayda is based upon MOSIP technology. 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).

An examination of the power dynamics in the implementation of its identity system and between it and the payments system shows that Ethiopia should be classified as an authentication-led digital identity system. In Ethiopia's case, 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 backed by national authorities and international donors from 2021 (Beny 2025, p. 166). The adoption was motivated in part by what was seen as Ethiopia's lagging position in the uptake of digital payment services (Alemu et al. 2021). In contrast with South Africa, the digital technology of the authentication function is more than crucial to the implementation of the system, it has been part of the design and drives the system's rollout. For instance, by 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. The function of real-time verification is endorsed by the national banks as part of the National ID Programme (Radier, 2023).

Ghana: A plural identity system

Ghana has a national identification scheme coupled with a working electronic authentication function and linked to a digital national payments system, thus qualifying as a significant African digital identity 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 license, 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 the past several years, the official Identity Verification System Platform (IVSP) has begun to authenticate holders of the Ghana card. The e-zwich card, a biometrically regulated smartcard which operates through the national payment system, arose out of the failure of a national identity card programme initiated through and driven by the National Identification Authority from 2001 (Breckenridge, 2010). A digital wallet (payment) functionality was announced to be integrated with the Ghana Card from April 2026 (Africa News Agency, 2026).

Turning to the power dynamics in the implementation of its identity system as well as between it and the payments system, Ghana may best be seen as a plural identity system, without dominance of 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 agency, the IVSP, across the country (Macdonald, 2023b). Biometric authentication of the holder of a Ghana Card is promoted by the banking and payment systems, though the payment system does not supplant or dominate the national identity system (Macdonald, 2025a). The biometric payment card, the e-zwich, 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 identity system

Kenya is in the process of rolling out national identification coupled with a working electronic authentication function and linked to a digital national payments system, thus qualifying as a significant African digital identity system. The current official system of identity numbers is the Maisha Namba, launched in October 2023 alongside amendments to the civil registration 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 identity system is provided by the National Integrated Identity Management System (NIIMS), Kenya's initial public sector large technology project (Caribou Digital, 2019, p. 30; Mutung'u & Rutenberg, 2020). Kenya's payments system has been dominated by the telecommunications firm Safaricom's mobile money platform, M-PESA since the 2010s. While it does not have anything like the size and power of Google and Facebook, Safaricom is an emerging markets-origin, multi-national enterprise, home-grown in Kenya (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, shows that Kenya is best characterised as a payments-led digital identity system. Indeed, Kenya is the globally paradigmatic case of a dominant firm in the telecommunications sector providing a form of 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). Creating a globally distinctive system of mobile money in the 2010s, Safaricom triumphed over the Kenyan banks in a contest for dominance over the national fast payments system particularly through contesting and winning the legal and institutional arrangements for credit information sharing (Breckenridge, 2019a; Dafe & Upadhyaya 2026). In view of Safaricom's dominance and the state's difficulties in implementing Huduma Namba, there is only a minimal degree of the foundational identity function and regulation with respect to the use case of identity in the payments system (Upadhyaya et al., 2025). The state's identity authentication service, NIIMS, does nonetheless operate as Maisha Namba is being established. In Kenya, in distinction to Nigeria, the issuance, authentication and use of identity within the national payment system is firmly in private hands rather than in those of a state agency and is not tightly linked to the foundational identity.

Nigeria: A payments-led identity system

Nigeria has a national identification scheme coupled with a working electronic authentication function and linked to a digital national payments system, thus qualifying as a significant African digital identity system. Under way from 2007, by July 2021, Nigeria's National Identity Management Commission (NIMC) had enrolled 60 million persons in the foundational identity scheme (Okunoye, 2022, pp. e37-2). By March 2025, 118 million persons had identity numbers. The project operates with a National Identity Number (NIN) format but aims to link to other identity schemes rather than provide 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 population associated with voter registration (84 million) and the subscriber identifier module (SIM) registration (190 million) (Okunoye, 2022, pp. e37-9). 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, pp. e37-4, 6). A fast payment system, the Nigerian Interbank Settlement Scheme (NIBSS) Instant Payment (NIP) was introduced in 2011 through the efforts of the Central Bank of Nigeria (Okunoye, 2025, p. 3). The authentication system is an approved app that individual NIN holders can download from Google Play and App Store (Macdonald, 2025b).

