DISCUSSION PAPER No. 404

Digital public infrastructure in the East African Community

By Melody Musoni, Raphael Pouyé and Steve Odhiambo

April 2026

Digital public infrastructure (DPI) refers to digital rails on which modern services run, linking systems for identity, payments and data exchange to enable secure, interoperable and large-scale service delivery. In the East African Community (EAC), DPI is increasingly seen not only as a tool for national digital transformation, but also as a practical pathway for advancing regional and continental integration.

This study assesses the state of DPI across the EAC, identifying key strengths, gaps and opportunities for both the bloc and its partner states. Findings show that the EAC adopts a broader 'DPI+' approach, which goes beyond the three conventional pillars, to include connectivity, digital skills and governance as foundational enablers. This reflects the realities of the region, where uneven infrastructure, institutional capacity and regulatory readiness continue to shape what can be implemented in practice.

Furthermore, the EAC has shown political commitment through frameworks such as the Cross-Border Digital Payments Masterplan and the Data Governance Framework, but progress remains uneven. While some countries are advancing across several DPI pillars, others are following more payments-led pathways. The report presents cross-border use cases of DPI as areas where the regional value of DPI becomes visible and points in particular to digital payments, trade and logistics, qualifications recognition and health as sectors where interoperable systems could make regional integration more tangible. The next phase will depend on stronger regional coordination, interoperable policy frameworks, investment in shared infrastructure and skills, and greater attention to data protection, cybersecurity, inclusion and accountability.

Table of contents

List of boxes

List of figures

List of tables

Acknowledgements

The authors would like to thank Sabine Muscat, Chloe Teevan, Sara Gianesello and Sasha Pearson for their research and contributions to this paper and Sabine Muscat for her peer review and constructive feedback on earlier drafts of this research. We are also grateful to GIZ EAC and the EAC Secretariat, as well as EAC Partner States, for their support on this research project. Additionally, we extend our appreciation to all the interviewees who took the time to participate and share their valuable insights.

The views expressed in this paper are those of the authors and do not represent those of ECDPM or any other institution. Any errors or omissions remain the responsibility of the authors. For comments and feedback, please contact mmu@ecdpm.org or cte@ecdpm.org.

Acronyms

AfCFTA	African Continental Free Trade Area
AU	African Union
B-Switch	Burundi National Payment Switch
CBDC	Central Bank Digital Currency
CDC	Centers for Disease Control and Prevention
CERT	Computer Emergency Response Team
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CRVS	Civil Registration and Vital Statistics
CSO	Civil Society Organisation

DHIS2	District Health Information Software, version 2
DIAL	Digital Impact Alliance
DITE	Digital Identity, Digital Trade and Digital Economy (UNECA initiative)
DP	Development Partner
DPA	Data Protection Authority
DPGA	Digital Public Goods Alliance
DPI	Digital Public Infrastructure
DRC	Democratic Republic of the Congo
DSM	Digital Single Market
EAC	East African Community
EAIDSNet	East African Integrated Disease Surveillance Network
EAPS	East African Payments System
EARDIP	East Africa Regional Digital Integration Project
EAHRC	East African Health Research Commission
ECOWAS	Economic Community of West African States
EEAS	European External Action Service
EMRO	Eastern Mediterranean Regional Office (WHO)
ENBIC	ECOWAS National Biometric Identity Card
EU	European Union
FCDO	Foreign, Commonwealth and Development Office (UK)
G20	Group of Twenty
GAVI	Global Alliance for Vaccines and Immunization
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
GMPC	General Multipurpose National Identity Card (Nigeria)
GovStack	Government Stack (public digital service architecture framework)
GSMA	Global System for Mobile Communications Association

HIE	Health Information Exchange
HISP	Health Information Systems Programme
HIV/AIDS	Human Immunodeficiency Virus / Acquired Immunodeficiency Syndrome
ICT	Information and Communication Technology
ID	Identity / Identification
ID4D	Identification for Development (World Bank initiative)
IDSR	Integrated Disease Surveillance and Response
ISO	International Organization for Standardization
KHRC	Kenya Human Rights Commission
LMICs	Low- and Middle-Income Countries
MOU	Memorandum of Understanding
MOSIP	Modular Open Source Identity Platform
MRPQ	Mutual Recognition of Professional Qualifications
NDI	National Digital Identity
NGO	Non-Governmental Organisation
NIMC	National Identity Management Commission (Nigeria)
NITA	National Information Technology Authority
NMB	National Microfinance Bank
PAERA	Public Administration Ecosystem Reference Architecture
PAPSS	Pan-African Payment and Settlement System
PKI	Public Key Infrastructure
PPP	Public-Private Partnership
QR	Quick Response (code)
REC	Regional Economic Community
RHEA	Rwanda Health Enterprise Architecture

R-Switch	Rwanda National Payment Switch
SATA	Smart Africa Trust Alliance
SDG	Sustainable Development Goal
SIPS	Somalia Interbank Payment System
SME	Small and Medium Enterprise
SSA	Sub-Saharan Africa
TIPS	Tanzania Instant Payment System
TLIP	Trade Logistics Information Pipeline
UEMOA	West African Economic and Monetary Union
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Programme
UNECA	United Nations Economic Commission for Africa
UNICEF	United Nations International Children's Emergency Fund
USA	United States of America
USPC	Uganda Security Printing Company
WARDIP	West Africa Regional Digital Integration Project
WB	World Bank
WHO	World Health Organization
W3C	World Wide Web Consortium
WURI	West Africa Unique Identification for Regional Integration and Inclusion
X-Road	Data Exchange Layer developed in Estonia

Executive Summary

Digital Public Infrastructure (DPI) is a **practical tool for supporting economic integration** within the East African Community (EAC). DPI can also serve the goal of continental integration under the African Continental Free Trade Area Agreement (AfCFTA) and the AfCFTA Digital Trade Protocol. An EAC approach looks beyond the globally leading framing of DPI as consisting of the pillars digital identity, digital payments and data exchange. It incorporates **infrastructure connectivity as a foundational layer** together with other enablers like **digital literacy and skills** (the "**DPI+ approach**"). These elements are critical for inclusive access to e-government services. The EAC has **demonstrated strong political commitment** to regional DPI through policy frameworks, such as the EAC Cross-Border Digital Payments Masterplan and the EAC Data Governance Framework, as well as through regional DPI use cases. EAC Partner States also view DPI as a vehicle for **building local capacity with the support of various partners** (international partners, donors and the private sector).

While the EAC has high-profile DPI experts, **regional coordination on DPI remains weak**. **DPI development in Partner States follows different paths**. Burundi, DRC, Somalia and South Sudan, are taking a payments-led approach in which mobile money precedes digital ID and government platforms. Kenya, Uganda, Rwanda, and Tanzania have set up several DPI pillars in parallel. These starting points influence adoption speed, stakeholder engagement and interoperability. **Digital payments are the most mature and dynamic** DPI pillar in the EAC, followed by cross-border data exchange, while cross-border digital ID uses are still largely in exploratory stages. The region still **needs to improve on data protection and cybersecurity** to build consumer trust and protect basic rights. Progress on this front would also heighten trust in the region and drive further demand for DPI.

Summary of main recommendations

1. **Apply a 'DPI+' approach.** The EAC needs to address uneven progress among Partner States, build on national successes and avoid importing off-the-shelf solutions. To unlock DPI's potential, the region will need sustained investment in infrastructure, regulation, innovation, and skills, while keeping costs and political realities in view.
2. **Treat DPI as foundational.** DPI should not be conceived as one-off projects. Future systems should be interoperable, modular and scalable, with inclusion and safety embedded from the outset. National procurement rules should prioritise open standards, vendor neutrality, and reusability. The regional focus should be on shared platforms such as federated IDs, payment switches and data exchange layers. Sustainability depends on

robust security and long-term planning. Donor support needs to be aligned with this systemic vision.

3. **DPI is not a silver bullet.** A public approach to DPI must centre human rights, treating infrastructure as a social process governed by equity, accountability and transparency. Poorly designed platforms risk excluding vulnerable groups and undermining trust.
4. **Build out regional infrastructure.** The EAC must strengthen the regional connectivity backbone, investing in satellite technologies to reach rural areas, and prioritising universal, affordable broadband. Regional data centres can provide a cost-effective way to support data sovereignty and the growth of a local digital industry.
5. **Develop enabling policy frameworks:**
    - 5.1. Adopt a regional **policy on interoperability and open standards** to reduce vendor lock-in and ensure scalability
    - 5.2. **Adopt a regional DPI Blueprint** to harmonise frameworks, embedding UNDP Safeguards and aligning with AU and AfCFTA standards
    - 5.3. **Develop national DPI frameworks** in alignment with regional DPI Blueprint, with Rwanda's forthcoming plan as a potential template
    - 5.4. **Strengthen privacy and data protection frameworks,** support countries that must enact laws, and push for Malabo Convention ratification to meet regional standards
    - 5.5. **Strengthen regional capabilities on cybersecurity**, with privacy-by-design, national cyber resilience, and regional CERTs, with baseline security controls embedded across all systems
6. **Support the private sector:**
    - 6.1. Develop a **'PPP for DPI' framework**, incentivising innovation, inclusivity, and private investment
    - 6.2. **Support local innovations** by investing in hubs, startups, and research institutions that use open-source building blocks to create scalable solutions for local needs
    - 6.3. **Support DPI sandboxes** at national and regional levels to test interoperability and regulatory frameworks, building on Rwanda's and Kenya's models
    - 6.4. Introduce **fintech licensing passports** to enable cross-border regulatory recognition, reduce hurdles for fintechs, and foster regional financial integration
7. **Establish regional and national leadership on DPI:**
    - 7.1. **Establish a regional DPI Centre** for coordinating strategies across sectors, embed DPI Safeguards, and provide political leadership

7.2. Ensure coordination and collaboration at national level through **inter-ministerial DPI taskforces** that promote joint planning and ecosystem-wide cooperation

7.3. **Create a regional DPI working group** under the EAC Secretariat, bringing together national authorities, regulators, private sector, and civil society to set common standards and develop the regional DPI Blueprint

7.4. **Adopt a global standard** such as GovStack PAERA when designing enterprise architecture at a regional level

8. **Ensure DPI sustainability:**

8.1. Ensure revenue streams for maintenance, build environmentally sustainable data centres, and assess human rights impacts before implementation

8.2. Establish baseline indicators for DPI Monitoring across Partner States to track progress, ensure accountability, and attract investment, building on emerging models in Rwanda and Kenya

8.3. Develop digital skills for public servants, policymakers, and innovators, and expand inclusive access for women, youth, refugees, and rural communities

8.4. Involve civil society, empower CSOs as equal partners to bring rights-based perspectives, accountability, and inclusivity into DPI design and governance

Methodology

The assessment drew on four main sources of evidence: 1) A review of laws, policies, strategies, and studies on national and regional DPI initiatives. 2) Interviews with public officials, academia, civil society representatives, international experts, as well as some private sector actors in the technology and telecommunications sector. 3) Questionnaires, which were each completed by an EAC partner state representative to ensure consistent country-level data. Finally, 4) all findings were examined through the UNDP DPI Safeguards Framework to assess risks and opportunities around inclusion, accountability, and sustainability.

The study faced some limitations. Responses to questionnaires varied in depth across Partner States, and the availability of up-to-date documentation differed significantly. While interviews helped fill these gaps, the findings rely on the perspectives of those consulted and available evidence at the time of research.

Introduction

The East African Community (EAC) strives for regional integration and for political, economic, social and cultural cooperation (EAC Treaty 2000). It increasingly views the concept of Digital Public Infrastructure (DPI) as a tool for completing the region's common market and monetary union (EAC Secretariat, 2025). DPI can make it easier for people in the region to move freely and access services using their digital IDs. It would also facilitate data sharing and seamless payments. With a functioning intra-regional DPI ecosystem, the EAC could position the region as a model for DPI-driven development across Africa and the Global South (G20 submission by EAC, 2025).

The report provides an overview of the state of DPI in the EAC region by exploring how each partner state approaches DPI from very different levels of national development. It then identifies the most relevant and promising DPI or DPI-like use cases as the region collectively is working towards an East Africa Stack – by building DPI that supports regional integration, through the cross-border sharing of data and digital services. It analyses policy ambitions, existing systems and technological choices, and the roles of public and private actors, identifying both constraints and opportunities for aligning national with regional DPI priorities.

The assessment is guided by the Universal DPI Safeguards Framework, which contains principles for the ethical, transparent, rights-respecting and sustainable development of DPI.[1]

1. What is Digital Public Infrastructure?

There is **no single definition of Digital Public Infrastructure**, but the concept is broadly defined as shared digital systems, which provide essential societal functions, analogous to physical infrastructure like roads, railways and electricity (UNDP, n.d.). A widely used definition by the G20 describes DPI as "a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and/or private services at societal scale" (G20 Digital Economy Ministers Meeting, 2023). These systems contain the pillars: (i) **Digital identification and e-signatures** to uniquely identify citizens and facilitate trusted authentication; (ii)

[1] Do no harm; Do not discriminate; Do not exclude; Reinforce transparency and accountability; Uphold the rule of law; Promote autonomy and agency; Foster communication engagement; Ensure effective remedy and redress; and Focus on future sustainability (DPI N.d.).

Digital payment platforms for instant financial transactions; and (iii) **Data exchange systems** to securely share data across government and private services with user consent (WB, 2025). In many countries, digital ID, digital payments, and data exchange exist independently – a DPI system pulls them together.

A good DPI system is designed to serve the **public interest**. The **Universal DPI Safeguards Framework,** which was developed by the United Nations Development Programme (UNDP), emphasises secure, interoperable systems built on open standards, governed by legal frameworks that ensure equitable access, innovation, competition, and respect for human rights (DPI, N.d.). The Global Digital Compact (GDC) similarly underlines that resilient and inclusive DPI can deliver services at scale, expand opportunities, and foster public trust through transparent, user-centred safeguards (Global Digital Compact, 2024).

Digital public infrastructure can transform service delivery, making government processes faster and more efficient:

Better service delivery: A well-implemented DPI can improve government services by connecting siloed systems and digitising processes, thus helping public services and commercial opportunities to reach people faster and more efficiently. During COVID-19, countries with interoperable digital systems were able to reach up to three times more people with emergency cash aid than those without. Togo's Novissi program illustrates this well as it provided direct cash transfers to eligible Togolese citizens who lost income due to Covid-19 (Tossou, 2021). A country like Estonia is said to save an estimated 2% of GDP annually in reduced paperwork due to its e-government system (Eaves and Vasconcellos, 2025).

Financial inclusion and economic opportunity: Digital ID and payments lower barriers to accessing financial services by making know-your-customer (KYC) processes cheaper and enabling small transactions. The case of India illustrates how the Aadhaar digital ID system enabled millions of people to access essential services, including opening bank accounts. In Africa, commercial mobile money services such as Kenya's M-Pesa have driven financial inclusion even without full integration with national digital ID systems.

Fraud reduction and transparency: Foundational ID systems curb duplicate entries in welfare programs. Using digital ID and biometric verification has helped Nigeria to remove 62,000 ghost workers and Zimbabwe to eliminate 10,000 from their civil service payrolls (Musoni, Domingo and Ogah, 2023). Integrated data also helps spot tax evasion. But digitisation alone does not guarantee trust or inclusion. DPI should not just serve to cut costs, but also to **empower and include** citizens through new services (Eaves and Vasconcellos, 2025).Transparency, accountability, and participation must be embedded from the start (UCL Report).

Cross-border digital services: Interoperable DPI systems can promote regional integration by facilitating cross-border digital services. The EU's eIDAS framework provides mutual recognition of national electronic IDs, so that an eID issued in one member state is accepted in all others (EC, 2025).

While DPI can generate significant public value, the DPI Safeguards Framework warns of risks that can undermine trust, inclusion, and sustainability:

Safety risks arise from privacy breaches, cyberattacks, and systemic digital insecurity, exposing individuals to identity theft, surveillance, or even physical harm when sensitive data is misused. Without robust data-protection frameworks, digital ID systems can be used as tools for constant surveillance (Roberts, 2025).

Inclusion risks include discrimination and unequal access. Onerous or mandatory enrolment often disempowers vulnerable groups.

Structural vulnerabilities, such as public distrust of digital technologies, weak rule of law and institutions, technical shortcomings, monopolistic concentration, and unsustainable financing or vendor lock-in (where a customer is dependent on a single service provider making it difficult or costly to switch service providers), can further erode the legitimacy and resilience of DPI systems (DPI, N.d.).

Systemic risks arise from greater interoperability as a failure in one system spills across the whole shared data infrastructure (Access Now, 2024). India's experience showed the challenge of ensuring data security for such a massive system when information of 815 million individuals was leaked in 2023 (The Hindu, 2023). Interoperability across a country's entire digital infrastructure also increases risks of commercial misuse (Roberts, 2025, Access Now, 2024).

Box 1: The complementary role of open standards and open-source systems

When governments and regional bodies design DPI, they often face the choice between adopting *open standards* and *open-source* systems or, more usefully, combining both. The distinction is subtle but important.

- **Open standards** are technical specifications that anyone can use to ensure systems can 'talk to' each other. They are usually developed through consensus by international or regional bodies, and they promote interoperability regardless of whether the underlying technology is proprietary or free. For example, the use of ISO 20022 in payments messaging allows banks in different countries to exchange information seamlessly, even when they rely on different vendors' software.

- **Open-source software**, by contrast, refers to code that is published under a licence that allows anyone to inspect, modify and reuse it. This does not automatically guarantee interoperability, but it can lower costs, build local capacity and reduce dependence on a single vendor. For example, the Modular Open Source Identity Platform (MOSIP)[2], developed in India and now adopted in several African countries, provides governments with a reusable framework for building digital ID systems. Modular design means building DPI in separate, reusable parts that can work together through open, well defined standards and each module can be developed, upgraded or replaced independently, without disrupting the whole system.

In practice, open standards and open source play complementary roles. Standards provide the common 'language', while open source offers adaptable tools. African policymakers weighing digital investments increasingly seek a balance: adopting open standards to safeguard long-term interoperability, while deploying open-source components where they offer flexibility and cost savings.

Source: ECDPM authors

[2] MOSIP is an open-source identity platform modelled on Aadhaar but designed for international adoption.

2. DPI in the East African Community

2.1 What does DPI look like within the EAC?

Though now framed as a comprehensive approach to building the digital roads and rails of public services, DPI is not entirely new to EAC Partner States, where previous digital developments fit the definition of DPI (Sang et al. 2025). For instance, Uganda developed a data exchange platform, UGHub, which enables seamless and secure sharing of data across Uganda's Ministries, Departments and Agencies (MDA's) and the private sector. Kenya has made progress on digital ID, leading to its *Maisha Namba* system, and it has also developed the eCitizen platform for digital government services. The United Republic of Tanzania (hereinafter 'Tanzania') locally developed the Jamii Stack, a system for secure data exchange and access to government services via digital ID. These platforms are interoperable across multiple systems. They facilitate service delivery through digital IDs and enable secure data sharing among institutions. In Kenya, for example, key systems such as eCitizen, IPRS, Huduma services, tax system, immigration, land registries, passport services are interconnected.

For the EAC, the DPI approach extends beyond the three pillars and considers the deeper foundations and broader ecosystem that a sustainable DPI requires. During the first and second EAC DPI Leaders Forums, Partner States emphasised that **infrastructure connectivity, digital skills and digital literacy are essential pre-requisites for DPI**. Accordingly, the development of DPI must integrate these baseline elements (EAC, 2024, EAC, N.d.c.). This **'DPI+' approach** is grounded in the realities of the region, where a significant part of the population remain unconnected and have low digital literacy. Initiatives such as the Eastern Africa Regional Digital Integration (EARDIP) project support the region not only across the DPI pillars but also by building connectivity infrastructures. The 'DPI+' framing is not unique. India, for instance, paired IndiaStack with large-scale digital literacy and connectivity efforts. What stands out in the EAC case is that these enablers are treated as integral to DPI design from the start, reflecting the region's higher rates of digital exclusion and uneven levels of development.

Although EAC Partner States broadly recognise the importance of interoperability and open-source tools, most have struggled to build such systems. Rwanda stands out for prioritising open-source solutions, with platforms like eKash built on

Mojaloop and oversight by the Rwanda Information Society Authority (RISA) to prevent vendor lock-in or monopolies. Kenya is transitioning from proprietary systems like M-Pesa to open, interoperable solutions under the Central Bank's guidance, while also moving from siloed legacy systems to modular platforms through initiatives like GovStack and the Shared Digital Services Framework.

Box 2: Overview of the GovStack building block approach

The **GovStack Approach** is a global initiative that enables governments to build and scale digital public services using a **modular, interoperable, and standards-based framework**. It promotes the use of **"Building Blocks"** — reusable software components such as identity, payments, and messaging — that can be combined to deliver end-to-end public services efficiently. By defining common technical specifications, governance models, and reference architectures, the GovStack Approach helps governments avoid duplication, ensure interoperability across systems, and accelerate digital transformation. It aligns closely with the principles of **DPI** and **Digital Public Goods (DPGs)**, fostering collaboration between countries, development partners, and technology providers to build inclusive, citizen-centric digital ecosystems.

Source: ECDPM authors

Somalia and South Sudan still use proprietary solutions and have not yet embedded modular design principles. Somalia also emphasised that it does not have a formal oversight mechanism to prevent vendor-lock in (Partner States Questionnaires). Burundi shows partial progress with some modular systems, but faces ongoing challenges of technical incompatibility that recent policy efforts aim to address. For its part, DRC is at an early stage in its DPI journey and does not have a clear stance on interoperability. Representatives of DRC mentioned Govstack as a useful resource for building interoperable e-government systems and avoiding fragmentation and vendor lock-in (DRC Interview, 2025).

2.2 What can EAC countries gain from regional DPI?

The EAC provides a compelling **case study for how regional blocs can pursue collective ambitions** in digital transformation despite significant differences in national capacities. While all eight Partner States share the goal of strengthening

DPI to facilitate cross-border services, trade and integration, they are not starting from the same baseline of digital readiness. Kenya, Rwanda, Tanzania and Uganda are digitally advanced compared to Burundi, DRC, Somalia and South Sudan. The digital front runners benefit from stronger mobile internet and broadband penetration, higher levels of digital literacy, and established e-government services. For example, Rwanda has digitised 85% of government services, supported by 96% 4G coverage and a digital literacy rate of 75.2%. Meanwhile, Somalia has digitised only 8% of its government services (Rwanda Questionnaire, 2025, Somalia Questionnaire, 2025). What could also explain the slower progress in Burundi, DRC, Somalia and South Sudan is that these countries face deeper infrastructural and institutional challenges, including political instability, civil conflict and weak foundational infrastructure.

Yet, despite these differences, there is **political will across the region** to cooperate on digital transformation. The EAC is navigating between frontrunners and countries still building digital foundations to ensure that such differences do not derail the collective ambition. For instance, the Cross Border Payments Masterplan addresses the hurdles for some partner countries to join the region's own payments system, the East African Payments System (EAPS). Importantly, less advanced countries are making progress in building their digital capabilities while also benefitting from the shared experiences (both successes and failures) of the front runners. Burundi and Somalia recently launched their national payment switches to facilitate digital payments. South Sudan, as a relatively new state, prioritises civil and vital statistics registration, laying the groundwork for a future digital ID system. DRC is testing a public-private partnership that may lay the groundwork for a future digital ID system. These efforts show that even amidst fragility, EAC countries are charting entry points into DPI.