Similar to Kenya, though not demonstrating the dominant power of a single private sector payments firm, the power dynamics in the implementation of the system and between it and the payments system shows that the Nigerian digital identity system is payments-led. The driving force for the increasing degree of linkage and interoperability within and across these two systems is the payment functionality. In the 2010s, this could 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 payment 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 National Identity Management Commission (NIMC) since 2024. According to the NIMC, this card will have “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 Digital Identity Systems and DPI Development

The above study of digital identity systems and DPI development in Africa stands to be complemented with an explanatory account as to why countries have developed along the different trajectories and to the different end states identified. Questions of interests, incentives, power, and governance should be central to understanding DPI (Shaffer 2026). Who are the principal actors promoting particular configurations of identity and payment systems? What 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 such account is beyond the scope of this article,⁹ this section begins to analyse the sources of variation among the four identified types using the African cases explicated in order to identify and sketch some of 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 the investment in and building of digital public infrastructure often take social form as public or public-private initiatives to change (modernize) existing African public identity systems and they. From around 2005, mobile money intellectuals began to draw on Kenya’s experience with Safaricom (an emerging markets large telecommunications firm) and M-PESA (a mobile payments system) to promote the potential for financial and payment systems working 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, this view later aligned with influential figures within the development sector who came to the position that the digital and biometric identification revolution embodied in India’s Aadhaar system could be of significant impact for sustainable development within the jurisdictions of Africa (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 2026), including 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 ID systems, with a particular focus on mutual recognition among states in order to foster intra-African trade, e.g. towards a “An Integrated, Prosperous and Peaceful Africa” (African Union 2022). As Burke 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...”

⁹ Such an account should embark upon a comparative study beyond South Africa. In doing so, it might well parallel Keith Breckenridge’s *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present* (2014a). For work along similar lines exploring the modern history of the state and its identification systems and politics, see in Kenya Weitzberg 2015 and 2020 and in Ivory Coast, Banégas, R, & Cutolo, A. (2024) as well as in India Sriraman 2018 and in Pakistan Hashmi 2021. 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. Weitzberg 2015: 411, 413, 425-426; Thornberry 2015.

(2026). As for the technology vendors, pointing to the dominance of European companies which sell biometric identification technology to African states with a particular focus on French companies in the former French Empire, Debos (2025) argues that African states have become increasingly dependent on corporate actors for both election management and citizen identification.

Given that much of the significant action of these actors within this legal order takes place at the national level, how then does one explain the emergence of one type of national identity system? A few factors that 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 Department of Home Affairs. In the South African case, the retention of this power appears to be linked to the continuing Home Affairs power over the civil registration function, also housed in that Department. Where such state power is not existent, a further factor explaining variation is the relative power of the telecommunications and banking industries. In particular, the Kenyan telecommunications sector is relatively more powerful than the one in Nigeria, with the banking sector the more powerful at least with respect to civil identification in South Africa. In the trio of Nigeria, Kenya, and South Africa, these factors may be taken to explain the variation between an identification-led African digital identity system and a payments-led one. Ghana represents a case where neither the state nor a private sector industry appears able to achieve dominance in this environment. Explaining the variation thus allows then the focus to shift to Ethiopia where an authentication-led digital identity system is emerging. With the citizen identification function historically and still firmly under state control, the local and paper-based character of the existing Kebele civil registration system has allowed for and contributed to the verification function, with its promise of digitally linking different domains, to emerge as characteristic of the Fayda system.

7. Conclusion

This study has made three contributions to the debates around digital national identity systems and DPI in Africa, with possible broader relevance. 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 foundational and functional ID distinction. Deepening the study of DPI, it has also problematised the relationship between a national identity system and a national payments system, arguing that the nature of this relationship is a crucial feature of the implementation of both these systems. It has critically applied a global set of DPI indicators to a set of African digital identity systems that are likely to continue to generate global dynamics within their fields of finance, information systems, and politics.

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 from the above that there can be no one-size-fits-all approach to investigating the policy question being posed with urgency in national jurisdictions across Africa, namely whether and how to use public resources to build digital public infrastructure (Eaves et al., 2024, 2025). Other significant regulatory and policy implications, such as the importance of pursuing privacy rights and data protection principles in an integrated fashion across the digital identity and the financial payments sectors or the fit of particular regulatory strategies to the problematics of digital identity systems, also remain to be explored (McCallum & Aziakpono, 2023).

Of particular urgency is the question of public value. The mapping undertaken in this article assists in evaluating the costs and benefits of investments in digital public infrastructure. This is a key question faced by jurisdictions across Africa: whether and if so how to use public resources to build a digital public infrastructure. 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). The DPI mapping constructed above, on the whole, encourages investment in public infrastructure. Infrastructures across Africa are inadequate to respond to the needs of the citizens and residents of various jurisdictions. As the South African example demonstrates, this stems from underinvestment as well as from lack of maintenance (Watermeyer & Phillips 2020). The provision of verifiable legal identity deserves public policy and financial support (Andreoni & Roberts, 2022). It is an attribute that is key, simultaneously, to the formal economy and

to the rule of law, and should be provided within identity systems design, with due attention to the risks of error and human rights harms (Roberts & Mare, 2025, Silva et al., 2023, Manby, 2021). There are concerns around panoptic surveillance, privacy, and the expansion of state monitoring capabilities that are directly relevant to the African cases discussed above.