2.3 How is DPI governed in the EAC?

The EAC is working to create policies and regulations that support digital transformation and DPI. The region is developing harmonised digital economy frameworks, regulations and laws, including on data protection, cybersecurity and electronic transactions, to build a secure environment for digital services.

In May 2025, the EAC validated its Digital Transformation Strategy, which provides a roadmap for using digital technologies for regional integration, socio-economic

growth and improved service delivery. The strategy aligns with the EAC Vision 2050, the African Union (AU) Agenda 2063 and the UN 2030 Agenda. It emphasises interoperable ICT systems, regional collaboration, and equitable digital access (EAC Digital Transformation Strategy). The EAC policy frameworks are also increasingly designed to align with the AU's economic integration objectives. Key AU instruments such as the African Union Interoperability Framework for Digital ID, the AU Data Policy Framework, the African Continental Free Trade Area Agreement (AfCFTA) and the AfCFTA Digital Trade Protocol provide direction for how EAC countries should develop DPI.[3]

3. DPI Pillars in the EAC: Payments, data exchange, and ID

3.1 Digital payments

The EAC is Africa's trendsetter in modern digital payment services and the leading regional economic community (REC) on mobile money payments. About 70% of global mobile money transactions take place in Africa, with East Africa generating the highest value.[4] For instance, the value of mobile money transactions processed by EAC Partner States like Uganda and Kenya runs over USD 110 billion annually (Gundaniya, 2025; AfricaNenda, N.d.). The success of this sector has triggered innovation and entrepreneurship, fuelling the region's growing digital economy and overcoming the limitations of an exclusionary financial sector. The EAC has committed to promote digital payments as a means to further regional trade and integration (Fincra, 2025, Monye & Monye, 2022; Ocran et al. 2024).

Mobile payment systems in the EAC

Mobile money launched by Safaricom's M-Pesa in 2007 has transformed digital payments in the EAC. Originally designed as a microfinance loan disbursement tool, it has evolved into a mobile wallet enabling deposits, withdrawals and transfers without the need for banks (Nyauntu and Shavdia, 2025). Kenya now shows near saturation, with users demanding broader services such as wealth

[3] Across the region, several national strategies focus on DPI pillars. Among them are Rwanda's ICT Sector Strategic Plan (SSP) (2024 - 2029), Kenya's National Digital Master Plan 2022–2032, Tanzania's Digital Economy Strategic Framework, Somalia's E-government Strategic Implementation Roadmap and Burundi's Master Plan for Digitisation of Public Services (2023-2033). Taken together, these national and regional policies and regulations position the EAC to drive digital transformation within the region and to contribute to the broader African vision of a single digital market.

[4] Digital payment or electronic payment is the transfer of value from one payment account to another using a digital device or channel and includes payments made with bank transfers, mobile money, QR codes, and payment instruments such as credit, debit and prepaid cards (Better than Cash Alliance, n.d.).

management, SME credit and digital tax payments (Gundaniya, 2025). Its success rests on high mobile penetration, extensive agent networks, 24/7 availability, and on offering faster, cheaper and safer alternatives to informal cash couriers (Fincra, 2025; Domingo, Arnold & Apiko, 2023). By contrast, banks were limited by high fees, slow systems and exclusionary requirements. Mobile money's convenience has pressured banks to digitise through mobile wallets and real-time settlement systems. Commercial banks have also launched mobile wallets and digital banking platforms, often complementing telco-led services.

Regional responses include the East African Payments System (EAPS), which reduces cross-border costs and delays[5] (see section 6.1.).

The EAC plans a **regional instant-retail payment switch** to make cross-border payments faster, cheaper and more inclusive (Cross Border Payments Masterplan). For this to work, partner countries must first upgrade their national switches and interlink them using common standards on security, consumer protection and fair participation. At present, Burundi (B-Switch), Rwanda (R-Switch), Somalia (SIPS) and Tanzania (TIPS) have national switches. Rwanda and Tanzania are expected to pilot the first link between R-Switch and TIPS, paving the way for a centralised regional system with strong governance and risk management (Interviews, 2025).

The EAC is also exploring **Central Bank Digital Currencies** (CBDCs) to support a modern, integrated and inclusive regional financial ecosystem (Cross Border Payments Masterplan). Rwanda plans to launch one by 2026 (National Bank of Rwanda), Burundi is considering the option, while other EAC countries have yet to begin.

Key stakeholders in digital payments

Key players include Mobile Money Operators (MMOs) and Mobile Network Operators (MNOs)[6] like Safaricom, Airtel, MTN, Vodacom and fintechs[7] such as Mojaloop, Flutterwave, Cellulant, Pesapal, Chura, Tala, Jumo, M-KOPA, Remitcore and Eversend. Banks like Tanzania's National Microfinance Bank (NMB), Equity

[5] The EAPS system is positioned as an enabler for boosting intra-regional trade and financial integration among EAC partner states (Central Bank of Kenya 2013; EAC, 2014).

[6] An MNO provides wireless communication services like voice and data and owns the physical network infrastructure. An MMO is an entity (often including MNOs or a financial institution) that provides mobile-based financial services such as sending and receiving money, and making payments through a mobile wallet system.

[7] Fintech is short for financial technology. Fintechs are companies that rely primarily on technology and cloud services to provide financial services to customers (McKinsey, 2024).

Bank and Ecobank have also introduced mobile services (Kuyoro and Flötotto, 2024). This ecosystem now supports peer-to-peer (P2P), peer-to-merchant (P2M), and peer-to-government (P2G) payments, social protection payments, and tax collection.[8] The EAPS ecosystem is overseen by Central Bank governors and the EAC Monetary Affairs Committee, with commercial banks participating through their national RTGS systems.

Digital payments as a driver of financial inclusion

Mobile money is a major driver of financial inclusion, particularly for women, informal traders, and rural populations. Initiatives by organisations such as the Better Than Cash Alliance (BTCA) and AfricaNenda Foundation have long promoted meaningful access to digital financial services for underserved groups: informal traders, women and the unbanked populations. Mobile money has become a powerful driver of financial inclusion, particularly for informal sector workers who have historically been excluded from formal banking. In Kenya, smallholder farmers, boda boda riders (motorcycle taxi operators), market vendors, and cross-border informal traders rely heavily on mobile money to transact, save, and access services (Kenya Questionnaire, 2025). Today, 75–80% of Kenyan adults use digital financial services, aided by strong policies and agent networks, while Rwanda reports 72% of women as active users through gender-focused initiatives. South Sudan and Somalia are still early in adoption, though Somalia's SOMQR and Burundi's digital literacy programs show progress (South Sudan Questionnaire, 2025; Somalia Questionnaire, 2025; Burundi Questionnaire, 2025).

QR code payments are expanding access for small traders and those with limited internet, offering low cost and sometimes offline transactions. Rwanda has integrated QR codes into its payment ecosystem, Kenya shows rapid uptake via private-sector solutions such as M-Pesa for Business, Equitel, and PesaLink, and Somalia has launched SOMQR (Somalia's national QR payment standard), while South Sudan lags behind. Digital financial services can boost women's financial participation, but most DPI projects lack gender-disaggregated monitoring, leaving some outcomes under-reported.

[8] In Kenya, for example, G2P (government to person) disbursements and social protection programs like Inua Jamii, National Health Insurance Fund (NHIF) payments, cash transfers for older persons, and the Hustler Fund are all facilitated by mobile money platforms. Additionally, tax collection has been streamlined through solutions like M-Pesa Paybill (Kenya Questionnaire, 2025).

Despite progress, critics warn against 'afro-optimism', noting that digital payments also bring risks such as predatory lending, fraud, data misuse, cybercrime, and high agent fees (Rodima-Taylor et. al. 2025, LeGrand et al. 2024). For instance, some merchants request customers to add a cash-out fee (referred to in Kenya and Tanzania as '*tuma na kutolea*', in Swahili), which is a fee that merchants are charged when cashing out the money (Domingo, Arnold and Apiko, 2023). Issues like non-reversible errors and monopolistic costs further burden users (Fintech News, 2025). In response, the EAC has introduced cybercrime laws and cybersecurity protocols.

Policy and legal frameworks on digital payments

The EAC region lacks a unified policy and regulatory framework for digital payments, which creates significant barriers to cross-border financial integration. Payment Service Providers (PSPs) operating across borders face costly and duplicative regulatory hurdles, as licensing processes differ among Partner States despite overlapping requirements (EAC, 2025b). To address the fragmented licensing landscape, the fintech community has called on EAC Partner States to introduce regional fintech licensing passports, enabling fintechs to operate across multiple countries under a single, mutually recognised licence (Mbego, 2024).

The absence of a common messaging standard such as ISO 20022 also undermines data transparency and quality, slows transaction processing and users have a poorer experience. However, Partner States like Rwanda, Kenya, Uganda, Tanzania, and Burundi have developed legal frameworks to permit digital payments both locally and across borders. Kenya's Central Bank launched the National Payments Strategy 2022 - 2025 to guide the development of a secure, fast, efficient and collaborative payments ecosystem. The Central Bank of Somalia is currently developing a National Payments System Strategic Plan, and a National Payments System bill is going through parliamentary procedure before it is passed into law (IMF, 2024, IMF, 2025). South Sudan is yet to enact a payments law. By putting in place the right laws and policies, EAC Partner States are making it easier for the payment ecosystem to grow.

3.2 Data exchange

The EAC region has made meaningful but uneven progress toward governing data exchange as a core building block of Digital Public Infrastructure. While some EAC countries have made progress in digitising public services, most are yet to adopt global data exchange frameworks. Protocols and rules for data exchange allow authorised entities to transfer both personal and non-personal data in a way that conforms to well-defined technical standards and regulations on data protection and data sharing. EAC partner countries will need a harmonised regime for data exchange to ensure efficient public service delivery, cross-border collaboration, and the realisation of the AfCFTA goals.

Data exchange in the EAC

EAC Partner States have made notable progress in digitising government services and data exchange. Examples of robust service portals include Kenya (*eCitizen*), Rwanda (*Irembo*), and Uganda (*UgHub*). These service portals provide access to eGovernment services such as business registration, tax filing, land management, and healthcare access among others. Tanzania's *Jamii X-Change*, is a data exchange platform that facilitates secure data sharing between government and private entities and applies the 'once-only principles' where citizens provide their data once, and it is shared across agencies as needed (DPI, 2024). These platforms have significantly reduced bureaucratic inefficiencies, improved transparency, and enhanced citizen engagement (Naeku et al. 2021). It is, however, important to note that the data exchange platforms mentioned above were built through PPPs between the respective governments and private companies using open standards and protocols. In the case of Kenya, eCitizen is owned, operated and maintained by WebMasters Kenya Ltd - a private company. This has raised concerns about the oversight over revenue streams processed by the developers and the potential for disruption of critical government services (KICTANet, 2025).

Technical Protocols, Policies and Frameworks

See box 3 below.

Box 3: Overview of global data exchange frameworks

- **The Data Empowerment and Protection Architecture (DEPA)** is a framework developed in India to enable secure, consent-based data sharing between individuals and institutions. It empowers users to control how their personal or organizational data is accessed and used by third parties, fostering trust and transparency in digital ecosystems. DEPA introduces the concept of 'consent managers' — licensed entities that mediate data sharing while ensuring privacy and compliance with regulatory standards. The model promotes interoperability across sectors such as finance, health, and education, supporting innovation while maintaining strong data protection and accountability principles.
- **X-Road** is an open-source data exchange platform originally developed in Estonia and now used by multiple countries as part of their digital government infrastructure. It enables secure, standardized, and decentralized data exchange between information systems across public and private institutions. X-Road ensures confidentiality, integrity, and traceability of data through strong encryption and digital signatures. Rather than storing data centrally, X-Road allows institutions to retain control over their own data while enabling interoperability through a trusted, federated framework. Its success has made it a global benchmark for cross-sector and cross-border data exchange.
- **The GovStack PAERA (Public Administration Enterprise Reference Architecture)** is a globally recognized framework that provides a common blueprint for digital government systems. It defines a set of interoperable building blocks and standards for data exchange, service delivery, and digital identity management within public administration. PAERA aims to help governments design and implement modular, reusable, and interoperable digital public services aligned with the principles of digital public goods (DPGs). By standardizing how systems interact and share data, PAERA promotes efficiency, scalability, and innovation while reducing duplication and vendor lock-in across government ICT ecosystems.

Source: ECDPM authors

Most EAC member states have not adopted global data exchange frameworks (e.g., Data Empowerment and Protection Architecture (DEPA), X-Road, GovStack PAERA (Public Administration Enterprise Reference Architecture). For instance, Tanzania has adopted X-Road, DEPA and GovStack. Rwanda and Somalia have adopted GovStack (Rwanda Questionnaire, 2025 Somalia Questionnaire, 2025), while Kenya is currently working with GovStack to design building blocks for DPI and considering the adoption of DEPA or X-Road (Kenya Questionnaire, 2025). As a result of this, the data exchange platforms mentioned above only facilitate data sharing at national and not at regional level. Cross-border data exchange remains a work in progress.

At the regional level, efforts are underway to establish enabling policies and frameworks. The EAC Digital Transformation Strategy has laid the groundwork for interoperable systems in line with the EAC's Vision 2050. Building on this, the EAC recently validated the Data Governance Framework (2025), which is pending adoption by Partner States. This framework seeks to balance free data flows with national sovereignty and rights protection, while fostering innovation, strengthening intra-EAC digital trade, and enhancing competitiveness in the global economy (EAC Data Governance Framework, 2025). Importantly, it is aligned with continental instruments, including the AU Digital Transformation Strategy, the AU Malabo Convention, and the AU Interoperability Framework for Digital ID.

The EAC also has the Legal Framework for Cyber Laws, whose provisions deal with the protection of personal data, consumer protection, and electronic transactions. The framework has been criticised for its limitations, including resource constraints for enforcement, lack of clarity on international best practices and reliance on voluntary adoption by Partner States.

At national level, the DRC, Kenya, Uganda, Rwanda, Tanzania, and Burundi have enacted cybersecurity regulations to curtail the growing spread of cybercrime and misuse of online platforms. Several states have enacted data protection laws, including for cross-border transfers of personal data or data exchange. Uganda, Kenya, Tanzania, Rwanda, and Somalia have standalone data protection laws. The DRC's Digital Code includes provisions on processing of personal data. Burundi and South Sudan are yet to enact data protection laws, though Burundi has a draft decree to create the Burundi National Commission for ICT and Protection of Personal Data. Some EAC Partner States have introduced data

localisation requirements, mandating that certain types of data be stored within the country (Beyleveld, 2021). These requirements may conflict with cross-border data exchange initiatives as they limit the scalability of data-exchange systems.

Box 4: Foundational DPI stack

Foundational DPI stack refers to the digital building blocks that enable the creation of interoperable digital public services at scale. Key components of this stack often include digital identity, digital payments and data exchange. These components form the basis upon which public and private solutions can be built to promote access to essential services for citizens (Clark et al. 2025).

The DPI stack in the EAC largely consists of **foundational digital systems** and **platforms** that enable the delivery of public services, drive economic growth, and promote inclusivity. Below is an overview of the foundational DPI stack in East Africa, highlighting **eGovernment platforms** such as Irembo, eCitizen, Jamii X-Change, and UGHub:

- **Jamii Stack** - Tanzania's DPI stack, comprises platforms such as **Jamii Namba** (digital ID), **Jamii Malipo** (digital payments) and **Jamii Data Shirikishi** (Jamii X-Change). These platforms are supported by four sublayers - consent, paperless, cashless and presenceless sublayer. Jamii X-Change, Tanzania's core data exchange platform, includes a consent management system, which manages and controls users' personal information including their consent (DPI, 2025).

- Rwanda's DPI stack is built on foundational services like the **iRembo** (eGovernment portal) platform and the **Single Digital ID** (digital ID), and aims to streamline access to digital services, enhance financial inclusion, and improve the performance of various sectors such as health and agriculture. Key components include digital identity, digital payments, consent mechanisms, and interoperable data exchange systems to facilitate secure and efficient digital services for citizens.

- Kenya's DPI stack consists of shared digital public goods including the **eCitizen** (eGovernment portal) and the **Maisha Namba** (digital ID) to ensure interoperability, access, and data security across sectors like finance, healthcare, and trade. The Maisha Namba, a unique personal

identifier assigned at birth and used throughout an individual's life, marks a pivotal shift toward a comprehensive and integrated identity management ecosystem.

- **Uganda's UGHub** (data exchange) forms the foundational layer of the country's broader DPI strategy, which involves building core digital public goods like digital identity, digital payments, and data frameworks.

Source: ECDPM authors

Impact of data exchange

Digitisation of government services has significantly improved efficiency in EAC countries, cutting processing times and costs while fostering entrepreneurship and economic growth (World Bank, 2022). eGovernment platforms enhance transparency and accountability, strengthening trust in public institutions. For instance, Rwanda's Irembo platform, which has digitised over 100 government services (Ministry of ICT Rwanda, 2025), has been lauded for its role in minimising corruption in service delivery (Transparency International, 2021). Uganda's UGHub platform has rapidly grown to include over 150 entities, spanning government agencies and private-sector organisations (NITA-U). As of 2025, Kenya is on track to meet its goal of integrating 25,000 services into its eCitizen platform by 2026 (eCitizen).

Box 5: Potential cross-border data exchange in the EAC

As mentioned above, data exchange use cases are mainly national in nature and implementation. Rather than trying to scale any particular service portal (**eCitizen, iRembo, Jamii X-Change or UgHub**) from one country to another, there is an opportunity to replicate a **Building Block** or a component from the **Application Layer** (GovStack, 2025) and scale this across the EAC region.

- The **Information Mediator (IM)** is a GovStack Building Block (GovStack, N.d.b.) that acts as a gateway for exchange of data and services to ensure interoperability and implementation of standards. IM is a channel through which external applications can connect to services such as registry services, identity services, and payment services.

- **GovBot,** is an application implemented using the **GovStack Approach** (GovStack, 2025). GovBot is a citizen-facing AI conversational chatbot for improved accessibility of eGovernment services, designed to address the challenge of fragmented service information. The chatbot provides citizens with 24/7 accurate answers sourced directly from official databases, includes source attribution for trust, and uses conversational memory to maintain context across multiple queries. A case in point is the **eCitizen GovBot** (GovStack, N.d.), an instance of the AI conversational chatbot currently being piloted on Kenya's **eCitizen** portal.

GovBot can be potentially integrated into existing service portals across EAC partner states. eGovernment services already offered on each service portal can be made more accessible by **increasing discoverability** of services and **reducing procedures** required to apply for services across the EAC.

Source: ECDPM authors

3.3 Digital Identity

EAC Partner States have made uneven progress in establishing digital identification as a core building block of Digital Public Infrastructure. Kenya, Rwanda, Uganda, and Tanzania operate more advanced national digital ID programs, while South Sudan, Somalia, Burundi, and the DRC are in earlier phases of implementation. Digital ID systems provide secure credentials and biometric authentication, which enable individuals to access services and facilitate transactions.

Most countries have designed their **IDs for domestic use**, shaped by national laws and regulations, which has **limited interoperability across borders.** Enrolment procedures, data standards, and governance rules differ widely, and there are no mechanisms for one country's ID to be recognised in another. To realise the full benefits of regional integration and cross-border mobility, EAC countries will need interoperable and mutually recognised digital IDs, supported by common standards and a harmonised regulatory framework.

Main stakeholders

Digital ID ecosystems in the EAC operate as hybrid constructs: International vendors supply critical biometric technology, PPPs take on secure credential production, and donor-brokered arrangements bring in both foreign public providers and large telecom groups, while civil society groups act as watchdogs.

A handful of global, mainly European vendors, such as Idemia, Veridos, Thales/Gemalto and De La Rue, have shaped digital ID in the EAC. These firms supply biometric systems, secure credential production and system integration, often through PPP structures. Some countries have also built their systems with the help of MOSIP, the Bangalore-designed open-source alternative. A case that combines both sources is Uganda's Security Printing Company (USPC), a 15-year joint venture with Veridos for ID cards and passports, while the ID authority simultaneously pilots MOSIP components with multilateral support. There are also new players in the game: Pakistan's national ID agency NADRA built Somalia's SNIDS system, which was launched in 2023.

The World Bank's Identification for Development (ID4D) initiative is a major player among international donors. It provides financing, technical assistance, and knowledge sharing for foundational ID projects in multiple African countries. In East Africa, the World Bank, with other partners, funded projects like the East Africa Regional Digital Integration Project (EARDIP) and country-specific ID system upgrades.[9] The United Nations Economic Commission for Africa (UNECA) hosts a new Centre of Excellence under its Digital Identity, Digital Trade and Digital Economy (DITE) initiative. International development agencies like GIZ and the UK's FCDO have also supported digital ID and civil registry reforms in the EAC. These partners contribute expertise on technical architecture (e.g. promoting open standards and digital public goods), as well as policy guidance on issues like data protection and digital ID for refugees/stateless persons, which is a key concern in the many regions of the EAC that host displaced populations.

Civil society organisations in the EAC, such as the Kenya Human Rights Commission (KHRC), Unwanted Witness in Uganda, and the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), have also become influential actors. They scrutinise digital ID rollouts, calling for stronger legal safeguards, independent oversight, and alignment with data protection

[9] It also backs the West Africa Unique Identification for Regional Integration (WURI) programme, which was often referenced by East African interlocutors in our interviews.

standards. Their pushback has in some cases slowed or redirected government implementation of digital ID systems.

Policy frameworks on digital ID

One of the AU's goals is to achieve universal identification coverage and a legal identity for everyone by 2030, in line with the Agenda 2063. A 'Digital Single Market' is a key goal under the AU's Digital Transformation Strategy (2020–2030), which mentions interoperable digital identity as a means to reaching it. The AU's Digital ID Interoperability Framework requires interoperability across AU states based on open standards, robust privacy and security safeguards, and clear institutional mandates with accountability (AU, 2023).

As early as 2020, a Digital ID Blueprint for Africa was formulated under Smart Africa's leadership to be a governance and technical framework for trusted digital ID systems continent-wide. The Smart Africa Trust Alliance (SATA) was established in 2023 as a public-private trust framework to enable mutual recognition of digital IDs across borders on a pilot basis (SATA 2023). Two EAC countries, Rwanda and Kenya, have been promoting this initiative.

Discussions with the AfCFTA Secretariat confirm that digital identity is now viewed as a core enabler of cross-border trade, mobility, authentication and payments. Under the AfCFTA Protocol on Digital Trade, member states are required to establish national digital identity systems. The Protocol commits to interoperable digital systems, including national digital identity systems and authentication, as a foundation for cross-border trust.[10]

Potential benefits and risks of digital ID

Digital identity systems, when designed and implemented well, can improve service delivery and reduce fraud. Foundational IDs allow governments to eliminate duplication in registries and to deliver health, education, and tax services more effectively. Kenya, Rwanda, and Tanzania explicitly link digital ID to efficient service delivery in their policy frameworks. They are also increasingly linked to financial inclusion, though this relationship is contested. On the one

[10] One of the annexes to the Digital Trade Protocol focuses on 'Digital Identities'. State Parties (which include all EAC Partner States) are obligated to establish and manage digital identity systems for individuals and legal entities, covering enrollment, issuance and credential management. The protocol sets common standards for implementing digital ID policies and a mutual recognition of digital ID systems. Article 12 on 'Interoperability' mandates member states to adopt "principles or common technical specifications including, but not limited to, open standards, digitally-signed logs, time-stamps, secure audit trails, secure communications, data sovereignty, privacy-by-design, or any other relevant key features" (AfCFTA Digital Trade Protocol).

hand, national IDs are central to tiered know-your-customer requirements and can streamline e-KYC for banks, insurers, and mobile money operators. Policymakers and development partners therefore often present digital ID as a gateway to deeper financial integration. On the other hand, East Africa's most successful inclusion story — mobile money — grew precisely because it operated with lighter KYC and without digital ID as a prerequisite.

Digital identity is a central enabler for the EAC's goal of a Single Digital Market. It can provide the trusted authentication layer for mobility, trade, education, and social protection. Digital IDs can also support labour mobility by making verification of professional qualifications easier. Finally, digital IDs could improve the continuity of humanitarian assistance, as systems set up by UNHCR and WFP have shown. Centralisation fears are warranted but could be solved. According to the World Bank's ID4D guidance, mutual recognition of IDs does not require a single supranational ID system. It can be achieved through interoperability standards and legal trust frameworks that let different systems 'talk' to each other and accept each other's assurance levels (World Bank, N.d.).

Critics argue that tying access too tightly to digital ID risks excluding those who remain undocumented or face enrolment barriers, undermining the very inclusion gains mobile money achieved. Without strong frameworks for privacy, data protection, and accountability, digital identity systems often face low adoption and public distrust. While governments and institutions such as the World Bank's ID4D initiative frame ID as a foundational layer of DPI and a prerequisite for financial integrity, civil society voices caution against one-size-fits-all solutions. The debate is therefore not only about technical enablers, but also about power, priorities, and the balance between inclusion, surveillance risks, and financial sector demands.

Digital ID development faces public backlash in several EAC Partner States (mainly Kenya, Uganda, and to some extent, the DRC). Civil society groups have warned that digital ID projects are often driven by private sector profit motives and government interest in expanding surveillance, with little to no meaningful public participation. There are also concerns that digital ID systems are exclusionary in nature, which leads to people in rural areas, the elderly, internally displaced persons, ethnic or religious minorities, refugees and previously undocumented groups being left out. Concerns also focus on biometric data collection, as many citizens see little added value—those without digital ID cards

can still access most government services and make digital payments without providing biometrics.

Box 6: Cross-border ID arrangements in the EAC

These cross-border arrangements are emerging among a core group of EAC Partner States:

Digital ID for cross-border mobility

Kenya, Rwanda, and Uganda already allow citizens to travel with national ID cards under the Inter-State Pass. The region has also adopted the East African e-passport (ICAO-compliant e-MRTD) to replace legacy passports. Recent ID programmes (e.g., Uganda's NIRA Phase II; Kenya's Maisha Card) include machine-readable zones and chips, paving the way for acceptance as electronic travel documents (World Bank, N.d.). An EAC framework, similar to Europe's eIDAS, would require Partner States to maintain agreed identity credentials (e.g., ID, e-passport) and establish a cross-border authentication node for real-time verification across borders.

Cross-border student enrollment

The Common Higher Education Area (CHEA) and the East African Qualifications Framework for Higher Education (EAQFHE) aim to harmonise standards and support mobility. Manual verification of credentials remains slow and prone to fraud. Several states now use online portals (KNEC–Kenya, UNEB–Uganda, NESA–Rwanda, NECTA/NACTVET/TCU–Tanzania). Somalia introduced a GovStack-enabled service for high school certificates, while the DRC launched a blockchain-based "e-Diplôme" platform in 2025 (Somalia Country Interview and DRC Country Interview).

Interoperable social security systems

The EAC Common Market Protocol grants workers equal treatment in social security, but portability is largely unrealised. In 2023, the EAC Secretariat, with ILO and AU–JLMP, drafted regulations on coordination of benefits, pending adoption (EAC N.d.j., ILO 2025). National funds already link to digital IDs and tax identifiers—Uganda's NSSF (NIN), Kenya's NSSF (National ID/eCitizen), and Rwanda's RSSB (online services) (NSSF Uganda; NSSF Kenya; RSSB Rwanda). A regional framework could build on these systems to authenticate workers, exchange records, and enable digital claims. Stakeholders such as the East African Trade Union Confederation (EATUC, 2016) stress that a trusted digital backbone is essential for labour market integration (EATUC).

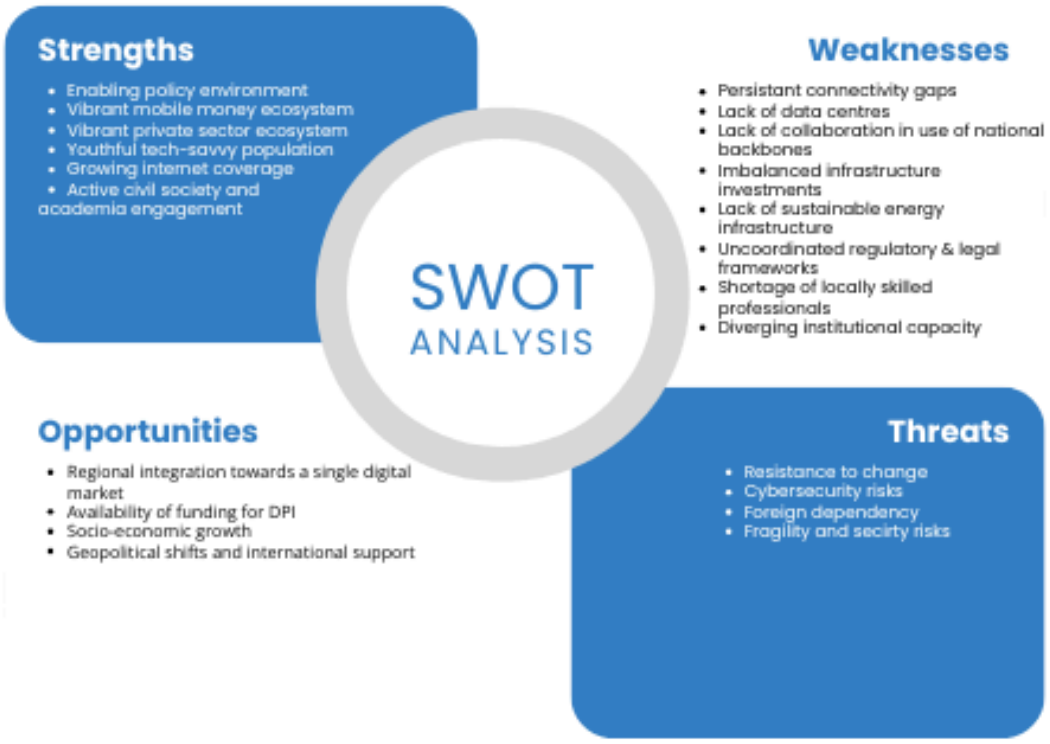
Source: ECDPM authors

4. Regional DPI readiness in the EAC - SWOT Analysis

The EAC views DPI as a tool for **generating value across the region** and for achieving a (digital) single market. The region benefits from a vibrant mobile money and digital payments ecosystem, its enabling policy environment, youthful and innovative population and fairly advanced connectivity infrastructure. However, implementation of DPI across EAC member states is a complex undertaking. The region has to solve structural challenges and mitigate risks of the development of digital infrastructure. The lack of modular systems creates rigidity as the existing systems cannot be easily upgraded or expanded. For instance, DHIS2, an open-source health information management system now adopted across all EAC countries, is designed on global interoperability standards. Yet in practice, national instances evolve differently, and variations in configuration, governance, and legal frameworks mean that seamless cross-border exchange is a long-term aspiration, not a present reality.

There are also promising examples for cross-border interoperability, such as the progress in digital payments in Kenya and beyond. Tanzania provides a concrete example for an interoperable data sharing mechanism through its Jamii Data Exchange (Data Shirikishi), a platform built with cross-border data-sharing capabilities. Tanzania is already piloting this with a European country to facilitate inter-continental cross-border interoperability (Tanzania Interview, 2025).

Figure 1: DPI SWOT Analysis



Source: ECDPM authors

The following section discusses the strengths, weaknesses, opportunities and challenges of deploying DPI in the EAC region.

4.1 Strengths

Enabling policy environment

The policy initiatives supporting DPI in the EAC region have laid a strong foundation for digital transformation, economic integration, and inclusive growth. EAC Partner States have demonstrated strong political commitment to advancing DPI through policy frameworks such as the EAC Cross-Border Payment System Masterplan and EAC Digital Transformation Strategy.

Vibrant mobile-money ecosystem

Mobile money in the EAC is a success story. Easy access to payment has supported financial inclusion and local innovation. Mobile money represents a

DPI-relevant system that the EAC can showcase internationally and offer as a model for the design of payment systems in other regions (See section 6.2 on cross-border mobile money).

Vibrant private-sector ecosystem

The EAC has a fast-growing consumer base, and a growing middle class demands sophisticated products. Due to regional integration, businesses have access to a large market of over 331 million people and a combined GDP of $313 billion in 2023 (EAC, n.d.i). The region is also well located for reaching other African markets.[11] Kenya's vibrant private tech ecosystem, often dubbed 'Silicon Savannah', thrives on private capital, foreign investment, and the emergence of local angel investors.

Youthful, tech-savvy population

The EAC region has one of the youngest populations globally, with over 70% under the age of 30 (UN, 2024). Despite the general digital skills shortage and digital divides in Africa, young people in the EAC are tech-savvy and enjoy access to smartphones, the internet, and digital platforms. To support youth innovation, governments and businesses are offering training for general digital literacy and technical digital skills. Kenya runs the Digital Literacy Program (DLP), Tanzania the SmartWASOMI, and Rwanda the Digital Ambassadors Program (DAP). Burundi, through the Ministry of Communication, Information Technology and Media, provides public training on responsible use of ICT, while Somalia offers basic digital skills training and awareness programs to its citizens. In addition, there are several youth-focused innovation and entrepreneurship initiatives across the EAC.[12]

Growing internet coverage

High-speed, reliable internet is essential for DPI applications like e-government, e-commerce, and digital payments. Over the past two decades, the EAC has improved on digital connectivity, mainly due to new submarine cables, terrestrial fibre backbones, and more recently satellite internet. The region is connected to

[11] Tanzania borders eight countries, with Dar es Salaam Port serving as a key hub for landlocked neighbors. Kenya, led by Nairobi's global air links, has a thriving tech-driven economy supported by fintech, agribusiness, logistics, startups, and strong policy backing.

[12] East African Communications Organization (EACO) and Envisage Incubator from Rwanda;: Koneta Hub and UNDP Accelerator Lab from South Sudan; Tanzania Startup Association (TSA) and Nelson Mandela African Institution of Science and Technology (NM-AIST) from Tanzania; Association of Startups and SME's Enablers in Kenya (ASSEK) and Kenya National Innovation Agency (KeNIA) from Kenya; StartHub Africa and Innovation Village from Uganda; Aclis Burundi from Burundi.

global internet infrastructure through undersea fibre-optic cables.[13] At national level, government-led investments have connected cities and rural areas through projects such as Kenya's National Optic Fiber Backbone Infrastructure (NOFBI) and Rwanda's KTRN. [14]

The region is also taking advantage of alternatives to fibre (microwave and satellite) for areas where fibre deployment is uneconomical (EIB, 2021). Somalia, DRC, South Sudan, Rwanda, Burundi and Kenya are using Starlink's low-earth orbit satellite communications technology to connect underserved regions (Starlink Availability Map). Even in conflict-affected regions like South Sudan, satellite connectivity is proving vital for digital inclusion (Sunny, 2024). Starlink's wide coverage and increasing affordability in the EAC presents a chance to close the last-mile connectivity gap in remote areas (Yaici, 2025).

Active civil society and academia engagement

While DPI projects are mainly led by governments and the private sector, the EAC also has an active civic space. Civil society groups such as KICTANET, Pollicy, Paradigm Initiative, Unwanted Witness, as well as research groups like Collaboration on International ICT Policy for East and Southern Africa (CIPESA) or Centre for Intellectual Property and Information Technology Law (CIPIT) have been vocal on DPI-relevant issues, from data protection to surveillance risks of digital IDs or payments. Partner States indicate that they involve civil society and academia in policy formulation, although civil society actors are not always convinced that this engagement is meaningful.

4.2 Weaknesses

Persistent connectivity gaps

Across EAC member states there are still significant gaps in internet connectivity, high cost of internet and low digital literacy. According to the EAC Regional Sectors Communication Report 2023, 2G coverage is at a regional average of 92%, ensuring that basic communication services are widely available. On the other hand, 4G coverage is at a regional average of 62%. Kenya and Rwanda lead with over 97% coverage, while 4G coverage in Tanzania stands at 79%, but Uganda,

[13] Such as SEACOM, the East Africa Submarine System (EASSy) (with landing ports in Somalia, Kenya and Tanzania), and The East African Marine System (TEAMS) (which links Kenya to the UAE).

[14] Uganda has started to deploy 5,845.75 km of fibre-optic cable to connect 70 districts and 2,800 sites. MyUG free Wi-fi is offered through 1,754 public access points, complementing ongoing private-sector activities (Uganda Presentation, 2025).

Burundi and South Sudan have only 35%, 32% and 29% respectively. Furthermore, broadband access costs vary across the EAC. Coastal countries benefit from direct submarine cable connections, while landlocked Partner States depend on regional networks. Although prices have declined, disparities persist, highlighting the need for continued regional cooperation to ensure affordable access for all. The cost of monthly mobile data plans greatly varies across EAC Partner States. South Sudan has the most expensive data plan at $6.25 and Rwanda has the cheapest at $0.76 (EACO, 2023).

Despite declining costs, internet access and digital devices remain unaffordable for many low-income households in the EAC region. In addition, many citizens, particularly in rural areas and among older populations, lack the digital literacy to effectively use DPI platforms. Women and girls often face additional barriers, including cultural norms. Many citizens are unaware of the availability and benefits of DPI services, such as e-government platforms, digital payments, and online education. Many DPI platforms lack locally relevant content and services, particularly in local languages, which reduces their appeal and usability. Groups such as the elderly, persons with disabilities, and refugees, are particularly vulnerable to digital exclusion due to these gaps.

Lack of data centres

The EAC region still lacks sufficient data centre and cloud computing resources to support e-government and e-services platforms and to host large amounts of data. Our interviews with EAC Partner States revealed the following: Tanzania, Kenya, Rwanda and Uganda have local tier 3 data centres. The DRC inaugurated two tier 3 data centres in 2024 and 2025. Somalia recently finished building its first data centre. South Sudan has no local data centres but there are plans by the National Communication Authority, Ministry of Finance and Central Bank of South Sudan to build micro data centres (critical IT load capacity <100 - 150 kW). The Burundi government uses a local mini data centre (critical IT load capacity <10 kW) while in the DRC, the central bank (Banque Centrale du Congo), the national tax authority, and the government headquarters all use their own data centres. The one used by the central bank is referenced as a tier 3 data centre (Partner States Questionnaires, 2025). According to the East Africa Data Centre Markets Brief, 2025, East African data centre capacity falls below Southern Africa levels when measured against population size. East Africa will need to add around 150 MW, or 25 to 50 new data centres, to meet rising demand.

Lack of collaboration in use of national backbones

The politics of access to fibre remains a delicate balancing act across the region. On paper, the region has embraced regional connectivity through initiatives such as EARDIP, which aim to ensure the landlocked countries have adequate internet access. Experience shows the limits of that cooperation. Uganda is strengthening cross-border connectivity through key border points.[15] More broadly, some governments have expressed frustration at inequitable access arrangements and the lack of transparency by coastal countries in setting terms for access to submarine cables (Partner States Interviews, 2025).

Imbalanced infrastructure investments

Digital infrastructure investments in the EAC region are heavily concentrated in Kenya, Tanzania, Rwanda, and Uganda, leaving Burundi, South Sudan, Somalia and the DRC lagging behind. Foreign Direct Investment (FDI) is the largest source of funding for infrastructure projects in the EAC. This leads to funding flowing into large and growing markets with abundant natural resources, competitive labour costs, and strategic advantages for expansion. This imbalance exacerbates economic inequalities between the more digitally advanced countries and the less developed ones. Unequal digital infrastructure undermines the EAC's goal of fostering seamless regional trade and collaboration.

Lack of sustainable energy infrastructure

The EAC region has various energy bottlenecks due to frequent power outages, limited access to the grid, soaring energy costs and the complexities of procuring and integrating renewable energy. In South Sudan, the energy crisis is worsened by military attacks on power stations (BBC News, 2025, South Sudan Interview).

This makes it difficult to catch up with the growing energy demands to power data centres or telecommunications infrastructure. Furthermore, the cost of electricity in the EAC region is often high, making it expensive to power digital infrastructure.[16] The EAC relies heavily on hydropower but lacks an efficient distribution infrastructure. Hydropower also exposes the region to impacts of climate change, such as droughts and floods, which can disrupt energy production and supply.

[15] Uganda highlighted the "lack of collaborations between countries especially in the use of the NBI (dark fibre) by land locked countries" (Uganda Presentation, 2025). Dark fibre refers to unused optical fibre capacity that has been laid but is not yet activated or made available for traffic. Burundi also raised concerns over the high transmission costs to connect to the fibre at the border with Tanzania (Burundi Presentation, 2025).

[16] The average price of electricity at the grid is $0.15 per kilowatt hour (KWh) - among the highest in the world, compared to Ethiopia at $0.8 per kWh (EAC, 2023).

In addition, inconsistent energy policies hinder regional coordination and investment in energy infrastructure. The East African Power Master Plan proposes joint action against power shortages, low access, high cost and poor power system reliability. As a region, the EAC is investing in green and climate-friendly energy solutions (EAC G20 Submission), but observers say that it has to be more strategic in its approach (Medinilla and Byiers, 2023).

Uncoordinated regulatory and legal frameworks

Despite regional efforts, differing legal and regulatory frameworks lead to inconsistencies in data protection, cybersecurity, and digital trade policies. Currently, only five EAC Partner States have both laws and institutions for data protection: Uganda, Rwanda, Tanzania, Kenya, and Somalia.[17] Countries with robust laws and enforcement institutions require recipient countries to provide an adequate level of protection, thus limiting data exchange with countries that lack similar standards. The EAC Data Governance Policy Framework (EAC, 2024c) addresses some of these issues, and will serve as a guiding instrument for Partner States as they develop their national data governance frameworks.

Shortage of skilled local professionals

Across the EAC region there is a shortage of skilled professionals in key areas such as software development, data science, cybersecurity, and digital infrastructure management. As a result of this, many DPI projects in the EAC region rely heavily on foreign consultants and technologies, reducing local ownership and sustainability. This dependence increases costs and limits the region's ability to innovate and adapt solutions to local contexts. Government agencies and organisations responsible for DPI often lack the capacity to manage complex digital initiatives, including planning, implementation, and monitoring.

Diverging institutional capacity

Significant differences in institutional capacity and digital maturity exist between the more advanced EAC countries (Kenya, Uganda, Tanzania, Rwanda) and the newer partner countries (South Sudan, Somalia, Burundi, DRC). These disparities make it harder to achieve interoperability and region-wide adoption of digital public infrastructure. For instance, South Sudan does not yet have a National Competition Authority, National Consumer Commission or a Data Protection

[17] The other three have yet to enact a framework but rely on various legislations to guide them on data protection. For instance, the primary data protection law in the DRC is part of the Digital Code (Tungali, 2024) which comprehensively covers digital activities and services, including the protection of personal data.

Commission to carry out specific institutional engagements needed to facilitate cross-border payments or transactions.

4.3 Opportunities

Regional integration towards a single digital market

DPI can be a catalyst for regional economic integration in the EAC region by enabling seamless digital payments, customs clearance, and data exchange among EAC Partner States. The African Union Digital Transformation Strategy (DTSA) lays the foundation for building a Single Digital Market (DSM) across the continent by 2030. This would ensure free movement of persons, services and capital, and individuals and businesses could seamlessly access and engage in online activities within the AfCFTA. An East Africa DSM would be the ninth largest in the world, based on population, creating the market size needed to attract significant digital investment (Torgusson et al. 2018).

Socio-economic growth

DPI solutions, such as mobile-money platforms, can expand access to financial services for unbanked and underbanked populations. This leads to economic empowerment, entrepreneurship, and poverty reduction. The development and scaling of DPI solutions create jobs in ICT, software development, digital services, and related sectors. DPI also supports economic diversification by enabling new industries, such as e-commerce, fintech, and digital agriculture. DPI platforms, such as e-government services and digital identity systems, can enhance the efficiency, transparency, and accessibility of public services, thus improving citizen satisfaction, reducing corruption, and boosting productivity.

Availability of funding for DPI

The EAC could advance development of cross-border DPI by tapping into readily available global funding sources. International organisations, bilateral partners and private donors, such as the World Bank, GIZ, Gates Foundation and African Development Bank (AfDB), are providing funding and technical support for DPI initiatives in the EAC region. Increased collaboration between governments, private-sector players, and development partners can accelerate regional DPI development in the EAC region. For instance, there is an opportunity to advocate for more EU funding under the framework of the Global Gateway by setting DPI-related funding targets. EAC Partner States can build evidence on linkages

between core DPI – which remains underfunded – and national development priorities or the SDGs (Aleina, 2023).

Geopolitical shifts and international support

Digital sovereignty has become a priority for many countries among political uncertainty. Global institutions and donors are increasingly backing open-source ecosystems as an alternative to dependency on proprietary systems. The ITU/UNDP Open Source Infrastructure Enabler project in Kenya, which established the country's first Open Source Programme Office (OSPO), illustrates this trend. Several other Sub-Saharan African countries have expressed interest in joining the initiative, highlighting its potential for regional expansion. By engaging strategically with these developments, the EAC can attract new funding, technical expertise, and political goodwill to advance regional DPI and the East Africa Stack.

4.4. Threats

Resistance to change

Government agencies and organisations often resist adopting new technologies and processes due to bureaucratic inertia and fear of disruption. Many stakeholders, including policymakers, businesses, and citizens, may not fully understand the benefits of DPI. This reduces support for DPI initiatives and hinders their adoption. For instance, the implementation and rollout of Kenya's initial digital ID system (Huduma Namba) faced significant challenges such as litigation, a lack of public participation, concerns over data privacy and security, exclusion of marginalised communities lacking prior IDs, and potentially high costs for citizens (Kenya Interview, 2025). Furthermore, the introduction of digital technologies may be perceived as a threat to traditional jobs by workers and unions. Established businesses and institutions may resist DPI initiatives that disrupt their business models or market dominance, leading to lobbying against DPI projects or non-cooperation in their implementation.

Cybersecurity risks

The EAC region has experienced a surge in cyberattacks, including ransomware, phishing, and Distributed Denial of Service (DDoS) attacks (Mutuku, 2025). These attacks disrupt DPI operations, compromise sensitive data, and undermine public trust in digital systems. EAC Partner States lack comprehensive cybersecurity laws and regulations. In addition, many users, including government officials, businesses, and citizens, lack awareness of cybersecurity best practices (UNECA,

2025). There is a shortage of skilled cybersecurity professionals, which negatively affects the region's ability to detect, prevent, and respond to cyber threats effectively. The lack of harmonised cybersecurity laws across EAC Partner States presents a significant threat to the implementation of DPI in the region.