The mapping of national identity systems explored here has overlaps with and implications for questions of belonging, recognition, citizenship and politics across the continent (Breckenridge, 2014a; Dalberto & Banegas, 2021; Manby, 2013). Of importance for the continent are questions about the processes and mechanisms of global digitalisation that are raised here. What are the politics and incentives driving the adoption and continuation of one or another of these types of identity systems, as well as their relationship with national payment systems? What is the terminology and who are the parties constructing and negotiating the power dynamics within the national identity systems as they go digital?

References

- Agency, Africa News. (2026). “Ghana: National ID Becomes Digital Wallet, Transforming Payments.” *Africa News Agency*, April 8, 2026. <https://africa-news-agency.com/ghana-national-id-becomes-digital-wallet-transforming-payments/>.
- 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>.
- 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, Oxford. <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*. Institute of Development Studies and partners. <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*. 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, Mark. (2026). The Political Economy of Digital Public Infrastructure Adoption in Digital Identity Systems. Substack newsletter. *DIGI-GOV-South Africa*, May 8, 2026. <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, and R 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*. Information and Communications for Development blog. <http://blogs.worldbank.org/ic4d/reflections-future-legal-identity>
- Dalberto, S. A., & Banegas, 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). “Goventrepreneurism” 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): 457–83. <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. (2020). *Draft official identity management policy*. https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf
- Department of Home Affairs (South Africa). (2026). “Draft Amendment to Identification Act Regulations (4 May 2026).” Accessed May 5, 2026. https://www.dha.gov.za/images/gazettes/54610_4-5_HomeAffairs.pdf.
- Digital Public Infrastructure Map (DPI Map). (n.d.). *Codebook*. <https://dpimap.org/codebook>
- 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*. 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?* https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/iipp_wp_2024-05.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*. 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.
- 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, Zehra. (2021). "Identifying Kin Biometric Belonging and Databased Governance in Colonial South Asia and Postcolonial Pakistan." 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>
- 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 to WISH seminar, WiSER, Wits University. <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 (SARB). <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, Melody, Raphael Pouyé, and Steve Odhiambo. (2026). *Digital Public Infrastructure in the East African Community*. <https://ecdpm.org/application/files/5217/7685/8488/Digital-public-infrastructure-East-African-Community-ECDPM-Discussion-Paper-404-2026.pdf>
- Mutung'u, Grace, Aaron Martin, and Magdalena Brewczyńska. (2026). "Regulatory Entrepreneurship's Threat to Digital Sovereignty: The Case of Worldcoin in Kenya." *Science and Public Policy* 53, no. 2: 289–99. <https://doi.org/10.1093/scipol/scag010>
- 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., & 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, Litha, and Deon Cloete. (2025). *Digital Public Infrastructure Futures: Charting Inclusive and Secure Transformation in the SADC Region*. Policy Insights No. 171. SAIIA. https://saiaa.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.stateofthenation.gov.za/assets/downloads/South_Africa_Roadmap_for_the_Digital_Transformation.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.itnewsafrika.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 for Omidyar Network. http://www.chyp.com/wp-content/uploads/2016/07/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*. <https://wiser.wits.ac.za/system/files/seminar/Okunoye2025.pdf>
- 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>
- Pakistan Today*. (2023, September 17). Somalia launches national ID system with Pakistan's help, a milestone ID4Africa. <https://www.pakistantoday.com.pk/2023/09/17/somalia-launches-national-id-system-with-pakistans-help-a-milestone-id4africa>
- 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*. <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*. <https://doi.org/10.23962/10539/21630>
- Roberts, T, and Mare, A, eds. (2025). *Digital Surveillance in Africa: Power, Agency, and Rights*. Bloomsbury Academic, 2025. <https://doi.org/10.5040/9781350422117>.

- Roitman, J. (2023). Platform economies: Beyond the North-South divide. *Finance and Society*, 9(1), 1. <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, Diana, Jane Munga, and Nanjira Sambuli. (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, Gregory. *The Transnational Legal Ordering of Digital Economies: Opportunities and Constraints for a Development Focus*. Edited by Georgios Dimitropoulos and Neha Mishra. 2026 (forthcoming).
- Silva, R., Breckenridge, K., Gruskin, S., & Klaaren, J. (2023, October 9). *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, Tarangini. *In Pursuit of Proof: A History of Identification Documents in India*. Oxford University Press, 2018.
- 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, Elizabeth. (2015). Keith Breckenridge. Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present. *International Feminist Journal of Politics* 17(3): 517–19. <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*, 1–23. <https://doi.org/10.1017/fas.2025.4>
- Weitzberg, Keren. (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>.
- Weitzberg, Keren. (2015). The Unaccountable Census: Colonial Enumeration and Its Implications for the Somali People of Kenya. *The Journal of African History* 56(3): 409–28. <https://doi.org/10.1017/S002185371500033X>.
- Whitley, E. A., & Schoemaker, E. (2022). On the socio-political configurations of digital identity principles. *Data & Policy*. <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>