Foreign dependency

The EAC region relies heavily on foreign technologies and funding for DPI development, which can limit local innovation and ownership. An over-reliance on foreign expertise discourages the development of local skills and capabilities in DPI-related fields, such as software development and cybersecurity. In most cases, foreign technologies and platforms involve storing data on external servers, raising concerns about data sovereignty and security. Furthermore, foreign companies and organisations may exploit the dependency by imposing unfavourable terms, high fees, or monopolistic practices. Unchecked foreign dependency can limit the economic benefits of DPI, as profits and jobs often flow to foreign companies rather than local economies.

Fragility and security risks

Chronic political fragility and security challenges in several EAC Partner States, including South Sudan, Somalia, DRC, and Burundi, pose serious obstacles to the stable deployment and regional integration of digital public infrastructure.

5. East Africa in the global DPI discourse

5.1 DPI at the G20

After India and Brazil, Africa sees it as its turn to shape the global DPI discourse. South Africa, which holds the G20 presidency in 2025, places a special focus on regional integration. It has maintained the DPI agenda but reframed it around regional diversity and measurement of societal impact. The government has announced the creation of a G20 Task Force on DPI and AI, with a focus on ensuring that infrastructure is designed inclusively and assessed against actual outcomes rather than technology-first promises. South Africa is also linking the G20 agenda with African Union initiatives, such as the AU's 2022 Digital ID Interoperability Framework.

The concept of DPI, though rooted in decades of e-government efforts, had first been brought onto the global stage by India's 2023 G20 presidency (Teevan et al.

2025). The G20 New Delhi Leaders' Declaration recognised that DPI, when "safe, secure, trusted, accountable and inclusive, respectful of human rights, personal data, privacy and intellectual property rights, can foster resilience, and enable service delivery and innovation" (G20 Leaders Declaration 2023b).[18]

India drew on its national experience with the India Stack, a combination of biometric ID (Aadhaar), real-time payments (UPI), and consent-based data sharing (DEPA). Modi's government framed DPI as a cost-effective and inclusive development model, which other countries could adopt. When Brazil assumed the G20 presidency in 2024, President Lula endorsed India's model. Brazil had already written its own DPI success story: the Pix instant payment system, launched by the Central Bank in 2020, which reaches over 150 million users (as of mid-2025).

Box 7: DPI as a global development strategy

DPI is increasingly framed as a global development strategy, championed by multi-stakeholder coalitions and backed by significant funding programmes and partnerships (for example, through the UNDP). International institutions and development agencies (UNDP, World Bank's ID4D, etc.) and coalitions (e.g. the Digital Public Goods Alliance, GovStack) promote DPI as a means to accelerate progress on SDGs. Philanthropic and multilateral actors have integrated DPI in development agendas. The Gates Foundation, through support for MOSIP (ID) and Mojaloop (payments), presents DPI as critical to financial inclusion (Gates Foundation - IIIT Bangalore, Gates Foundation - Mojaloop).

Networks like Co-Develop, the Centre for DPI, and the 50-in-5 campaign (launched by UNDP and partners in 2023 to help 50 countries adopt DPI in five years) provide technical and funding support. These coalitions argue that without coordination, countries risk duplications and systems fragmentation, as well as vendor lock-in. Within the EAC, Uganda is part of this campaign, while Rwanda, Kenya and Tanzania are in discussions to join. Rwanda and Uganda are

[18] The declaration launched a "G20 Framework for Systems of DPI" (G20 Annexure 1, 2023a) and endorsed the creation of a Global DPI Repository and the One Future Alliance (OFA), a voluntary platform to mobilise finance and technical support for DPI globally.

also members of the Digital Public Goods Alliance, which promotes open-source technologies to advance sustainable development goals.

Yet, the availability of funding raises critical questions about who is setting and shaping the DPI agenda and whether developing countries themselves are driving the demand for a DPI-centric approach to digital transformation (Interview, 2025).

Source: ECDPM authors

5.2 Greenfield vs. brownfield: India and Brazil

As EAC country leaders consider DPI, they can draw lessons from India's **"greenfield" and Brazil's "brownfield" approaches** to building digital infrastructure. India built a comprehensive DPI largely from scratch. In about one decade, it developed the India Stack, a suite of federated digital platforms including the Aadhaar ID system, UPI payments, and data-sharing frameworks. This greenfield strategy allowed India to design the system holistically with modern principles such as open APIs and interoperability.

India is a valuable DPI partner for Africa given its experience with large-scale financial inclusion and service delivery. To support other countries, India backed the creation of MOSIP. As of February 2025, of the 11 MOSIP-implementing countries, eight were in Sub-Saharan Africa, namely Burkina Faso, Ethiopia, Guinea, Madagascar, Niger, Sierra Leone, Togo, and Uganda (Sang et al. 2025). Countries like South Sudan, which are not yet digitally advanced, could benefit from this greenfield approach. However, India's journey cannot serve as a single blueprint as its focus was on developing DPI for one country with over one billion people. This centralised top-down solution is difficult to reproduce in Africa, a continent of 54 countries with different legal and governance systems. In addition, the greenfield approach **is not a good fit** for countries with fragmented legacy systems.

The Brazilian model of integrating existing systems could be suitable for EAC frontrunners like Kenya, Rwanda and Tanzania. Brazil's example shows that countries with existing digital systems can evolve towards DPI through incremental reforms, one component at a time. Brazil's path is more sector-led

than stack-wide: The Central Bank designed the Pix instant payment system as a real-time, low-cost public rail with rules for large institutions. In parallel, the website gov.br serves as the state's Single Sign-on (SSO) for access to public services. In so doing, Brazil gradually unified access to services through gov.br, instead of creating a brand-new identification system. This mix of regulatory orchestration and platform consolidation is now referenced internationally as a DPI approach distinct from India's. Brazil interprets DPIs as a series of collaborative, transformative processes. Brazil's federal constitutional order grants autonomy to states, which has produced a lively sub-national digital ecosystem: States have developed their own portals and apps—often integrating with the federal gov.br login, which now serves as a single sign-on for citizens to access thousands of previously fragmented e-government services.

5.3 Focus on regional integration: Latin America, the EU and ECOWAS

As EAC countries explore regional integration of their systems, they could also look to Latin America or the EU. For example, the Mercosur Digital Citizen project aims to connect national eID systems across five countries (IADB, 2024). Since 2024, Uruguay and Brazil have piloted integrated digital ID "broker" systems, which allow Brazilian citizens to securely access 40 Uruguayan e-government services with their Brazilian credentials (Interview with Agesic Uruguay). A comparable case in Europe is the Estonia–Finland 'X-Road' connection, where each country keeps its own population registry but a shared data-exchange layer lets services query across borders. For example, a Finnish official can verify an Estonian citizen's records in real time.

Around the world, examples of this kind of interoperability are still very rare. But initiatives like the Smart Africa Trust Alliance (SATA) are working to make them a reality in Africa. Continental policy now anchors this direction via the AU Data Policy Framework and the AU Interoperability Framework for Digital ID, under which countries and regions progressively connect existing systems. In West Africa, ECOWAS is increasingly adopting the DPI approach to advance regional integration, enhance financial inclusion, and improve service delivery. Through frameworks such as ECOWAS E-Commerce Strategy 2023 and the Digital Sector Development Strategy 2024 - 2029, the bloc is building the legal and institutional foundations for interoperable digital systems. However, uneven progress among member states, infrastructure deficits, and the withdrawal of Niger, Mali and

Burkina Faso pose challenges to harmonised implementation and cross border DPI applications (Asadu, 2024, MacDonald, 2024c).

Box 8: ECOWAS approach to DPI

Legal and policy environment: ECOWAS has developed a robust legal and policy framework to drive DPI, anchored by the 2023 ECOWAS E-Commerce Strategy and Implementation Plan and the Digital Sector Development Strategy 2024 - 2029 (Ecoroads). It has advanced regional connectivity through the ECOWAS Roaming Regulation (ECOWAS Regulation No. C.REG/21/12/17 on Community roaming within the ECOWAS space). Recently, Ghana, Togo and Benin implemented this regulation by launching the ECOWAS Free Roaming initiative (Graphic Online, 2024; Khoza, 2024). It also leads Africa's Regional Economic Community (REC) on data protection, backed by its Supplementary Act on Data Protection and members' (Cabo Verde, Ivory Coast, Ghana, Guinea, Senegal and Togo) ratification of the Malabo Convention (Malabo Convention Status List). To enhance digital security, ECOWAS also enforces a Cybersecurity and Cybercrime Strategy requiring national cybersecurity frameworks, establishment of cybersecurity authorities, and creating Computer Security incident Response Teams (CSIRTs) (Digwatch, 2021).

ECOWAS digital payments: Mobile money is the main driver for financial inclusion in West Africa, with active accounts rising by 11% to reach 514 million in 2024 (GSMA, 2025). ECOWAS supports financial inclusion through interoperable systems to enable cross-border payments and e-commerce (ECOWAS Digital Financial Inclusion Strategy). However, cash dependency and low financial literacy hinder wider adoption. The Pan-African Payment and Settlement System (PAPSS), now operating continent wide, supports instant local currency transfers and the 2025 launch of the PAPSSCard enhances interoperability. Within the West African Economic and Monetary Union (UEMOA), a common market framework further facilitates regional payments (UEMOA Amended Treaty).

ECOWAS data exchange: Data exchange remains the least developed DPI pillar in ECOWAS. The West Africa Regional Digital Integration Project (WARDIP) addresses this gap by supporting infrastructure development, harmonising regulatory frameworks, and promoting cross-border connectivity and private-sector investment.

ECOWAS Digital ID: The West Africa Unique Identification for Regional Integration and Inclusion (WURI) program is a flagship initiative driving interoperable, inclusive ID systems to enable cross border access to services and jobs across Ivory Coast, Guinea-Bissau, Burkina Faso, Niger, Togo, Ghana and Nigeria. Complementing this, ECOWAS National Biometric Identity Card (ENBIC) supports free movement and regional integration, though uptake remains slow (MacDonald, 2024b).

Nationally, progress varies: Ghana leads its integrated Ghana Card and universal QR Code (Mobile ID World, 2025, MacDonald, 2024a, Teevan and Domingo, 2022). Benin has advanced data exchange via X-Road and PKI systems (Interview, 2025). Nigeria plans to launch its General Multipurpose National Identity Card (GMPC) in October 2025, integrating payment systems, government subsidies, and financial services (NIMC, 2024, Enoch, 2025). Sierra Leone has partnered with MOSIP to pilot an open-source national digital ID system through its National Civil Registration Authority (Burt, 2023, MOSIP, 2023).

Source: ECDPM authors

6. Scaling DPI across borders: Regional DPI use cases in the EAC

We identified six use cases of DPI to illustrate both the diversity and interconnectedness of initiatives in the EAC region. The selection was not driven by a direct alignment with any single pillar of DPI (identity, payments or data exchange), but instead by how these examples demonstrate linkages across multiple domains and their relevance to the EAC's priority of regional integration through digital interoperability.

The levels of maturity of these solutions vary: Some are fully operational and demonstrate measurable impact, while others remain in pilot or early adoption stages, but have potential to be scaled up. Some of the use cases are private sector-led, while others are government-led. Each use case was assessed against the UNDP DPI Safeguards Framework, with attention to its degree of interoperability, contribution to inclusion, public value, and potential to scale not only across the EAC, but also within the wider AfCFTA market.

Collectively, the six cases provide insights into how DPI in East Africa is evolving as a connected ecosystem, which advances both national priorities and regional integration. These concrete cases of DPI implementation hold the potential to accelerate growth and development across the region.

Table 1: Rating proposed cross-border use cases

Use case	Interoperability	Inclusion	Public value	Scalability
Cross border mobile money*	🟢/ 5	🟢/ 5	🟢/5	🟢/ 5
EAPS* (East African Payments System)	🟡/3	🔴/2	🟢/ 5	🟢/ 5
TLIP (Trade Logistics Information Pipeline)	🟢/ 5	🟡/3	🟢/5	🟢/ 5
MRPQ** (Mutual Recognition of Professional Qualifications)	🟢/ 5	🔴/1	🟡/3	🟡/3
EAIDSNet (East Africa Integrated Disease Surveillance Network)	🟢/4	🟡/2	🟢/5	🟢/4
Portable individual health records****	🟡/ 3	🟡/ 3	🟢/4	🟢/5

Rating: 🔴 Low / 0 - 1. 🟡 Medium / 2 - 3. 🟢 High / 4 - 5

*Mature and scaled **Early adoption *** Pilot stage **** Ideas/concept stage

Source: ECDPM Authors

6.1. Use case 1: East African Payment System (EAPS)

Box 9: Summary on EAPS

Short description: Developed by EAC central banks to address inefficiencies in cross-border trade and financial flows; currently used by 4 of 8 Partner States.

Impact: Strengthens regional economic sovereignty by reducing reliance on external currencies and correspondent banks, while serving as a digital payments corridor for high-value transactions.

Scalability and sustainability: Cross Border Payments Masterplan seeks to expand EAPS through hard currency settlement, governance and technical reforms, and the introduction of retail/low value systems to complement existing infrastructure.

Safeguards check:

- **Interoperability and extensibility**: Limited to commercial banks. Not interoperable between banks and MMOs. Not available 24/7 (Aloo, 2024).
- **Inclusion and non-discrimination**: Not suitable for low-value transactions. Excludes micro-enterprises, women, and marginalised communities without bank accounts. Absence of regional switch keeps costs high (Quenum, 2025; Trademark Africa, 2025).
- **Transparency, accountability and oversight**: Central banks provide oversight.
- **Privacy, security and protection**: Some EAPS Partner States have data protection laws safeguarding transactional data.

Source: ECDPM authors

In 2013, the East African Monetary Union Protocol laid the groundwork for **deeper financial and economic integration** in the EAC. To support this, regional central banks developed the East African Payment System (EAPS) to ease cross-border trade and financial flows. Previously, payments were routed through foreign correspondent banks, incurring high fees, delays and liquidity challenges. Transactions relied on foreign currencies, mainly the US dollar, which required double conversions and thus exposing traders to exchange rate risks and draining regional foreign currency reserves.

Impact and uptake

As a platform for wholesale payments, the EAPS system has significant public value. It strengthens the region's economic sovereignty by reducing dependence on external currencies and external correspondent banks. The system remains an important digital payments corridor for intra-regional trade.

Most government agencies rely on EAPS for cross-border payments. But overall, EAPS uptake has been slow compared to mobile money. Over a decade after its 2013 launch, only four countries use the system, Kenya, Tanzania, Uganda, and Rwanda. DRC, Burundi and South Sudan face technical barriers, while Somalia remains excluded for lacking a local currency. Many banks still prefer foreign correspondent banks, casting doubt on EAPS' relevance (Burundi Times, 2024). Meanwhile, all eight EAC states have joined or plan to join other regional payment systems such as COMESA's REPSS, SADC's TCIB or PAPSS (Interviews, 2025). But there has been a considerable uptick recently. In the EAC's 2023/2024 fiscal year, EAPS adoption grew by 40%. This growth has been attributed to a surge in intra-regional trade, which encouraged traders to adopt EAPS for convenience (Owino, 2024).

Modernising the system requires addressing the challenges faced by Burundi, South Sudan, DRC, and Somalia, which have not joined or experienced delays. The Cross-Border Payments Masterplan seeks to modernise it by creating a retail and low-value system to boost financial inclusion. Key proposals include: (1) evaluating the use of hard currencies (USD/EUR) within EAPS; and (2) studying its technical, operational, and governance challenges. This study on EAPS challenges will consider a centralised settlement system, a potential regional currency, and measures to cut costs and risks—such as fund pre-allocation, improved liquidity and exchange management, and system upgrades for speed, automation, and real-time visibility.

6.2. Use case 2: Cross-Border Mobile Money

Box 10: Summary on Cross-Border Mobile Money

Short description: Cross-border mobile money is increasingly used in the EAC for remittances, trade payments, and personal transfers, aligned with regional integration and AfCFTA.

Impact: It advances financial inclusion—especially for women and rural populations—reduces cash-related crime, supports remittances, tax and social protection payments, and business salaries. In 2024, it recorded US$649B in transactions across 459M accounts.

Scalability and sustainability: Adoption is growing, reinforced by EAC/continental integration and expanded government use for G2P and P2G transactions, embedding mobile money in the formal economy.

Safeguards check:

- **Interoperability and extensibility**: Extensible with cross-domain, near real-time payments. Guided by the EAC Cross Border Payment System Masterplan, interoperability enabled by prior private sector bilateral and multilateral agreements linking wallets and bank accounts (Vixio 2024; EAC 2024, EAB 2022).
- **Inclusion and non-discrimination**: Accessible, low-cost channels (apps, USSD, agents) for P2P, P2G, P2M transactions. P2P-focused, real time, phone based, with agent networks and low fees, though cross border costs remain high.[19]
- **Transparency, accountability and oversight**: Limited transparency via bilateral agreements; regulated under national laws.
- **Privacy, security and protection**: Data and consumer protection laws in some states; fraud prevention measures exist.

Source: ECDPM authors

Mobile money has revolutionised cross-border payments in the EAC, making them faster, easier, and safer than carrying cash. Individuals and businesses, including informal traders, use these services for sending and receiving money and remittances. This is particularly vital for remittance-dependent countries like

[19] Some statistics even show that sending money from Tanzania to Kenya costs 35% of the transaction value (compared to 30% to Uganda and 20% to Rwanda), which is far above the global average of 12.5% (Nyauntu and Shavida, 2024).

Somalia (Domingo, Arnold & Apiko, 2023, Monye & Monye, 2022, (Majid, Adbirahman and Hassan, 2017, World Bank, 2018).

The popularity of these cross-border mobile-money payments stems from the quick and seamless process: Users simply dial a short code (an Unstructured Supplementary Service Data or USSD number), follow instructions, confirm details, and the recipient instantly receives payment in their mobile wallet (Thitu, 2025). These advancements significantly boost intra-regional trade and regional economic integration within the EAC, aligning with the AfCFTA.

Impact and uptake

Mobile money has significantly increased financial inclusion, especially for unbanked individuals in rural areas and women, and has been linked to reduced crime in cash-based societies (Smires, 2025). In 2024, East Africa saw an estimated $649 billion in mobile money transactions across 459 million accounts. Governments and businesses increasingly use mobile money for social protection services and salary payments.

Previously, MMOs primarily handled domestic payments but have since established bilateral agreements for intra-EAC payments (Cook, 2018, The East African, 2020). Key players like Vodacom, Tigo, Airtel, MTN MoMo and M-Pesa have expanded partnerships, enabling real-time wallet to wallet transfers across countries such as Kenya, Rwanda, Tanzania and Uganda. The most active cross-border mobile-money corridors are: Kenya - Tanzania, Kenya - Rwanda, Kenya - Uganda, Uganda - Rwanda, and Uganda - Tanzania.

Cross-border mobile money is also expanding globally through partnerships, such as Safaricom's collaboration with Mastercard, Visa and Alipay for remittances and transactions between Kenya and China (Wainana, 2025). South Sudan receives inbound remittances from Uganda and Kenya via a partnership between MTN and Onafriq and the mGurush mobile money wallet supports outward international remittances and payments in both US dollars and South Sudanese pounds (O'Grady, 2025). Burundi is developing its cross-border capabilities, and DRC and Somalia are following similar expansion patterns.

A significant challenge to the sector's growth is the lack of a harmonised regional framework for business model principles. The recently adopted EAC Cross Border Payments Masterplan will expectedly guide Partner States on harmonisation.

Cross-border mobile money is highly sustainable and continues to grow driven by regional and continental integration efforts. Linked products further boost its adoption. Governments' increasing use of mobile money for G2P payments (e.g., social welfare) and P2G collections (e.g., taxes, fees) (like IremboGov) solidifies its role in the formal economy.

6.3. Use case 3: TLIP (Trade Logistics Information Pipeline)

Box 11: Summary on TLIP

Short description: TLIP is a pioneering initiative in the EAC to automate cross-border trade processes.

Impact: It boosts efficiency by digitising data exchange, cutting time and costs, and enhancing transparency through real-time tracking, which reduces corruption and fraud.

Scalability and sustainability: TLIP aligns with EASCT and AfCFTA to support regional integration, with the forthcoming EAC Data Governance Framework expected to harmonise trade data standards.

Safeguards check:

- **Interoperability and extensibility:** Integrated with Kenya's TradeNet and Rwanda's Single Window, but limited in other EAC states.
- **Inclusion and non-discrimination:** Supports SMEs, though women-owned and informal traders remain underrepresented.
- **Transparency, accountability and oversight:** Provides real-time tracking but lacks clarity on governance structures.

Privacy, security and protection: Complies with EAC data protection laws, though concerns remain over third-party data sharing. Using IOTA, trade documents are tokenized as Electronic Transferable Records, accessible only with verified digital identities.

Source: ECDPM authors

The Trade Logistics and Information Pipeline (TLIP) is a pioneering initiative in the EAC for automating trade processes to overcome inefficiencies like border delays, cumbersome paperwork, and lack of transparency (Tony Blair Institute, 2024). These challenges increase the cost of doing business and limit the continent's ability to fully leverage the AfCFTA. This digital solution reduces trade time and cost, improves transparency, and fosters regional economic integration by

digitising and automating trade. TLIP also promotes inclusivity by making cross-border trade accessible to sSMEs and marginalised groups.

A private sector-led innovation, TLIP was developed by Trademark Africa (TMA) with support from the Netherlands and the UK, and in partnership with IOTA. TMA secured seed funding and political buy-in from government agencies (e.g Kenya Revenue Authority (KRA), KenTrade, KEPHIS), importers and exports, as well as logistics providers. Built on the IOTA Tangle Distributed-Ledger Technology (DLT), TLIP offers scalability, interoperability, decentralisation, cost-efficiency, security, and energy efficiency. Through bilateral agreements,TLIP integrates with authorities such as the KRA and KenTrade, enabling exporters to receive permits and export declarations instantly. Consignment data and documents are easily stored, accessed and used for reports. TLIP focuses on critical EAC trade corridors such as the Northern (Mombasa-Kampala-Kigali) and Central (Dar es Salaam-Bujumbura-Kigali) Corridors.

Impact and uptake
TLIP drives economic growth and job creation by lowering trade barriers and digitising processes, which improves efficiency, transparency, and governance. It empowers SMEs and marginalized groups, supports regional integration, and provides valuable data for policy-making. By reducing paper-based systems, TLIP enhances resilience and sustainability, making it a key tool for inclusive economic development in the EAC.

TMA's collaborations with East Africa governments through the TLIP platform have significantly boosted monthly trade transactions by 29% and average transaction value by 15%, utilising electronic Single Windows, Integrated Customs Management Systems and Regional Electronic Cargo Tracking (TeVelde et al. 2024). The EAC's Single Customs Territory (SCT) facilitates goods clearance at the first point of entry (EAC SCT), with Partner States implementing National Electronic Single Windows (e.g. Kenya's KenTrade, Rwanda's eSW, Uganda's UeSW, and Tanzania's TeSWS) and Regional Electronic Cargo Tracking System (RECTS) to reduce transit times and improved transparency (WCO RECTS). Customs systems across Kenya, Uganda, Tanzania, Rwanda, and Burundi are connected via a Centralised Platform, also linking Kenya's and Tanzania's ports authorities.

TLIP marks a key step in trade digitisation within the SCT but its reliance on a centralised system raises data integrity and management risks. The absence of a

harmonised data-exchange framework in the EAC further heightens security concerns for sensitive trade data. Initially piloted in Kenya–Netherlands flower trade, TLIP streamlined supply chains and created a single source of truth for trade documents (WEF, 2025). Following the 2013 adoption of the EAC SPS Protocol, TLIP integrated a Sanitary and Phytosanitary component (SPS-IP) to share health-related data electronically, reducing paperwork and enabling interoperable communication among states (SPS-IP).

6.4. Use case 4: Mutual Recognition of Professional Qualifications (MRPQ)

Box 12: Summary on MRPQ

Short description: The EAC Common Market Protocol outlines a regional framework for recognising professional qualifications, with Mutual Recognition Agreements (MRAs) in accountancy, engineering, architecture, and veterinary medicine. Pilots like DIGEAT link credential verification to digital ID, aiming for seamless e-government services.

Impact: It accelerates skilled labour mobility by reducing delays and manual checks, builds trust in credentials, curbs rent-seeking, and helps address shortages in health, engineering, and finance.

Scalability and sustainability: Expansion of DIGEAT to more professions, alignment with the EAC Strategy for Trade in Services and AfCFTA, and continued regulatory reform, capacity-building, and standards harmonisation will drive sustainability.

Safeguards check[20]:

- **Interoperable and extensible:** Based on regional data exchange standards; designed to connect professional registries across countries and extend beyond engineering to other professions.
- **Inclusion and non-discrimination:** Must support professionals without digital IDs, using multilingual, user-friendly systems and outreach to women and rural professionals.
- **Transparency, accountability and oversight:** EAC-level frameworks and audits ensure accountability, though trust among regulators remains key.
- **Privacy, security and protection:** National data protection laws apply; safeguards include encryption, consent, audit trails, and limited data sharing. Strong cybersecurity and user rights to access/correct records are essential.

Source: ECDPM authors

[20] This use case remains an exploratory idea and the safeguards outline what the system should do to align with DPI principles.

The EAC has established Mutual Recognition Agreements (MRAs) for professions like accountancy, engineering, architecture, and veterinary medicine, providing a legal basis for cross-border practice (EAC Secretariat). Article 11 of the EAC Common Market Protocol further mandates the mutual recognition of academic qualifications. The 2023-2033 EAC Strategy for Trade in Services highlights the need for digital credentials and identification systems to modernise and streamline this recognition process (EAC Secretariat, 2023). Digital ID systems could enable seamless recognition of academic and professional qualifications across Partner States.

Currently, professionals seeking work in other EAC countries face lengthy, manual verification processes that take months or even years, undermining mobility and the benefits of the common market. A digital approach would help eliminate discrimination and non-recognition, foster regional hiring, curb reliance on unofficial intermediaries, and better harness the region's skilled workforce.

The technical foundation for MRPQ lies in linking a secure digital platform to national digital ID systems. This would allow regulators to instantly verify qualifications and licenses through home-country registries, removing paper-based requirements and reducing fraud. The DIGEAT pilot is establishing such a data exchange mechanism for engineers across Kenya, Uganda, Tanzania, Rwanda, with South Sudan to be included (EAC press release). This involves digitising records, standardising data formats, and building a secure query system. In February 2023, a draft regional regulatory framework and a prototype platform connecting the engineering boards were produced (DIGEAT).

Impact and uptake

A digital ID–enabled system for MRPQ could transform the EAC labour market, making cross-border mobility faster, cheaper, and more reliable. This would expand career opportunities for professionals, allow employers and governments to fill skills gaps with verified talent, and reduce bureaucracy and corruption, thereby strengthening governance and fostering regional integration through enhanced professional networks. Aligning with AfCFTA frameworks could establish the EAC as a continental model for digitally supported professional mobility. Recent assessments by the EAC–World Bank and IOM highlight slow progress in operationalising MRAs and a lack of standardised verification for cross-border data sharing among regulators (IOM 2023). To bridge this gap, the Digitalisation for East African Trade and Integration (DIGEAT) programme, funded by GIZ and BMZ, is piloting a secure digital data exchange mechanism for engineering

regulators, enabling them to share licenses and professional standing data (DIGEAT factsheet). The Leveraging Integration Frameworks for Trade in Services and CSOs in the EAC (LIFTED) project complements this by supporting policy reforms to reduce re-registration barriers (LIFTED factsheet). Both initiatives aim to transform MRAs from paper commitments into digitally verifiable, interoperable systems.

6.5. Use case 5: EAIDSNet (East African Integrated Disease Surveillance Network)

Box 13: Summary on EAIDSNet

Short description: EAIDSNet is a regional initiative that strengthens disease surveillance and response capabilities across EAC Partner States through digital technology, data sharing, and regional collaboration.

Impact: It has improved detection and monitoring of infectious diseases, curbed outbreaks and enhanced coordination and information sharing for faster, more effective emergency responses.

Scalability and sustainability: Long-term success depends on local ownership through training, and financial sustainability through joint support from governments, private sector and development partners.

Safeguards check:

- **Interoperability and extensibility:** Integrates with existing national systems, though differing data formats pose challenges.
- **Inclusion and non-discrimination:** Draws data from diverse sources, including healthcare facilities, laboratories, and community health workers but rural areas face digital access and skills gaps.
- **Transparency, accountability and oversight:** Oversight under the EAC Secretariat's Disease Surveillance & Control Unit with clear governance.
- **Privacy, security and protection:** Complies with data protection laws in EAC Partner States.

Source: ECDPM authors

The East Africa Integrated Disease Surveillance Network (EAIDSNet), launched in 2000, is a regional initiative within the EAC aimed at strengthening disease surveillance and response. It utilises digital technology, data sharing, and regional collaboration to improve the detection, monitoring, and control of infectious diseases and public health emergencies. Established to address challenges like malaria, tuberculosis, HIV/AIDS, Ebola and COVID-19, EAIDSNet is part of the EAC's

broader strategy to strengthen regional health systems and achieve SDG 3 (Good Health and Well-being). Through digital tools, training, and technical support, it enhances healthcare capacity while fostering cross-border collaboration and harmonised policies to better manage health threats and improve public health outcomes. Supported by organisations such as the Rockefeller Foundation, WHO, CDC, and the AU, the program builds on existing national surveillance systems such as One Health Initiative while integrating innovative technologies and collaborative frameworks for enhanced regional coordination.

Impact and uptake

Since its inception, EAIDSNet has significantly improved disease surveillance and response capabilities in the EAC region. It has enhanced detection and monitoring of infectious diseases, reducing outbreak spread, and improved coordination and information sharing among EAC member states for more timely and effective responses to health emergencies. EAIDSNet has also strengthened healthcare systems through capacity-building and advanced digital technologies, increasing regional preparedness for emerging health threats. Its impact led to the establishment of the Disease Prevention and Control Unit within the EAC Secretariat, which has successfully conducted a pandemic influenza preparedness exercise and piloted a web-based portal for linking animal and human health disease surveillance (Ope M et al, 2013).

6.6. Use case 6: Portable individual health records

Box 14: Summary on Portable Individual Health Records

Short description: Proposed EAC-wide system for portable, cross-border health records, anchored in national DHIS2 and linked to digital ID/ CRVS. Initial focus: immunisation continuity and TB treatment for mobile populations, building on EAC's COVID-19 trust framework.

Impact: Ensures continuity of care for migrants/refugees, prevents TB drug resistance, safeguards immunisation records, enhances disease control, reduces duplication, and advances regional digital identity interoperability.

Scalability and sustainability: All Partner States already use DHIS2, with sustained funding from WHO, Gavi, and Global Fund. This can be scaled incrementally, starting with high-traffic borders and priority diseases, then

extending to broader health services. Sustainability will depend on harmonising data protection laws, linking health IDs to CRVS/NDI systems, and securing regional financing.

Safeguards check:

- **Interoperable and extensible:** The system should leverage DHIS2, apply common standards such as HL7 FHIR and W3C verifiable credentials and adopt a regional trust framework (e.g., EACPass with PKI and QR verification).
- **Inclusion and non-discrimination:** Supports patients without formal ID via multiple identifiers and CRVS-linked newborn registration.
- **Transparency, accountability and oversight:** Ministries of Health issue/verify records; Data Protection Authorities provide oversight where they exist. EAC-level governance and public verification tools (as used during COVID) can reinforce transparency.
- **Privacy, security and protection:** Data minimisation, consent, encryption, audit trails. Only signed summaries cross borders. Gaps in data protection laws (e.g. Burundi, South Sudan) remains a challenge.

Source: ECDPM authors

Cross-border e-health in the EAC does not yet exist, but strong foundations are in place. All EAC Partner States use DHIS2 as their national health data backbone and get support from different stakeholders including the East African Health Research Commission (EAHRC), national Ministries of Health, CRVS authorities, Data Protection Authorities (DPAs), DHIS2 developers (University of Oslo, HISP groups), and global partners (WHO, UNICEF, Gavi, and the Global Fund) (DHIS2 Partners).

Rwanda and Somalia already demonstrate national models of portable health records through DHIS2 linked to IDs or unique identifiers (DHIS Rwanda, Somalia WHO EMRO). However, clinical systems and health information exchanges still vary across countries, and no EAC-wide mechanism for sharing patient summaries or e-prescriptions exists (Tanzania's Health Information System Guidelines, Rwanda's RHEA/OpenHIE, Kenya's HIE framework, Uganda's HIE guidelines).

The EAC Health Sector Strategic Plan III (2024-2030) mandates interoperable electronic health records anchored in CRVS-based patient identity, supported by the Regional Health Data Governance Framework (EAC, 2024). In practice, records would remain in national DHIS2 systems, with only minimal, digitally signed

summaries (e.g. vaccination status, treatment cards) crossing borders. Verified against an EAC trust list, similar to EACPass, these ensure continuity of care without centralising data or exposing full records, and can be validated at borders or by accredited providers across the region.

Impact and uptake

Models like EACPass and the Regional Electronic Cargo and Driver Tracking System (RECDTS) already show the impact and uptake of regional health credentials in the EAC. These models were successfully used during COVID-19. These initiatives demonstrate that public key infrastructure (PKI) based trust frameworks can support mutual recognition of digital health credentials across Partner States (EEAS RECDTS). Building on these foundations, implementation would be incremental, starting with immunisation and TB records at high-traffic border posts, then expanding to maternal health, HIV, and non-communicable diseases. The region can build on a trust framework for cross-border digital health credentials during COVID-19 (EEAS RECDTS). As EAC's cross-border data flow framework becomes operational, it will institutionalise data sharing and sustainability, reinforcing regional health integration.

7. A roadmap for the East Africa Stack: Policy options and recommendations

Based on existing cross-border use cases and the SWOT analysis of national and regional DPI deployment, the EAC can take a number of practical steps towards developing a regional Digital Public Infrastructure.

7.1 Build regional connectivity and data infrastructure for equitable benefits

The EAC has made progress through investments in telecoms infrastructure and submarine cables but must still close connectivity gaps by expanding rural broadband and satellite access, particularly in lagging Partner States. Data centres are recognised as vital for building a local digital industry and ensuring data sovereignty in the EAC Digital Transformation Strategy. The strategy also sets a target for green data infrastructure by 2030 (EAC Digital Transformation Strategy, 2025). However, few Partner States currently host their own data centres (see section 3.1.). This underscores the need for regional facilities to meet cloud demands while upholding data residency requirements.

7.2 Develop enabling policy frameworks

a. Mandate interoperability by design

EAC countries recognise the benefits of open-source over proprietary solutions (see section 2.1.), but the transition is slowed by vendor lock-in contracts and resistance from both large and small providers. To overcome this, the EAC should adopt a clear interoperability policy requiring digital systems to be designed with regional interoperability in mind.

b. Adopt a regional DPI Blueprint

The EAC has policy frameworks such as the Cross-Border Payments Masterplan and the Data Governance Framework to promote interoperability in data and payments. National laws on data protection, sharing, and digital ID further support DPI, but differing approaches across countries highlight the need for a clear **regional DPI blueprint**. Such a blueprint would set common principles, guide engagement with partners and donors, draw on the DPI Safeguards Framework, and align with the AU and AfCFTA's continental vision.

c. Develop national DPI frameworks

Alongside the Regional DPI Blueprint, Partner States need national frameworks aligned with their National Development Plans. Rwanda expects to publish its first national DPI Blueprint in 2025, providing baseline indicators for DPI monitoring and evaluation.

d. Strengthen privacy and data protection

The EAC lacks a robust regional data protection framework. While six Partner States have national laws, Burundi and South Sudan do not. The EAC Cyber Laws Framework is inadequate as it omits individual rights, controller obligations, and processing principles. At the continental level, the AU Malabo Convention provides clearer guidance but only Rwanda has ratified it (AU Convention on Cyber Security and Personal Data Protection 2014, Musoni and Okechukwu, 2024). Effective implementation requires national adoption and the establishment of data protection authorities. Weak regional compliance undermines adequacy with trading partners like the EU. The EAC should support Burundi and South Sudan to enact laws and create baseline mechanisms, such as Data Commissioner's offices.

e. Strengthen regional capabilities on cybersecurity

The region must embed privacy-by-design and privacy-by-default in DPI, beyond passing laws. Strengthening national cyber resilience requires empowered authorities, regional CERTs, and baseline cybersecurity controls (e.g., multi-factor authentication, encryption). These should be integrated across government systems and DPI platforms.

7.3 Support the private sector

a. Develop a 'PPP for DPI' framework

EAC member states can develop an adaptive Public-Private Partnership (PPP) framework '**PPP for DPI'** to encourage experimentation and innovation within a secure environment. This framework can include a commitment to inclusive design. PPPs have enormous potential to catalyse private and public sector investment by showcasing the social and economic value of DPIs, according to the Harvard Business Review. Therefore, a '**PPP for DPI'** framework can not only accelerate DPI projects, but ensure their sustainability.

b. Prioritise local innovation

Digital solutions for the local context, developed with local talent and expertise, should be a top priority of DPI development in the EAC. Innovation should be based on how to build digital platforms and services that address real needs. EAC countries should invest in digital innovation hubs, startups, and research institutions that can use open-source building blocks to create scalable solutions for health, agriculture, logistics, and education.

c. Support DPI sandboxes

EAC countries should set up and expand national and regional DPI sandboxes. A regional sandbox is a controlled environment in which Partner States can innovate and test new DPI solutions while preparing the appropriate regulatory support. The regional DPI sandbox can be used to test cross-border interoperability, from eKYC to payments and data exchange. At present, only Kenya, Rwanda and Tanzania have digital innovation sandboxes, Kenya via its Central Bank, Rwanda through the DPI Center and Tanzania via its central bank and its Ministry of Finance. In contrast, Somalia, South Sudan and Burundi do not currently have such environments. Rwanda is offering other countries access to

its DPI Center of Excellence to experiment on DPI (Rwanda Presentation, May 2025).

d. Introduce fintech licensing passport

The EAC, in collaboration with national financial regulators and central banks, should explore the development of a regional fintech licensing passport framework to facilitate cross-border operations and digital financial integration. Such a framework would enable mutual recognition of fintech licenses issued within EAC Partner States, reducing regulatory barriers and promoting innovation, competition and interoperability across digital financial ecosystems (Mbego, 2024,Fintech News, 2025). The EAC could build on existing bilateral initiatives such as Rwanda-Ghana MOU on cross-border interoperability for fintechs to design a harmonised regional model.

7.4 Establish regional and national leadership on DPI

a. Establish a regional DPI Centre

DPI should be mainstreamed into trade, finance, health, and regional cooperation agendas through cross-sector dialogue. The EAC should establish institutional oversight for DPI, ensuring DPI Safeguards are upheld across ministries (DIAL, 2024). Clear governance roles are needed for data exchange, digital ID, and payments, with senior leaders (finance ministers, central bankers, ICT ministers) aligning on digital priorities and structural reforms (Interview, 2025). Rwanda's DPI Center already serves as a model for peer learning. An EAC Centre of Excellence could scale this role, supporting capacity building, coordination, and external partnerships.

b. Ensure coordination and collaboration at national level

There is a need for inter-ministerial DPI taskforces to promote collaboration and coordination (including communication and joint planning). Coordination should be framed as horizontal, not as one ministry or authority dominating others. Some EAC Partner States have no coordination between ministries, while others indicated limited coordination in our interviews.

c. *Create a regional DPI working group*

While the EAC has been consistent in hosting DPI Leaders Forums, a more effective approach would be to set up a regional DPI working group. The purpose of the working group would be to support the EAC and Partner States in developing common standards for digital ID, payments and data exchange in alignment with the DPI Safeguards or GovStack or DPGA reference models. The working group could also be tasked with developing the regional DPI Blueprint. The group representatives can advise Partner States on cross-border DPI development. The group can be led by the EAC Secretariat together with members drawn from all the Partner States and representing identity authorities, central banks, ICT ministries, trade ministries and regulators. The group should also include the private sector and civil society.

d. Adopt GovStack PAERA for regional enterprise architecture

Kenya, Tanzania, Rwanda and Somalia have already adopted the GovStack Approach for national digital services. At the regional level, the EAC could adopt the GovStack Public Administration Ecosystem Reference Architecture (PAERA), which applies the "Cross-border by Default" principle. This would ensure interoperability and standardisation, advancing AU DSM objectives for seamless regional service delivery (GovStack PAERA Implementation Framework).

7.5 Ensure DPI Sustainability

a. Assess financial, environmental and social impact

EAC Partner States need sustainable DPI strategies. Financially, steady revenue streams are needed to maintain and update systems such as digital IDs, avoiding risky private-sector data access deals. Environmentally, data centres' high energy and water use must be considered. Socially, governments should assess how technologies meet community needs and potential human rights risks before deployment (Access Now, 2024).

b. DPI Monitoring

EAC Partner States should establish baseline indicators to enable consistent accountability and progress tracking of DPI initiatives. Rwanda and Kenya, which have partial monitoring mechanisms in place should share methodologies and lessons learned to inform regional standards. Meanwhile Somalia, South Sudan,

and Burundi should be supported through targeted capacity building and technical assistance, to develop and institutionalize national frameworks for DPI performance measurement.

c. Build professional digital skills and basic digital literacy

EAC Partner States should support the development of digital skills among public servants, policymakers, and innovators to ensure effective implementation and stewardship of DPI systems. There should be efforts to expand DPI access to women, youth, refugees, and rural communities through inclusive design and digital literacy programs.

d. Ensure meaningful and active involvement of civil society

Governments should engage civil society groups in a meaningful way (Access Now). CSOs can safeguard rights and accountability, acting as watchdogs against exclusion, as shown in Kenya's Huduma Namba and Uganda's Ndaga Muntu IDs (Onyango, 2025). Frameworks like the UN DPI Safeguards demonstrate how CSOs can shape rights-centred governance (Onyango, 2025).

e. Centre human rights in DPI design and development

Treating DPI as quick fixes, such as linking digital ID to financial access, risks exclusion and rights violations (Nwanta, 2020, Access Now). To serve public value, DPI must embed safeguards of equity, transparency, and accountability, ensuring systems empower rather than coerce or discriminate (DPI Safeguards Framework).

8. Conclusion

The East African Community stands at a pivotal moment in its digital transformation journey. Some Partner States have made considerable progress - both by developing national Digital Public Infrastructure and by supporting cross-border use cases like mobile money, EAPS, MRPQ, TLIP, and EAIDSNet. But the region as a whole will have to solve remaining challenges to achieve full interoperability. The EAC can build on existing foundations on its way towards an East Africa Stack. For that it will have to foster robust governance and inclusive design, and harmonise regulatory frameworks. By doing this, the EAC can use DPI to drive sustainable economic growth, deepen regional integration, and improve the lives of its citizens, ultimately serving as a model for digital transformation

across Africa. The DPI use cases identified in this report show that there has been significant progress in the regional development of DPI in some sectors, as well as real potential to scale use cases in others.

Regional DPI in the EAC must start with the realisation that the eight Partner States are not on the same level of digital development. This means that proposed solutions must be practical and adaptable by all the countries - and that some countries might need additional support to become 'DPI ready'. The development of the East Africa Stack should follow a 'DPI+' approach, which considers DPI as foundational infrastructure and does not treat it as a series of one-off projects. EAC Partner States should tailor DPI to their local realities rather than copy external models. This framing would prevent development partners and investors from offering off-the-shelf DPI solutions. A DPI approach that does not build on local successes will likely run into political and administrative headwinds given the costs of DPI systems and limited budgets. Unlocking the full potential of DPI in the EAC still requires sustained and targeted investments in infrastructure, policies and regulations, capacity building, and innovation.

Ongoing and future digital projects in the region should be rolled out with a 'DPI approach' mindset. This means that digital systems need to be **interoperable, modular, expansive, and scalable. Vendor neutrality can be ensured by open source and open standards** The EAC should ensure that principles of inclusion and safety as articulated in the DPI Safeguards Framework are also embedded in digital development. What this would entail in practice is for EAC Partner States to reform their procurement policies and rules.

Beyond implementing DPI principles at a national level, the EAC Partner States should consider **developing regional DPI platforms.** As this study has shown, there are several DPI use cases which are serving or have the potential to serve the social and economic needs of the entire region. These use cases support the development of **shared digital public goods,** including federated Partner States ID systems, payment switches, and data exchange layers that enable cross-border DPI platforms for mobility, trade, and cross-jurisdictional services. For countries like South Sudan which have not yet started building national ID systems, a regional interoperability mindset ensures that from the get go the country can adopt open standards and modular architecture for digital IDs that can be recognised across the region.

Similar to physical infrastructure like roads and rails, DPI systems require regular maintenance. Procurement managers must factor in updates and add-ons to ensure sustainability. Procurement processes and technical specifications should give preference to open applications that prevent vendor lock-in and encourage more robust security standards. This DPI thinking should also inform and shape how EAC Partner States engage with development partners and private donors. While these actors may have an interest in one pillar or the other DPI enablers, a systemic DPI thinking will ensure that such 'standalone' projects align with the region's own DPI framing.

Annexes

Burundi

Burundi's Digital Public Infrastructure is still at an early stage, but gradual progress is visible across the main pillars. The government is developing biometric national identity cards and strengthening civil registration to provide citizens with secure credentials. In payments, mobile money services such as Lumicash and Ecocash are used, while the central bank is advancing B-Switch to connect banks and prepare for regional integration with Rwanda and Tanzania. Early e-government platforms for taxation, migration and procurement signal a growing focus on digital public services. Progress remains uneven, constrained by high internet costs, weak data protection and low digital skills. Even so, the World Bank-backed Digital Foundations Project has added momentum to efforts to build a more integrated DPI framework that can support inclusion and regional integration.

Foundational DPI Layers

Identity: No national digital ID yet. The Ministry of Interior announced biometric ID cards by 2025, after earlier stalled attempts. Existing biometric IDs include Driving Licenses (2017) and EAC e-passports (2017), supported by Government Service Centres (GUP).

Payments: Mobile money drives inclusion but remains nascent overall. EcoCash (2011) and LumiCash (2017) dominate. However, B-Switch, the national payment switch (2021), links banks and is one of only three in the EAC.

Data Exchange: No national data exchange layer. Existing use cases include DHIS2 in health and financial services APIs.

Sectoral DPI applications

E-government: Fragmented services, no single portal. Ranked 183 out of 193 on UN EGDI (2024, score 0.2481). Burundi is prioritising the digitisation of public services, with a national committee and a Master Plan for Digitisation of Public Services (PDDSP 2023–2033).

Health: Most advanced sector. Platforms: DHIS2, OpenClinic, SidaInfo. Partnerships: UNDP–eGov Foundation, GSMA & Pathfinder (mobile maternal care), iCOHS.

Education: Limited digital adoption. Initiatives: Burundi Education & Research Network (BERNET), NKINGIRA project, National ICT Development Plan (PNDTIC).

Agriculture: Digital uptake remains low. Project example: Good Agricultural Practices for All (GAP4A).

Finance: PayWay (payments aggregator), AuxFin (UMVA e-banking, payments, remittances for rural farmers).

E-commerce: Nascent. Barriers include low user trust, weak infrastructure, high device costs and logistics constraints.

Tech enablers	
Energy	- Only ~12% of the population has access to electricity (2023). - Access is uneven: ~63% in urban areas vs. ~2% in rural areas.
Connectivity	- *Urban*: High-speed internet is concentrated in cities, but overall speeds are among the lowest globally. - *Rural*: Vast areas (84% of population) face either no internet or only slow 2G/EDGE; most online services remain inaccessible. - Burundi's investment in Wananchi Telecom in Tanzania aims to facilitate regional access to submarine cables, but costs remain high.
Device ownership	- 8 million mobile connections in January 2025 (56.6% of population). - Mostly 2G/3G. - Only ~1% of households own a computer. - Smartphone affordability is a major barrier: the cheapest device (~$52) costs 221% of the average monthly income.
Data centres and cloud uptake	- 2 small data centres: Smart Burundi, Burundi Backbone System. - No carrier-neutral facilities.

Non-tech enablers	
Oversight and accountability	- Ministry of Communication, Information Technologies and Media (MINOCTIM) - Burundi Agency for Regulation and Control of Telecommunications (ACRT) - National Communication Council (CNC) - SETIC (Secrétariat Exécutif des TIC – UGP) - Note: limited civil society role; CIPESA is active at the regional level
Legal framework	- No comprehensive data protection law; no privacy or cross-border data safeguards - work ongoing - Cybercrime laws: Law N°1/10 (2022) on Cybercriminality; Penal Code Act No.1/95 (2009) provisions

	- National Cybersecurity Strategy under development
Digital skills and literacy	- Low digital skills remain a core challenge. Planned initiatives: - National telecenters project - Tech as a Driver of Women's Economic Opportunity in Burundi (EIF/ITU/EQUALS) - Burudigi Project: hubs, digital & entrepreneurship training, startup support.

Part 2. Stakeholder mapping

Government	- Ministry of Communication, Information Technologies and Media (MINOCTIM) - Ministry of Health (leads on sectoral digitisation) - Secrétariat Exécutif des TIC (SETIC – UGP)
Regulators	- National Communication Council (CNC) - Burundi Agency for Regulation and Control of Telecommunications (ACRT)
Tech providers (companies and tech community)	- Mobile money: Ecocash and Lumicash together account for nearly 99% of the mobile money users in the country. - Telcos: Econet (PanAfrican) and Lumitel (owned by a Vietnamese company)
Development partners/ investors	- World Bank (Burundi Digital Foundations Project) - EU (EU-funded "Digital solutions to strengthen resilience of education & health systems") - UNDP/Joint SDG Fund (Country programme to strengthen SDG financing architecture. - UNCDF (Migrant Money programme: Burundi Payment Infrastructure & Remittance Policy diagnostics, 2025) - UNICEF (CRVS/digital birth registration interoperability pilots, 2024–2025) - AfDB (Africa Digital Financial Inclusion Facility—ADFI; AfDB ICT/digital connectivity support. - Enabel (digitisation of health services; ongoing cooperation portfolio in Burundi)
Advocates (civil society, researchers)	- CIPESA (regional), Association for Progressive Communications (global), etc.

Part 3. DPI in Burundi: Performance and potential (SWOT analysis)

Strengths	**Weaknesses**
- Government adoption of a 10-year Master Plan for the Digitisation of Public Services (2023–2033) - International development support (World Bank, EU, AfDB, UNDP/UNCDF, UNICEF, Enabel, Smart Africa Alliance) - Launch of several e-government platforms (migration.gov.bi, umutangakori.obr.gov.bi, isoko.gov.bi, online tax and business registration services)	- Regulatory frameworks are largely missing or severely delayed. - Systemically unreliable electricity, disrupting connectivity and digital service delivery. - Broadband penetration is low; networks are mostly 2G/3G, with limited 4G, and costs are high. - Most people outside main cities lack affordable internet access. - Funding constraints - Human capital gap: very few ICT professionals in public institutions; low digital literacy in the wider population. - Isolated ICT systems developed by ministries/donors without coordination.
Opportunities	**Risks**
- Regional integration via EAC: cross-border payments, trade/customs digitisation, mutual recognition of digital ID, harmonised standards. - Shared infrastructure investments: data centres, fibre extensions, One Network Area, cybersecurity frameworks. - Capacity building and knowledge sharing through EAC, Smart Africa and AU. - Open-source DPI platforms: sovereignty, cost-efficiency, donor alignment, local ecosystem building.	- Mismatch in digital maturity with neighbours makes regional integration challenging. - Potential conflicts between national and regional DPI frameworks. - Sustainability risks: heavy donor reliance, limited government budget. - Macroeconomic fragility: fiscal space and debt stress are slowing ICT investment.

Part 4: Recommendations

1. **Accelerate the development and adoption of core regulatory frameworks** (data protection, cybersecurity, interoperability, digital ID governance) to provide a trusted legal foundation for DPI.
2. **Prioritise greenfield DPI investments** in identity, payments, and interoperability, while modernising existing systems (CRVS, tax, health).
3. **Strengthen digital skills and human capital** by integrating ICT training into education, investing in civil service capacity, and building a local ICT ecosystem.

4. **Promote open-source, interoperable solutions to reduce reliance** on proprietary systems and support local developers.

Democratic Republic of Congo (DRC)

The Democratic Republic of Congo's Digital Public Infrastructure is still taking shape, with uneven but increasingly structured progress. The government has set out its ambitions in the Horizon 2025 strategy and created a dedicated digital development agency (Agence de développement du numérique - ADN) alongside new institutions under the 2023 Digital Code. A national digital ID is not yet operational, but is being tested for verifying diplomas and work credentials. Payments are more advanced, with over 48 million mobile wallets and a national switch under implementation to connect banks and integrate with regional systems. E-government services such as e-Visa, tax filing and the SEGUCE single service hub for external commerce are in place, supported by both public and private data centres. Yet coverage gaps, a fragile backbone network and low digital skills continue to slow expansion, while financial inclusion remains limited. With strong donor backing and growing regional engagement through the EAC, DRC now has an opportunity to turn institutional foundations into an integrated DPI framework that improves access, trust and inclusion.

Foundational DPI Layers

Identity: No national digital ID yet. The government is preparing DRCPass, a public–private partnership intended to complement physical IDs under the National Digital Identification System (SNIN) managed by Office national d'identification de la population (ONIP). Horizon 2025 sets digital ID as a priority, with pilots on diploma verification and SIM/tax credentials. Corruption allegations had led to the cancellation of previous initiatives. ADN (2022) and the entities created through the Digital Code (2023) are being put in place.

Payments: Mobile money is widespread with ~48m wallets. Vodacom M-Pesa, Airtel Money and Orange Money dominate. A national switch is under implementation to link banks, cards and wallets, with regional REPSS/SIRESS connections planned.

Data Exchange: No government-wide layer yet, but limited interoperability exists. Authorities are considering a GovStack approach with base registries and API gateways.

Sectoral DPI applications

E-government: Early services exist but are fragmented. Platforms include e-visa, online tax filing (DGI e-NIF, télé-déclaration) and SEGUCE trade single window. Authorities consider GovStack to guide design and avoid silos.

Health: Most mature use case. DHIS2 has been used nationwide since 2013-2014. Partnerships such as Flowminder–MoH use mobile data for vaccination planning and mobility estimates.

Education: A new initiative to curb diploma fraud is inspired by Benin's verification model.

Trade & commerce: SEGUCE facilitates customs and trade. Merchant base (~49,350) and POS network expanding, but cash remains dominant.

Finance: Mobile money is dominant with M-Pesa, Airtel Money and Orange Money. National Switch is under implementation to connect banks and wallets.

E-commerce: Still nascent, with low trust, affordability barriers and weak logistics limiting uptake.

Tech enablers	
Energy	- Electricity access at 55% (2024, official). - Urban–rural disparities remain significant.
Connectivity	- Mobile penetration: 67%; internet: 34%. - Coverage: 2G 75%, 3G 55%, 4G 45%. - National fibre backbone (50,000 km) is only 23% complete.
Device ownership	- 2G phones remain dominant (~65%). - Smartphone penetration ~30%. - Affordability barriers persist.
Data centres and cloud uptake	- Public DCs in use (BCC, DGI, DGDA, SEGUCE). - Private Tier III DCs operational in Kinshasa (OADC/TEXAF, Raxio).

Non-tech enablers	
Oversight and accountability	- Ministry of Posts, Telecommunications & Digital (policy) - Agence pour le développement du numérique (ADN – 2022) - Banque Centrale du Congo (payments) - ARN, APD, ANCY, ANCE (trust bodies)
Legal framework	- Digital Code (2023) establishes data protection, cybersecurity and digital transactions. - National Cybersecurity Strategy was adopted in 2023.

Digital skills and literacy	- Digital capacity building is a Horizon 2025 priority, but no official data on digital literacy. - Capacity gaps remain across government and schools. - KPI reports published in 2019, 2022 and 2024 to track progress.

Part 2. Stakeholder mapping

Government	- Ministry of Posts, Telecommunications & Digital leads DPI policy. - Agence pour le Développement du Numérique (ADN, 2022) drives implementation. - Central Bank of Congo (BCC) oversees national payment system. - Sector ministries (Health, Finance) are active in digital health and tax digitalisation (DGI e-NIF).
Regulators	- Established under the Digital Code (2023): ARN (digital regulator), APD (data protection authority), ANCY (cybersecurity agency), ANCE (e-certification authority). - Operationalisation is ongoing.
Industries	- 4 major mobile network operators (~68m subscriptions), - ~40 internet service providers (~33m subs - 9 backbone fibre operators. - Mobile money is dominated by Vodacom M-Pesa, Airtel Money and Orange Money. - Banking sector includes 15 commercial banks, 35 aggregators, and 109 IMF/COOPEC.
Tech providers (companies and tech community)	- Carrier-neutral Tier III data centres operated by OADC/TEXAF and Raxio in Kinshasa. - Smaller local providers include metro fibre operators in urban areas. - The emerging local tech community is active in fintech and e-commerce, but still fragmented.
Development partners/investors	- World Bank (IDEA/DRC, $400m IDA), AFD, UNICEF, Enabel, UNCDF and other donors support digital ID, connectivity, financial inclusion and service delivery. - Regional initiatives include EAC's shared data centres and the integration of REPSS/SIRESS payments.
Advocates (civil society, researchers)	- Rudi International supports digital rights alongside regional civil society groups such as CIPESA. - Flowminder: non-profit research partner providing mobility analytics for health planning.

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- National Digital Plan *Horizon 2025* gives a clear DPI orientation. - Digital Code (2023) created trust institutions (ARN, APD, ANCY, ANCE). - ADN (2022) was established as a digital development agency. - Large mobile money ecosystem (~48m wallets, 860k agents). - Public and private Tier III data centres are operational. - Significant donor support (World Bank IDEA/DRC, AFD, UNICEF, UNCDF, Enabel).	- No operational national digital ID; foundational registries are incomplete. - National Switch not yet live; interoperability still limited. - Backbone deficit: only 23% of the 50,000 km fibre target built. - Broadband penetration is low; 4G coverage is only 45%, mostly in urban areas. - Internet affordability remains a barrier; smartphone affordability is only ~30%. - Weak digital literacy and a shortage of ICT professionals in government. - Institutions under Digital Code are not yet fully operational (boards, budgets).
Opportunities	**Risks**
- Use GovStack to standardise e-government modules and registries. - Regional integration via REPSS/SIRESS and EAC shared data centres. - Leverage Flowminder and MNO data to fill census/statistics gaps. - Growing youth and start-up ecosystem in Kinshasa and provincial hubs. - Public and private data centres can host local content and services.	- Urban–rural digital divide deepening with uneven connectivity. - High deployment costs for energy, fibre and devices. - Risks of cybersecurity breaches, fraud, and weak data protection enforcement. - Persistent political instability and conflict are undermining investment. - Over-dependence on donors for digital projects; fragmented initiatives.

Part 4: Recommendations

1. Finalise operationalisation of ADN and trust institutions (ARN, APD, ANCY, ANCE) to ensure governance and oversight of DPI.
2. Complete rollout of National Switch and enforce interoperability across banks, wallets, and cards.
3. Prioritise foundational registries and sequence digital ID development through high-value use cases (diplomas, SIM, tax) with privacy safeguards.

4. Strengthen procurement and contracting in the ID sector to prevent corruption and ensure transparent, competitive processes.
5. Accelerate backbone fibre expansion and extend 4G coverage beyond urban centres, leveraging Universal Service Fund and regional integration projects.
6. Invest in digital skills by integrating ICT training in schools, strengthening government capacity, and supporting local tech communities.
7. Promote open standards and GovStack-aligned approaches to avoid siloed systems and donor-driven fragmentation.

Kenya

Kenya has made significant strides in establishing a foundational Digital Public Infrastructure stack, leveraging systems such as M-Pesa (mobile payments), Maisha Namba (digital ID), and eCitizen (data exchange). The country's broader strategy is outlined in a new roadmap focused on interoperability and standards; innovation and economic growth; inclusivity and sustainability; trust, security and privacy; and sustainable implementation. Kenya's DPI roadmap was developed by the Ministry of Information, Communications and the Digital Economy with support from international development partners such as the ITU and GIZ.

Foundational DPI Layers

M-Pesa: The mobile payments system, M-PESA, is currently available in more than 170 countries globally, serving over 70 million customers.

Maisha Namba: Maisha Namba is defined as a unique personal identification number assigned to every Kenyan citizen upon registration, typically at birth. This number will be a lifelong personal identity number from birth to death.

eCitizen: eCitizen is Kenya's unified government portal offering over 22,000 services from more than 100 government entities, including passport applications, police clearance, and tax services.

Sectoral DPI applications

E-government:	eCitizen
Health:	TaifaCare, AfyaYangu
Education:	NEMIS, DLP, Kenya Education Cloud
Agriculture:	KAOP, e-Voucher, UjuziKilimo, Agri-Wallet
Finance:	M-Pesa, PesaLink
E-commerce:	Arifu

Tech enablers	
Energy	- 67% rural, 100% urban (2023) - 79% total electrification (2023) - energy mix: 90% renewable (2023)
Connectivity	- 4G coverage at 98% (2025) - 3G coverage at 99% (2025)

	- broadband penetration: 80% mobile, 4.5% fixed (2025)
Device ownership	- mobile phone penetration 131.5% - smartphone penetration 72.6% - feature phone penetration 59.6%
Data centres and cloud uptake	- 15 data centres, 10 in Nairobi - iXAfrica, NXTRA/ Airtel, EcoCloud/ G42 under construction - Cloud use is growing in e-gov, finance, health, and education

Non-tech enablers	
Oversight and accountability	- Ministry of Information, Communication & the Digital Economy (MICDE) - ICT Authority (ICTA) - Office of the Data Protection Commissioner (ODPC)
Legal framework	- Computer Misuse & Cybercrimes Act (2018) - Data Protection Act (2019) - National AI Strategy 2025 - 2030
Digital skills and literacy	- Kenya School of Government (KSG), Smart Government Initiative - Digital Literacy Program (DLP) for public schools, Ajira Digital Programme for youth, Jitume, Tujifunze Digital Literacy Initiative for women and informal sector, Women in Tech (Safaricom, KEPSA, UN Women), Konza Technopolis Digital Skills Academy - Huduma Centres, Digital Innovation Hubs (ICT Authority) - Grow with Google, Huawei ICT Academy, Microsoft Skills for Jobs

Part 2. Stakeholder mapping

Government	- Ministry of Information, Communication & Digital Economy (MICDE) - ICT Authority - Smart Government - eCitizen Directorate
Regulators	- Central Bank of Kenya - National Identification Authority (NIDA)

	- Office of the Data Protection Commissioner (ODPC)
Tech providers (companies and tech community)	- Financial & business services: robust banking, insurance and fintech sectors - ICT & digital services: Silicon Savannah, Fintech innovations (M-PESA, Tala, M-KOPA, Pesapal) - Telcos (Safaricom, Airtel) - AI Startups (Apollo Agriculture, Fastagger, Sama)
Development partners/ investors	- World Bank, IMF, AfDB, KfW, IFC - EU, GIZ, - UNDP - Gates Foundation
Advocates (civil society, researchers)	- KICTANet, CIPIT, CIPESA

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- Robust foundational DPI stack - Government commitment to digital transformation - Increasing broadband connection - Strong mobile money ecosystem - Data protection laws were enacted	- Rural digital divide remains stark - Cybersecurity vulnerabilities - ICT skills gap in public institutions - Data privacy concerns
Opportunities	**Risks**
- AI strategy could boost innovation - Leveraging on big data & AI - Expanding e-commerce - Strengthening regional integration	- Cybersecurity risks are increasing with digitisation - Resistance from legacy bureaucratic systems - Regulatory catch-up with tech innovation - Gender and rural-urban disparities in access

Part 4: Recommendations

1. Increase DPI funding through public-private partnerships (PPP) and budgetary allocation.
2. Promote digital literacy and skills development.
3. Foster innovation in digital services and the data economy.
4. Enhance collaboration between the government, the private sector, and civil society.
5. Expand rural broadband access and digital inclusion programs.

Rwanda

Rwanda has made significant strides in establishing a foundational Digital Public Infrastructure stack through systems such as mobile money platforms, Irembo (a digital services platform), and a national digital ID program. The country's broader strategy is outlined in the National Strategy for Transformation (NST1) and Smart Rwanda Master Plan. These strategies focus on digital literacy and skills; cybersecurity and data protection; digital inclusion and accessibility; e-government and service delivery; and private sector engagement. Rwanda's DPI initiatives are spearheaded by the Ministry of ICT and Innovation with support from international development partners such as the World Bank, GIZ, Gates Foundation and CoDevelop.

Foundational DPI Layers

R-Switch: R-Switch is the national e-payments switch of Rwanda and driver of the Smartcash brand, which enables electronic payment settlements, interoperability and other financial services.

Single Digital ID: Rwanda launched its single digital ID system, the Rwandan National Identity System (RNIS). The system provides a unified digital identity for citizens, refugees, and foreign residents. It incorporates biometric data like fingerprints and iris scans.

iRembo: iRembo, Rwanda's eGovernment platform, has digitised 100 public services, making it easier for over 8 million Rwandans and foreigners to access them.

Sectoral DPI applications

E-gov: iRembo

Health: Rwanda Health Information Management System (RHIMS)

Education: Rwanda Digital Schools Project

Agriculture: Smart Nkunganire System (SNS), FDiVi Project

Finance: Airtel Money, MTN Momo, EKash

E-commerce: iHuzo Initiative

Tech enablers	
Energy	- 74% total electrification (2024) - energy mix: 53% renewable (2024)
Connectivity	- 4G coverage at 95% (2025) - 3G coverage at 97% (2025)

Device ownership	- mobile phone penetration 73.4% - smartphone penetration 72.6% - feature phone penetration 59.6%
Data centres and cloud uptake	- Africa Data Centres (ADC), PAIX Kigali, AOS Ltd, TrAC Kigali

Non-tech enablers	
Legal framework	- The Smart Rwanda Master Plan 2 (2024-2029) - ICT Sector Strategic Plan (SSP) - Rwanda National AI Policy (2023) - Rwanda eCommerce Policy (ongoing) - Data Protection Law (2021) - National Cybersecurity Policy (2022) - Cyber Crime Law (2018) - ICT Law (2016)
Digital skills and literacy	- Digital Ambassadors Program (DAP), Community Digital Centers (CDC), One Laptop Per Child (OLPC), Smart Classrooms - Smart Africa Digital Academy (SADA), Rwanda ICT Chamber - Digital Acceleration Project (World Bank) - Girls in ICT Rwanda Initiative, Ms Geek Rwanda, Rwanda Coding Academy

Part 2. Stakeholder mapping

Government	- Ministry of Information Communication, Technology & Innovation (MINICT) - National Cyber Security Authority (NCSA) - Rwanda Information Society Authority (RISA) - DPI Centre of Excellence
Regulators	- National Bank of Rwanda - National Identification Agency (NIDA) - Rwanda Data Protection Office (RDPO)
Tech providers (companies and tech community)	- ICT & digital services: IremoboGov and Smart Africa - Financial & business services: Kigali International Finance CenterFintechs (AgriGO, JUMO) - Telcos (MTN, Airtel) - AI Startups (CircuitNotion, HyperLink Digital System, WiredIn, eVolve)
Development partners/ investors	- World Bank, IMF, AfDB, KfW, IFC

	- EU, GIZ, ITU - UNDP, Mastercard Foundation - Gates Foundation, CoDevelop
Advocates (civil society, researchers)	- FSD Rwanda, CIPESA, Mojaloop

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- Strong government leadership and policy commitment - Well-developed digital identity and foundational DPI systems - Advanced eGovernment infrastructure and interoperability framework - Supportive institutional and innovation ecosystem, i.e., DPI Centre of Excellence - Strong data governance and protection frameworks	- Limited interoperability across legacy systems - Limited private sector integration - Urban-rural digital divide - Dependence on external technical support and funding - Capacity and skills gaps
Opportunities	**Risks**
- Regional leadership in DPI development - Expansion of digital financial services - Public-Private Partnerships for innovation - Youth and digital talent development - Data-driven governance and AI adoption	- Cybersecurity and data privacy risks - Overdependence on a few technology vendors - Regulatory catch-up with rapid technology innovation - Regulatory and institutional fragmentation - Gender and rural-urban disparities in digital access

Part 4: Recommendations

1. Leverage the DPI Centre of Excellence to strengthen regional collaboration, knowledge exchange, and standards alignment.
2. Expand digital inclusion by targeting rural areas, women, refugees, and marginalised groups with affordable access and services.
3. Enhance digital skills through workforce-focused programmes that prepare youth and public servants for an AI-driven economy.
4. Strengthen cybersecurity by investing in national capacity, regulatory enforcement, and cross-border threat intelligence sharing.
5. Foster innovation by supporting digital entrepreneurship, scaling local startups, and deepening private sector engagement in DPI.

Somalia

Somalia's Digital Public Infrastructure is still nascent but advancing. The first national biometric ID was launched in 2023, with a target of 15 million by the 2026 elections. The Somalia Instant Payment System (SIPS) began in 2025, adding real-time and QR-based transactions to widespread mobile money use and new prepaid card services. A national data integration platform is planned, but not yet interoperable. Early sectoral applications span telehealth, e-learning, agriculture and e-commerce. Progress is slowed by high energy costs, uneven rural connectivity and low digital literacy, yet new laws, backbone projects, and data protection measures provide a foundation for a more integrated and inclusive DPI.

Foundational DPI Layers

Digital ID: The National Identification and Registration Authority rolled out the first national biometric ID system in 2023. The plan is to issue 15 million biometric IDs by the 2026 elections.

Digital payments: Somalia Instant Payment Systems (SIPS) switch launched in January 2025. SIPS introduces real-time transactions and QR-based payments. Mobile money is widely used. Salaam Somali Bank and Mastercard launched a multi-currency prepaid card for global payments.

Data exchange: National integration platform still in early stages. Not fully standardised. Government databases are not yet interoperable. No national mechanisms to ensure transparency and auditability of data-sharing decisions.

Sectoral DPI applications

E-government:	Ministry of Communication and Technology is developing E-government.
Health:	Telehealth services like Hello! Caafi / SomDoctor / Baano Healthcare
Education:	Learning Passport, an e-learning platform
Agriculture:	M-Dalag Market Information System connecting farmers with input sellers.
Finance:	Nothing advanced
E-commerce:	Rikaab (for mobility and food deliveries), Gulivery (for food deliveries)

Tech enablers	
Energy	- Energy access is low, unreliable and costly. Of 15 million Somalis, 9 million lack access to electricity, and power costs are among the highest in the world.
Connectivity	- Somalia's fixed broadband infrastructure is nascent but improving. 72.7% of mobile connections in Somalia can now be considered "broadband". Connectivity in rural and remote regions is far more limited.
Device ownership	- Hormuud Telecom reports that 90% of Somalis own a mobile phone, with 70% connected to a network. SIM cards are cheaper than in neighbouring countries, making mobile access widespread.
Data centres and cloud uptake	- The government has no data centres of its own yet, but the Ministry of Communications and Technology has constructed a data centre that is expected to be operational soon.

Non-tech enablers	
Legal framework	- Data Protection Act 2023 - National Communications Law 2017 - National ICT Policy and Strategy (2019 -2024) - Identification and Registration Act - Mobile Money Regulation 2020 - ICT Regulatory Transformational Strategy and Roadmap - E-government Strategic Implementation Roadmap - Digital Inclusion Policy - National Payment System Bill - No national data, AI strategy or policy yet - An agreement with Saudi Arabia to cooperate on developing regulatory frameworks and standards. The Somali AI Summit was held in 2024 to explore how AI can transform the country's socio-economic landscape.
Digital skills and literacy	- Nothing extensive is in place yet. UNDP and the MoCT recently launched digital skills training for IT students. There are also digital skills programs designed for high school and university students.

Part 2. Stakeholder mapping

Government	- Ministry of Communication & Technology (MoCT)
Regulators	- The National Identification and Registration Authority (NIRA) - Data Protection Authority - National Communications Authority - Central Bank of Somalia
Tech providers (companies and tech community)	- Hormuud Telecom - Somtel - Golis Telecom - SomLink Telecom and eBesa
Development partners/ investors	- World Bank - IFC - EU - UK - Gulf countries - Pakistan National Database and Registration Authority (NADRA)
Advocates (civil society, researchers)	- Zamzam University - Bareedo Platform - Digital Shelter - AI Somalia Community

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- Over 4,000 kilometres of national fibre-optic backbone are under construction, improving inter-regional connectivity and government network resilience - Submarine fibre-optic cable landing stations in Mogadishu, Berbera and Bosasso serve as entry points for 2Africa, DARE1, and EASSy cables, significantly boosting international bandwidth and reducing latency and costs. - Weak legacy infrastructure allows the adoption of modern digital architectures (cloud, satellite, mobile)	- Somalia's telecom network is weak, with poor power supply, sparse rural coverage, and insecurity from Al-Shabaab deterring investment. - Internet and device costs remain high relative to incomes, leaving many Somalis undercovered but unable to connect. - Cities have strong networks, but rural areas often lack coverage, deepening the digital divide and limiting opportunities. - Oversight has improved with the new regulator, but weak enforcement, regional fragmentation, and policy gaps still hinder sector growth. - Heavy reliance on USD limits digital payments and regional integration, though a new local currency project is underway. - Limited skills and knowledge restrict many Somalis from fully participating in the digital economy.

- Licensing of satellite providers expands coverage in rural areas.	- State fragility turned telecom firms into de facto governors, forcing them to self-manage security, legitimacy, and finance in a regulatory vacuum until the state slowly re-entered the picture.
Opportunities	**Risks**
- SIPS supports standardised QR codes, which facilitate seamless regional payments - SIPS complies with ISO 20022 standards, which ensure cross-border interoperability	- Digital ID and verification systems carry risks in fragile or conflict-affected contexts, including data misuse, identity theft, and cyberattacks. - The country's broader security situation remains volatile, increasing risks to infrastructure, operations and public trust. - If connectivity and skills gaps are not addressed, DPI may widen rather than narrow inequalities. There is a risk that rural and displaced populations may continue being excluded. - Infrastructure may be vulnerable to damage in conflict zones.

Part 4: Recommendations

1. Strengthen and harmonise legal frameworks, with a focus on interoperability, cybersecurity, data protection and digital ID governance, to build trust and coherence across DPI.
2. Mobilise investment from both public and private actors to expand backbone infrastructure, lower energy costs, and operationalise national data centres
3. Scale up digital literacy and skills development through education, vocational training and civil service capacity-building, ensuring citizens and institutions can effectively use emerging DPI.
4. Develop local talent, maintenance capacity and business models for DPI so that progress is sustainable and less donor-dependent. Work with the private sector, diaspora and development partners to accelerate and scale DPI components, while retaining national ownership.
5. Enhance cybersecurity measures and awareness to safeguard new systems, such as SIPS and biometric ID, and reduce the risk of fraud and data breaches.

South Sudan

South Sudan's Digital Public Infrastructure is in its nascent stages as the world's youngest country is still setting up administrative structures to support governance, while navigating political instability, economic stagnation, and poverty (UNDP, 2024). Digital payments are slowly picking up, but the country remains predominantly cash-based due to an underdeveloped financial sector and challenges of financial inclusion. However, mobile money has been critical in enabling humanitarian organisations to replace in-kind aid with cash transfers and to reduce the security risks of moving large amounts of cash through high-risk areas of the country (UNDP, 2024). The country has also facilitated data and information exchange in the context of humanitarian aid. For example, the International Organisation for Migration (IOM) and the United Nations World Food Programme (WFP) reached an agreement to harmonise and synchronise biometric data of individuals registered in their respective systems to improve the delivery of assistance. This data-sharing mechanism is subject to robust data governance (WFP, 2019).

Foundational DPI Layers

Digital ID: National ID system remains limited, with many relying on paper nationality certificates (often with inaccurate birthdates) or lacking ID entirely, leaving refugees and returnees at risk of statelessness (Interview with South Sudan). Regulations for civil registration and ID were updated in 2024, and the World Bank is supporting digital registries, such as a biometric payroll. The priority is expanding basic ID coverage so adults can access rights and services. Long term, building a digital population register and simplifying enrollment are essential to ensure inclusion and economic participation (Biometric Update, UNHCR).

Digital payments: The Bank of South Sudan (BOSS) launched the National Instant Payments System Switch in February 2025. It is designed to enable real-time, secure and cost-effective transactions, promoting interoperability between banks, mobile-money providers and other financial institutions. Mobile money like mGurush and NilePay is available, though uptake has been low, with less than 6% of adults with mobile money accounts.

Data Exchange: The government is yet to develop a data exchange architecture. However, within the humanitarian context, an Information Sharing Protocol was developed in 2023 as a common framework for information and data exchange in the country, subject to agreed data and information sensitivity classification.

Sectoral DPI applications

E-government:	South Sudan eServices Portal (business registrations and visa applications functionalities are now live; other functionalities are not live yet).
Health:	Nothing in place yet
Education:	EDUCARE and Junub Academy as e-learning platforms
Agriculture:	e-Registry Platform launched by Ministry of Agriculture and FAO
Finance:	Nothing in place yet
E-commerce:	Dukaanye, the country's first online marketplace

Tech enablers	
Energy	- In 2023, only 5.4. - 8.4% of the population had reliable electricity access. Despite oil wealth, the country lacks refineries and relies on imported diesel, with power plants concentrated in Juba and no national grid. The government plans to expand access through a national transmission network and a large hydropower plant.
Connectivity	- As of early 2024, internet penetration reached 12.1%, with approximately 1.36 million users, reflecting a modest increase from 7.0% in 2023. Active cellular mobile connections also grew to 3.97 million, accounting for 35.5% of the population.
Device ownership	- A 2019 report says over 45 per cent of the population owns a phone in South Sudan, but this varies across locations. While 63% of urban residents own a phone, only 38% of rural residents do.
Data centres and cloud uptake	- No local data centers but there are plans by the NCA, BOSS and Ministry of Finance to build micro data centers.

Non-tech enablers	
Legal framework	- Constitution of the Republic of South Sudan (Article 22 on privacy) - BOSS Electronic Money Regulation 2017 - Civil Registry Act, 2018 - Revised National Development Strategy 2021 -2024 - Cybercrimes and Computer Misuse Provisional Order 2021 - Digital Government Strategy (draft)

	- Digital Transformation Strategy (draft) - The country has no national data protection law - The country has no strategy for data and AI
Digital skills and literacy	- MTN launched a digital skills initiative to equip communities with basic digital skills

Part 2. Stakeholder mapping

Government	- Ministry of Information, Communication Technology & Postal Services - Ministry of Trade & Industry - Ministry of Finance & Economic Planning - Ministry of Interior - Ministry of Public Service - Directorate of Civil Registry, Nationality, Passport, and Immigration (DCRNPI) (Ministry of Interior)
Regulators	- National Communications Authority (NCA) - Bank of South Sudan (BOSS) - No Data Protection Authority yet
Tech providers (companies and tech community)	- MTN - Zain - mGurush - Nilepay - Digital Telecom
Development partners/ investors	- African Development Bank - AfricaNenda Foundation - European Union - Universal Service Access Fund (USAF) - UNHCR - UNDP
Advocates (civil society, researchers)	- Koneta Hub - Internet Society South Sudan Chapter - South Sudan Internet Governance Forum - Freedom of Expression Hub

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- Actively working on improving connectivity via projects like EARDIP, with financing from World Bank, aimed at creating a single connectivity market and a single data market - Plans for national data centers in Juba can improve data sovereignty	- Limited broadband and fibre-optic coverage and higher costs of internet access make access unaffordable for most people - Low digital and financial literacy means most citizens lack the skills needed to benefit from online

and provide a foundation for digital public services - Government showing intent and commitment to adopt digital transformation and infrastructure - Diverse digital partnerships with international partners like the European Union, World Bank and African Development Bank - Most mobile money services are still free (e.g., there are no charges for sending mobile money)	services and participate in the digital economy - Absence of comprehensive legislation on data protection, consumer rights, payments, etc creates uncertainty, limits investor confidence and weakens user trust in digital systems - A fragmented policy environment undermines coherent digital transformation efforts. - The national ID system is still being developed, and most people still don't have ID documentation. There is no standalone ID authority which limits institutional independence and capacity - Low citizen awareness and limited incentives for ID registration further hinder adoption
Opportunities	**Threats / Risks**
- Underdeveloped digital infrastructure also means an opportunity for significant growth and potential for leap-frogging older legacy systems - Participation in regional initiatives can open up cross-border digital trade, connectivity and services, aligning South Sudan with larger digital markets - Growing mobile penetration and digital awareness mean opportunities for innovation, start-up ecosystems, mobile banking, remittances, etc	- Cybersecurity weaknesses, data protection gaps and weak regulation could lead to breaches, misuse of data undermining trust in public digital systems - Dependence on foreign technologies raises risks of vendor-lock-in, strategic dependencies or external political pressures - Persistent low energy/electricity supply and infrastructure fragility may lead to underutilisation and investments risk being stranded - Conflict, instability or damage to infrastructure remains a threat - Competing priorities: large investments needed for DPI, but the country faces other significant development and humanitarian needs

Part 4: Recommendations

1. **Accelerate the establishment of governance frameworks** (data protection, cybersecurity, consumer protection, and DPI coordination) to build trust and align government, private sector, and humanitarian actors.
2. **Prioritise foundational DPI investments** in digital ID, instant payments, and data exchange, while modernising civil registration and government payroll systems to ensure inclusion and service delivery.
3. **Expand energy and connectivity access** through phased national grid development, mini-grids, off-grid solar, and rural broadband rollout, supported by an independent electricity regulator and investor incentives.
4. **Strengthen digital skills and institutional capacity** across government, civil society, and the private sector, while coordinating funding and promoting inclusive, locally adapted solutions.

Tanzania

Tanzania has developed one of East Africa's most coherent and state-led digital ecosystems, guided by the Digital Economy Strategic Framework 2024–2034 and supported by a strong legal and policy foundation, including the National ICT Act, the e-Government Act of 2019, and the Data Protection Act of 2022. The country has made significant strides in establishing a foundational DPI stack — encompassing digital identity (Jamii Namba), digital payments (Jamii Pay), and data exchange (Jamii X-Change). More than 25 million citizens are registered in the national ID system, which is now linked to health and financial services. Tanzania is positioning itself as a regional leader in inclusive, standards-based digital transformation, though rural connectivity and digital skills gaps remain important challenges.

Foundational DPI Layers

Jamii Namba (Digital ID): Over 25 million registrations since 2014. Integrated with access to health, financial and social services through linkage with NIDA and the National Health Insurance Fund.

Jamii Pay (Digital Payments): National digital payments platform connecting government systems and financial institutions. Includes GePG (government e-payments), TIPS (instant interbank payments), and ZANMALIPO, supporting real-time and interoperable transactions.

Jamii X-Change (Data Exchange): National data exchange platform built on GovESB and aligned with international frameworks such as X-Road and GovStack. Enables secure data sharing across fourteen sectoral systems.

Jamii Card (Citizen Access): Citizen-facing payment tool within the Jamii Pay ecosystem, promoting cashless transactions and financial inclusion.

Sectoral DPI applications

E-government:	Tanzania e-Gov Portal, GovESB, **e-Mrejesho** (feedback system) Jamii Portal, e-Office, m-GOV, TANCIS
Health:	Digital Health Portal, Afya-Tek, Jamii ni Afya (Zanzibar), TNMCIS
Education:	Kisomo, Smart schools, e-Fahamu, Instant schools
Agriculture:	eKilimo, Mobile Kilimo, ARDS, Agri-Inputs Platform
Finance:	Selcom, Tunzaa Fintech, Jamii Africa
E-commerce:	Agrobot, e-Shangazi, draft National AI Strategy

Tech enablers	
Energy	- 84% village coverage, but only 42% population-level connection - Target: 50% renewable energy by 2030 under the DESF's "Enabling Digital Infrastructure" pillar
Connectivity	- 4G coverage projected at 26.16% by 2025 - 3G coverage projected at 85.7% - Broadband penetration: 48.5% mobile, 1.3% fixed (2021) - Dar es Salaam Port serves as a regional connectivity hub linking neighbouring countries
Device ownership	- 82.5% own mobile phones - 22.3M still on 2G - Only 29.1% use the internet
Data centres and cloud uptake	- 9 data centres, mostly Dar es Salaam - Cloud use is growing in e-gov, health, and education - Raxio Tier III Data Centre launching in 2025

Non-tech enablers	
Legal framework	- National ICT Act - e-Government Act (2019) - Data Protection Act (2022) - Data Processing Regulations (2023) - Cybercrime Act (2015) and National Cybersecurity Strategy (2022) - National Interoperability and Standardisation Framework - Tanzania ICT Governance and M&E Frameworks
Digital skills and literacy	- dLab and DA4TI: digital literacy and advocacy - Ie-GovRIDC and RAFIC – ICT capacity building for civil servants - Digital Literacy and Skills Development (core pillar of DESF 2024–2034)

Part 2. Stakeholder mapping

Government	- Ministry of Information, Communication & ICT (MICIT) - Tanzania e-Government Authority (eGA)
Regulators	- e-Government Authority (eGA) – central DPI coordinator - Bank of Tanzania manages FinTech Regulatory Sandbox and digital payments oversight - Cloud computing guidelines & fintech sandbox - National Identification Authority (NIDA): - Personal Data Protection Commission (PDPC)
Industries	- Digital finance: Selcom, NALA, Tunzaa, Jamii Platforms - Telecommunications: Vodacom, Airtel, Tigo, Halotel, TTCL - Health: Afya-Tek, Jamii ni Afya, NHIF - Agriculture: eKilimo, Agri-Inputs Platform, Mobile Kilimo - Education: Smart Schools, e-Fahamu, Instant Schools - Data and cloud services: Raxio, Raha, TTCL Data Centre
Tech providers (companies and tech community)	- Fintechs (Selcom, Tunzaa) - Telcos (Vodacom, mobile operators) - AI Startups (Parrot AI, Agrobot) - Cloud and data providers (Raxio, TTCL, Raha)
Development partners/ investors	- World Bank (Digital Tanzania Project) - EU (eGovernance Support) - UNDP (Joint SDG Fund) - Gates Foundation, PATH, African Development Bank (AfDB)
Advocates (civil society, researchers)	- dLab (University of Dar es Salaam) - DA4TI (Digital Access for Transformation Initiative) - Policy think tanks and advocacy groups working on digital inclusion and data governance

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- Robust foundational DPI stack (ID, payments, data exchange) - Strong government ownership (eGA, MICIT, BoT) - Active digital health and education platforms - Fintech ecosystem is growing rapidly - Data protection and cybersecurity frameworks enacted - Adoption of international standards (X-Road, GovStack, DEPA)	- Persistent rural connectivity and affordability gaps - Limited cloud adoption outside Dar es Salaam - ICT skills gap in public institutions - Persistent 2G reliance and low internet use - Uneven implementation capacity across agencies
Opportunities	**Risks**
- Digital Economy Strategic Framework 2024–2034, guiding coordinated DPI growth - AI strategy could boost innovation in AgriTech and health - International partnerships (EU, WB, UNDP, Gates Foundation) - Data centers expanding capacity (Raxio, TTCL) - Inclusive digital skills programs (e.g., dLab, RAFIC) - Potential for regional data exchange and EAC interoperability	- Cybersecurity risks are increasing with digitisation - Resistance from legacy bureaucratic systems - Regulatory catch-up with tech innovation - Gender and rural-urban disparities in access - Implementation delays between policy and rollout

Part 4: Recommendations

1. Expand rural connectivity and device access by leveraging Universal Service Funds, PPPs, and affordable handset schemes to close the 2G–4G divide.
2. Strengthen DPI governance and coordination under the Digital Economy Strategic Framework 2024–2034 by aligning oversight across identity, payments, data protection, and data exchange.
3. Deepen trust in digital systems through full implementation of data protection and interoperability frameworks.
4. Invest in digital skills and innovation by scaling ICT training for civil servants, youth, and entrepreneurs, while supporting fintech, AI, and data-driven startups.

Uganda

Uganda's Digital Public Infrastructure is anchored in the Digital Transformation Roadmap (2023/24–2027/28) and led by the National Information Technology Authority (NITA-U). The national ID (*Ndaga Muntu*) launched in 2014 covers over 98% of adults, with a major renewal drive underway. The upgraded system adds iris recognition, civil registration links and MOSIP integration and is set to connect with a forthcoming UPI-style payment switch. The Bank of Uganda is also upgrading Real Time Gross Settlement (RTGS) to align with the ISO 20022 international standard, while a feasibility study for Central Bank Digital Currency (CBDC) has been completed. Data exchange across government institutions is facilitated through the UG Hub, which enables secure information sharing for services such as KYC verification, tax administration and mobile money. UG Hub also supports shared services such as UGPASS, IFMIS, e-Procurement and HCM. National connectivity continues to expand under NBI Phase 5 and the World Bank–backed UDAP-GovNet initiative, which are extending fibre infrastructure, rural broadband coverage and public Wi-Fi access across the country. Persistent gaps remain in internet access, electricity, digital skills and regulation, but with strong donor backing and regional integration, Uganda is emerging as a leader in interoperable DPI in East Africa.

Foundational DPI Layers

Identity: The national ID (*Ndaga Muntu*), launched in 2014, covers over 98% of adults. A 2025 renewal adds iris biometrics, MOSIP integration and future UPI linkage. A court case raised exclusion risks, but the rollout continues.

Payments: Bank of Uganda is preparing a UPI-style national switch (pending approval) and upgrading RTGS to ISO 20022. Mobile money dominates, and a CBDC feasibility study is complete.

Data Exchange: UG Hub underpins KYC, tax and mobile money, alongside UGPASS, IFMIS, e-Procurement and HCM. Integration is domestic only, with no cross-border functionality.

Sectoral DPI applications

E-government: Shared services consolidated under NITA-U include UG Hub, UGPASS, IFMIS, e-Procurement, HCM and a Citizen Portal. About 43% of services are online and 60% integrated, hosted in the National Data Centre.

Health: Most advanced sector. DHIS2 is used nationwide for health reporting. Policy discussions underway to link health data with digital ID and explore regional interoperability.

Education: Limited dedicated platforms. Schools and universities connect through UG Hub and backbone expansion projects, but digital adoption remains uneven.

Agriculture: Digital uptake is low. No large-scale platforms reported, though pilots exist within connectivity and data initiatives.

Finance: Mobile money drives financial inclusion. Bank of Uganda is preparing a UPI-style national switch and upgrading RTGS to ISO 20022; CBDC feasibility study complete.

E-commerce: Nascent. Constrained by the affordability of devices, weak logistics, and low consumer trust.

Tech enablers	
Energy	- Electricity access at 50% of the population. - Government target to expand renewable capacity under the Digital Transformation Roadmap. - Reliability gaps persist, especially in rural areas.
Connectivity	- Internet penetration 28%. NBI Phase 5 adds 5,800 km fibre, 21 transmission sites and 2,800 last-mile links; - UDAP-GovNet (World Bank) adds 1,500 km fibre, rural broadband masts and 1,000 Wi-Fi hotspots, including in refugee districts. - MyUG public Wi-Fi provides free internet access at 526 hotspots (schools, hospitals, markets, universities and gov. offices.)
Device ownership	- ~43% of individuals aged 10+ own a mobile phone (2024 Census). - ~38.6 million mobile connections (≈76% of population) as of 2025. - ~35% smartphone share among active subscribers (late 2024).
Data centres and cloud uptake	- National Data Centre (Tier II, upgrading to Tier III) hosts 132 entities and 306 apps. - Additional Tier III facilities planned

Non-tech enablers	
Oversight and accountability	- NITA-U leads digital transformation under the Digital Transformation Roadmap, while NIRA is the legal custodian of IDs and civil registration. - Bank of Uganda oversees payments.

	- Coordination between NITA-U and NIRA is essential to avoid fragmentation in the identity system. - Bank of Uganda oversees payments. - Coordination with NIRA (IDs) and sector ministries remains uneven.
Legal framework	- Data Protection and Privacy Act (2019). - Cybersecurity legislation exists, but gaps remain in interoperability and data-sharing rules. - Roadmap calls for updates to align with emerging DPI systems.
Digital skills and literacy	- Digital skilling is a Roadmap pillar. - Capacity gaps persist in schools, civil service and the wider population, slowing adoption of e-services. - Donor-backed training initiatives are filling some gaps but remain fragmented.

Part 2. Stakeholder mapping

Government	- Ministry of ICT & National Guidance (policy lead); - NITA-U (digital transformation and shared services); - NIRA (civil registration and IDs); - Bank of Uganda (payments oversight); sector ministries including Health, Education and Finance.
Regulators	- Uganda Communications Commission (UCC) for telecoms and spectrum - NIRA for identity enrolment and registry functions - Bank of Uganda for financial regulation - Personal Data Protection Office
Industries	- MTN and Airtel dominate mobile money and connectivity. - Commercial banks and fintechs are integrating with a planned UPI-style switch
Tech providers (companies and tech community)	- National Data Centre and local cloud vendors; - International partners supporting MOSIP integration and ABIS upgrades; - Innovation hubs and incubation centres in Kampala and regional cities.
Development partners/ investors	- World Bank (UDAP-GovNet), - GIZ, AFD, Enabel, UNCDF and UNICEF support infrastructure, payments, and service digitisation.
Advocates (civil society, researchers)	- CIPESA, Unwanted Witness and academia active in digital rights, governance and inclusion debates - Local CSOs promote digital literacy and citizen engagement.

Part 3. Performance and potential of existing DPI (SWOT analysis)

Strengths	**Weaknesses**
- Digital Transformation Roadmap (2023/24–2027/28) sets clear priorities. - NITA-U was established as the central implementation agency. - National ID (*Ndaga Muntu*) covers 98% of adults; renewal and MOSIP upgrade underway. - UG Hub, UGPASS, IFMIS, e-Procurement and HCM provide shared services. - National Data Centre operational, Tier III upgrade in progress. - Strong donor support (World Bank UDAP-GovNet, GIZ, AFD, UNCDF, UNICEF).	- DPI is not explicitly framed in the national strategy; overlapping mandates between NIRA (IDs) and NITA-U (digital transformation) create coordination challenges. - UPI-style switch still pending approval; interoperability is limited. - Internet penetration is low (28%). - Smartphone penetration ~38%. - Skills and literacy gaps across government and citizens. - Gaps in cybersecurity, data-sharing and interoperability rules.
Opportunities	**Risks**
- MOSIP integration strengthens scalability and regional interoperability. - UDAP-GovNet extends backbone, rural broadband and Wi-Fi, including refugee areas. - Renewal campaign adds millions of new ID holders, especially youth. - Regional pilots are possible in health (DHIS2), education, and professional credentials.	- Funding shortfalls could delay implementation. - Court cases highlight the risks of exclusion for citizens without IDs. - Weak inter-agency coordination could undermine execution. - Limited cross-border use of existing fibre (NBI dark fibre).

Part 4: Recommendations

1. Clarify DPI framing in the Digital Transformation Roadmap, explicitly linking identity, payments, and data exchange.
2. Finalise approval and implementation of the UPI-style national payment switch; complete RTGS ISO 20022 upgrade.
3. Ensure inclusive delivery of the ID renewal campaign, with safeguards against exclusion.
4. Accelerate backbone expansion (NBI Phase 5, UDAP-GovNet) and rural broadband deployment, including in refugee-hosting districts.
5. Upgrade the National Data Centre to Tier III with full backup and disaster recovery, and expand secure cloud services.

6. Strengthen legal frameworks on cybersecurity, data exchange, and interoperability to build trust.
7. Pilot regional interoperability in payments, health data and professional qualifications under EAC frameworks.

References

Access Now (2024). A human rights-centered approach to digital public infrastructure. (Accessed 22 October 2025).

Adegoke, K. (2024). Key facts about the proposed new General Multipurpose National Identity Card. National Identity Management Commission (NIMC). (Accessed 17 October 2025).

AfricaNenda (N.d.). Who we are. (Accessed 20 October 2025).

Aleina, F.C. (2023). Financing DPI for inclusive and sustainable development. DonorTracker.

Aloo, B. (2024). East African Payment Systems more harm than good on small businesses. Liberty Sparks.

Asadu, C. (2024). West Africa regional bloc approves exit timeline for 3 coup-hit member states. AP News.

AU (N.d.). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. Addis Ababa: AU.

AU (N.d.b). Agenda 2063: The Africa We Want. Addis Ababa: AU.

AU (2014). African Union Convention on Cyber Security and Personal Data Protection. Addis Ababa: AU.

AU (2014b). List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. Addis Ababa: African Union.

AU (2018). Agreement Establishing the African Continental Free Trade Area. Addis Ababa: AU.

AU (2020). Digital Transformation Strategy for Africa 2020-2030. Addis Ababa: AU.

AU (2022). AU Data Policy Framework. Addis Ababa: AU.

AU (2023). AU Interoperablility framework for digital ID. Addis Ababa: AU.

Better than cash alliance (N.d.). Defining digital payments?

Burt, C. (2023). Sierra Leone signs up for national digital ID pilot built with MOSIP. Biometric Update.

Burundi Times (2025). EAC calls for tech-driven cross-border payment system.

Central bank of Kenya (2013). Commence of the East African payment system (EAPS).

Chakravorti, B. (2023). The case for investing in digital public infrastructure. Harvard Business Review.

Clark, J., Marin, G., Ardic Alper, O.P. and Galicia Rabadan, G.A. (2025). Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1. Washington, DC: WB.

Communications Africa (2015). Mobile money transfer between Kenya and Rwanda made easy.

Connecting Africa (2020). Tigo Tanzania opens up mobile money services to East African competitors.

Cook, W. (2018). East African interoperability: Dispatches from the home of M-Pesa. CGAP.
D4DHUB (2025). East Africa data center markets. A Xalam market brief.

DHIS2 (N.d.). Developing & sustaining DHIS2 as a Digital Public Good through long-term partnerships with HISP. (Accessed 22 October 2025).

DHIS2 (2022). Interoperability of CRVS and EIR systems for improved EPI management in Rwanda.

Digwatch (2021). ECOWAS Regional Cybersecurity and Cybercrime Strategy.

Domingo, E., Arnold, S. and Apiko, P. (2023). Interoperability of digital payment systems: Lessons from the East African Community. Maastricht: ECPDM.

DPI (N.d.). The Universal DPI Safeguards Framework is live. (Accessed 21 October 2025). East African Community.

DPI (2024). Tanzania's Digital Transformation: The Foundation of a 10-Year Economic Strategy. (Accessed 22 October 2025).

DPI (2025). Jamii Platforms - Tanzania stack. (Accessed 22 October 2025).

EAC (N.d.a). Common Market. (Accessed 20 October 2025). East African Community.

EAC (N.d.b). Monetary Union. (Accessed 17 October 2025). East African Community.

EAC (N.d.c). EAC hosts Leaders Forum on Digital Public Infrastructure. (Accessed 20 October 2025). East African Community.

EAC (N.d.d). Eastern Africa regional digital integration project. (Accessed 21 October 2025). East African Community.

EAC (N.d.e). East African Integrated Disease Surveillance Network. (Accessed 17 October 2025). East African Community.

EAC (N.d.f). Mutual Recognition Agreements. East African Community.

EAC (N.d.g). Sanitary and phytosanitary measures (SPS). East African Community.

EAC (N.d.h). Single Customs Territory. East African Community.

EAC (N.d.i). Overview of EAC. East African Community.

EAC (N.d.j). Regional Mechanism for Coordination of Social Security Benefits. East African Community. East African Community.

EAC (2008). EAC Framework for Cyberlaws. East African Community.

EAC (2010). Protocol on the Establishment of the East African Community Common Market. Article 11: Harmonisation and Mutual Recognition of Academic and Professional Qualifications. East African Community.

EAC (2014). Launch of the East African Payment System (EAPS). Tralac.

EAC (2023). Produtive sectors UPDATE. East African Community.

EAC (2024a). The East African Community Champions Digital Public Infrastructure at UNGA 79 – Paving the Way for a Digital Future in East Africa (GIZ). East African Community.

EAC (2024b). The Republic of South Sudan signs Mutual Recognition Agreement for Engineers, advancing cross-border mobility and regional integration. East African Community.

EAC (2024c). EAC set to advance data governance and protection with development of a regional policy framework. East African Community.

EAC (2025). The East African community crossborder payment system masterplan. East African Community. East African Community.

EAC (2025b). EAC Unveils Regional Payment System Masterplan to Drive Financial Integration and Digital Trade. East African Community. (Accessed 20 October 2025).

EAC Germany (n.d.). Leveraging Integration Frameworks for Trade in Services and CSOs in the EAC (LIFTED). Fact sheet.

EAC Germany (2023). EAC Strategy for Trade in Services 2023 - 2033.

EACO (2023). Communications Sector Regional Report. East African Communications Organisation.

EATUC (2016). Joint Position Paper on Portability of Social Security Benefits in East African Community. East African Trade Union Confederation.

Eaves, D. and Vasconcellos. B. (2025). Digital Public Infrastructure is the New Global Tech Bet—But Everyone's Betting on Something Different. Tech Policy Press.

EC (2025a). eIDAS Regulation. Shaping Europe's digital future. (Accessed 21 October 2025).

EC (2025b). Global Gateway in Africa: European Union and African Union take stock of significant progress. Directorate-General for International Partnerships.

Ecobank (N.d.). Ecobank in Burundi. (Accessed 17 October 2025).

ECOWAS (2010). Revised ECOWAS Treaty.

ECOWAS (N.d.). Trade policy. (Accessed 22 October 2025).

eCitizer Kenya (N.d.). Government of Kenya services simplified - All your government records unified. (Accessed 20 October 2025).

EEAS (2020). EAC rolls out regional electronic cargo and driver tracking system. Brussels: European External Action Service .

EIB (2021). Unlocking digital connectivity in Africa. European Investment Bank.

Enoch, R. (2025). Nigeria unveils new multi-purpose digital ID card to boost access to services by October 2025. Citizenship Rights in Africa Initiative.

Equity (N.d). Mobile Banking. (Accessed 20 October 2025).

Fincra (2025). The State of cross-border payments within Africa.

Fintechnews Africa (2025). Key Fintech Trends in Africa to Watch in 2025. (Accessed 22 October 2025).

G7G20 (2023). G20 Digital Economy Ministers Meeting Outcome Document and Chair Summary.

G20 (2023a). G20 Digital Economy Ministers' Meeting — Outcome Document and Chair's Summary.

G20 (2023b). G20 New Delhi Leaders' Declaration. (Accessed 21 October 2025).

GAVI (N.d.). Digital health information (DHI). (Accessed 20 October 2025).

GIZ (2023). Digitalisation for East African Trade and Integration (DIGEAT). GIZ / East African Community.

Government of Burundi (2022). Plan directeur de digitalisation des services publics du Burundi. Ministere de la communication, des technologies de l'information eet des medias.

Government of Kenya (2022). The Kenya national digital master plan 2022-2032.

Government of Rwanda (2025). ICT Sector Strategic Plan (2024-2029). Ministry of ICT and Innovation.

Government of Somalia (2025). E-Government strategy & implementation roadmap.

GovStack (N.d.). EGOV-1 - AI Chatbot for Discoverability of Government Services.

GovStack (N.d.b). GovStack.

GovStack (2025). How to use the Playbook.

Graphic Online (2024). Ghana's involvement in ECOWAS Free Roaming Initiative: What it is, benefits.

Gundaniya, N. (2025). Uganda vs Kenya: A Mobile Money Growth Comparison. Digipay.

IADB (2024). Presentan 'Ciudadano Digital Mercosur', iniciativa para mejorar la prestación de servicios y simplificar trámites. Banco Interamericano de Desarrollo

ILO (2025). The East African Community Advances towards Regional Frameworks in Social Protection and Skills Mobility. International Labour Organization.

International Monetary Fund. Middle East and Central Asia Dept (2024). Statement by Mr. Mahmoud Mohieldin, Mr. Ali Alhosani, and Mr. Abdulqafar Abdullahi on Somalia May 29, 2024.

International Monetary Fund. Middle East and Central Asia Dept (2025). Statement by Mohamed Maait, Executive Director Somalia, and Abdulqafar Abdullahi, Advisor to Executive Director July 9, 2025.

IOM (N.d.). When the Waters Recede, Life Returns to South Sudan.

Jamii Stack (N.d.). Jamii Stack Alliance. (Accessed 20 October 2025).

JEPA Africa (2025). Digital Public Infrastructure in East Africa: Charting a Policy Pathway to Regional Transformation. (Accessed 17 October 2025).

Kenya Ministry of Health (2020). Kenya Health Information Systems Interoperability Framework.

Khoza, L. (2024). Ghana launches free roaming initiative with Togo and Benin. ITWeb Africa.

Khumalo, E. (2024). Silicon Savannah: Africa's thriving tech ecosystem. Further Africa.

KICTANET (2025). e-Citizen Platform Contract Raises Concerns.

Kuyoro, M. and Flötotto, M. (2024). Redefining success: A new playbook for African fintech leaders. McKinsey.

LeGrand, C., Paterson, C. and Wiegratz, J. (2024). Fintech is sold as the answer to Africa's problems, but digital money services have downsides which media often overlook. The Conversation.

Macdonald, A. (2024a). Ghana unveils biometric border-management system e-gates at main airport. Biometric Update.

Macdonald, A. (2024b). ECOWAS agrees to accelerate implementation of ENBIC regional ID card for stronger integration. Biometric Update.

Macdonald, A. (2024c). Mali, Niger announce common biometric passport to consolidate ECOWAS exit. Biometric Update.

Majid, N., Abdirahman, K. and Hassan, S. (2017). Remittances and vulnerability in Somalia: Assessing sources, uses and delivery mechanisms. Rift Valley Institute / World Bank.

Mastercard (2024). Safaricom and Mastercard partner to expand remittances and payment acceptance to over 636,000 merchants in Kenya. (Accessed 20 October 2025).

Mbego, S. (2024). Africa Fintech Festival Advocates "Passporting" For Continental Fintech Growth. Tatu city: CIO Africa.

McKinsey (2024). What is fintech? (Accessed 22 October 2025).

Medinilla, A. and Byiers, B. (2023). The political economy of green industrialisation in Africa. Maastricht: ECDPM.

Ministry of Health, Division of Health Information (2023). The Uganda Health Information Exchange and Interoperability Guidelines. Kampala: Ministry of Health.

Ministery of ICT Rwanda (2025). Irembo kick off phased migration of all services to its brand new platform. Accessed 20 October 2025).

Mobile ID World (2025). Ghana launches digital ID-based vehicle toll system using National Ghana Card. (Accessed 21 October 2025).

Mojaloop Foundation (2025). Powering Rwanda's Payments Future: How Mojaloop Enables RNDPS 2.0 and eKash.

Monye, O. and Monye, E. (2022). Regional integration in Africa: Proposals for an Africa-wide payment system. In: Law, Democracy and Development vol. 26 Cape Town.

MOSIP (2023). MOSIP and Sierra Leone sign MoU to pilot national digital ID system.

Muia, W. (2025). Sudan paramilitary attacks leave key city without power. BBC News.

Musoni, M., Domingo, E. and Ogah, E. (2023). Digital ID systems in Africa: Challenges, risks and opportunities. Maastricht: ECDPM.

Musoni, M. and Okechukwu, N. (2024). Interactive tool: Data policies in African countries. Maastricht: ECDPM.

Mutuku, M. (2025). Has increased digitisation of services led to more cyber exposure? A desk review. East African Journal of Information Technology, 8(1), 320-326. DOI: https://doi.org/10.37284/eajit.8.1.3283

Naeku, C. and Juma, K. (2021). The Effect of E-Government on Government Effectiveness and Control of Corruption among UN Member Countries. Nairobi: Kippra.

National Bank of Rwanda (N.d.). CBDC. (Accessed 20 October 2025).

National Information Technology Authority (N.d.). Integration Service (UGHub).

NITA (N.d.). Integration Service (UGHub). (Accessed 22 October 2025).

NMB (N.d.). About us. (Accessed 20 October 2025).

Nyauntu, N. and Shavdia, K. (2025). Digital Public Infrastructure in East Africa: Charting a Policy Pathway to Regional Transformation. JEPA Africa.

Nwanta, N. (2020). Digital Identification and Inclusionary Delusion in West Africa. Center for Human Rights & Global Justice.

Ocran, M.K., Abor, J.Y., Ofori-Sasu, D. and Nambafu, D. (2024). Payment and Settlement Systems and the African Continental Free Trade Area. In: The Palgrave handbook of International Trade and Development in Africa. Palgrave Macmillan.

Odhiambo, A., Kamajugo, R. and Zizane, J. (2017). Taking Advantage of a Window of Opportunity: The Rwanda Electronic Single Window for Trade Efficiency. In: IFC SmartLessons. https://doi.org/10.1596/26291.

O'Grady, V. (2025). South Sudan – and beyond: Africa continues to make digital payments headlines. Developing Telecoms.

Onyango, R. (2025). DPI can be transformative for Africa's digital future. Civil society has a critical role to play. Digital Impact Alliance. (Accessed 21 October 2025).

Ope, M., Sonoiya, S., Kariuki, J., Mboera, L. E. G., Gandham, R. N. V., Schneidman, M. and Kimura, M. (2013). Regional initiatives in support of surveillance in East Africa: The East Africa Integrated Disease Surveillance Network (EAIDSNet) experience. In: Emerging Health Threats Journal, 6. DOI: 10.3402/ehtj.v6i0.19948.

OpenHIE (2020). Creating a Health Information Exchange System in Rwanda.

Owino, V. (2025). EAC cross-border transactions hit record US$2 bn. The EastAfrican.

Pan-African Payment & Settlement System (PAPSS) (2025). Africa launches first Pan-African card scheme – PAPSSCARD.

Quenum, A.C. (2025). East Africa moves closer to a unified, modern payment system. Ecofin Agency.

Raithatha, R. and Storchi, G. (2025). The State of the Industry Report on Mobile Money 2025. GSMA.

Roberts, T. (2025). Decolonising digital public infrastructure. Appropriating technology.

Rodima-Taylor, Paterson, Wiegratz and LeGrand. (2025). The Making of FinTech in Africa: Actors, Interests, Narratives, Challenges. Democracy in Africa.

Sang, D., Munga, J. and Sambuli, N. (2025). Digital Public Infrastructure: A Practical Approach for Africa. Carnegie Endowment for international peace.

Smires, C.B. (2025). How digital wallets have transformed lives of millions in Africa. SBS.

Sunny, D. (2024). South Sudan's communications regulator approves Starlink. Techpoint.Africa.

Tanzania Revenue Authority (n.d.). TeSWS (Tanzania Electronic Single Window System).

Teevan et al. (2025). From India Stack to EuroStack: Reconciling approaches to sovereign digital infrastructure. Maastricht: ECDPM.

Te Velde, D. W., Ayele, Y., Mendez-Parra, M. and Calabrese, L. (2024). Trade facilitation report: driving African trade through digitalisation. TradeMark Africa.

The East African (2015). Mobile money now crosses borders in four East Africa countries.

The Hindu (2023). How the personal data of 815 million Indians got breached, explained.

Thitu, N. (2025). How to Send Money Across Borders in East Africa. Techweez.

Tony Blair Institute for Global Change (2024). Unlocking Africa's Trade Potential: The TWIN Digital Trade Platform. (Accessed 17 October 2025).

Torgusson, C., Paradi-Guilford, C., Hayward, I., González-Berenguer Peña, I., Sepúlveda, E., Kende, M., Morgan, R., Gandal, N. & Abecassis, D. (2018). A Single Digital Market for East Africa: Presenting a vision, strategic framework, implementation roadmap and impact assessment. World Bank.

Tossou Y. (2021). COVID-19 and the impact of cash transfers on health care use in Togo. BMC Health Serv Res. 2021 Aug 27;21(1):882.

TradeMark Africa (2024). East Africa unveils blueprint for accelerating regional cross-border payments to boost trade and financial inclusion. (Accessed 21 October 2025).

Transparency International (2021). Corruption Percetions Index 2021.

Tungali, A. (2024). Londa 2023: Digital rights and inclusion in the Democratic Republic of Congo. Paradigm Initiative.

UEMOA (2003). Traité modifié de l'UEMOA. West African Economic and Monetary Union. (Accessed 20 October 2025).

UN (N.d.). Global Digital Compact. Office for digital and Emerging Technologies.

UN (2024). World Population Prospects 2024 - Summary of Results.

UNCTAD (2023). Roadmap for building a trade single window.

UNDP (N.d.). Digital public infrastructure (DPI). (Accessed 20 October 2025).

UNECA (2025). Cybersecurity for development in the fourth industrial revolution: Research report.

United Republic of Tanzania (2024). Tanzania digital economy strategic framework 2024-2034. Ministry of information, communication and information technology.

Vigueras, R. S. and Pardo Ostos, R. (2021). Concept Project Information Document – Western Africa Regional Digital Integration Program (P176932). World Bank.

Vodafone (2015). Vodafone launches M-Pesa payments between Tanzania and Kenya.

Wainaina, N. (2025). M-PESA's impact on digital payments beyond borders. The Star.

World Bank (N.d.). Mutual recognition of IDs across borders. ID4D Practitioner's Guide.

World Bank (2018). Somali Poverty and Vulnerability Assessment. Summary of Chapter 6: Remittances.

World Bank (2022). Reaching for the potential for the digital economy in Africa - digital tools for better governance. Washington: WB.

World Bank (2025). Digital public infrastructure and development: a World Bank group approach. Digital transformation white paper, volume 1.

World Customs Organization (2017). Kenya, Rwanda and Uganda officially launch Regional Electronic Cargo Tracking System.

World Economic Forum (2025). This initiative could cut the cost of global trade by 25%.

World Health Organization, Regional Office for the Eastern Mediterranean (2024). Somalia launches electronic immunization registry in latest leap of innovation.

Yaici, K. (2025). Connecting Africa: The Performance and Impact of Starlink's Satellite Internet. Ookla Research.

About ECDPM
ECDPM is an independent 'think and do tank' working on international cooperation and development policy.

Since 1986 our staff members provide research and analysis, advice and practical support to policymakers and practitioners across Europe and Africa – to make policies work for sustainable and inclusive global development.

Our main areas of work include:

- EU foreign and development policy
- Migration and mobility
- Digital economy and governance
- AU-EU relations
- Peace, security and resilience
- Democratic governance
- Economic recovery and transformation
- Climate change and green transition
- African economic integration
- Sustainable food systems

For more information please visit www.ecdpm.org

In addition to structural support by ECDPM's institutional partners: The Netherland, Austria, Belgium, Denmark, Estonia, Finland, Ireland and Luxembourg, this publication also benefits from a contribution by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ).

ISSN1571-7577

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

ecdpm

HEAD OFFICE
SIÈGE
Onze Lieve Vrouweplein 21
6211 HE Maastricht
The Netherlands *Pays Bas*
Tel +31 (0)433 502 900

BRUSSELS OFFICE
BUREAU DE BRUXELLES
Avenue des Arts 44, 1040
Brussels *Bruxelles*
Belgium *Belgique*
Tel +32 (0)2 882 50 08

info@ecdpm.org
www.ecdpm.org
KvK 41077447