

FLAGSHIP RESEARCH / 29 OCTOBER 2026

Digital Public Infrastructure in Africa: Procurement, Interoperability and Accountable Service Delivery

A decision framework for building digital identity, fast payments and data exchange as reliable public-service infrastructure



StoneComms Research & Intelligence / Public-source desk research

RELEVANT SDGS / PRIMARY: 9

9

16

10

STANDFIRST

Digital public infrastructure can shorten the distance between a person and a public service. It can also concentrate failure, exclusion and supplier dependence inside systems that become difficult to replace. As African governments move from pilots to national and cross-border platforms, the central question is no longer whether to digitise. It is how to procure a modular, governed service that people can use, challenge and trust.

01 / ANALYSIS

Executive Summary

IN BRIEF

- Treat digital identity, fast payments and trusted data exchange as one service system with separate, replaceable components.
- Procure measurable public outcomes, operating capacity and exit rights, rather than a platform licence alone.
- Make inclusion, redress, privacy, security and uptime contract deliverables, tested through real service journeys.

The African Union's sixth ministerial session on communication and ICT is considering a continental digital public infrastructure roadmap, minimum standards for digital-ID interoperability and the next phase of the Digital Transformation Strategy for Africa. The timing matters. World Bank and UNDP programmes are also moving from foundational platforms towards scale, while countries are linking identity, payments and public services in different institutional forms.

The opportunity is substantial. Shared digital capabilities can reduce repeated identity checks, speed payments, let agencies verify information with consent and make a service available without a journey to an office. Yet the same shared capability can turn a design defect, outage or exclusion rule into a problem across many services. A platform that is efficient for the state can still be costly for the resident if it requires an unaffordable device, a long trip for enrolment, a specific language, repeated biometric attempts or an agent who charges an unofficial fee.

This paper argues that digital public infrastructure should be commissioned as a public-service operating model. Architecture still matters, but procurement and governance determine whether interoperability survives the first contract, whether alternative suppliers can enter, whether data can move safely, and whether a person can obtain a remedy when the system is wrong.

Five conclusions follow.

1. The unit of value is a completed service journey.

Identity credentials, payment rails and data exchange create public value only when people can use them to complete a task such as receiving a benefit, registering a business or proving eligibility. 2.

Interoperability is both technical and institutional.

Common interfaces do not settle legal authority, liability, service ownership, consent or responsibility for correction. 3. **Procurement creates long-term market structure.**

A monolithic contract can move quickly while creating dependency. Modular contracts, open interfaces, government control of core data and tested exit provisions preserve future choices. 4. **Safeguards must be operational.** Privacy, cybersecurity, offline alternatives, assisted access and appeal mechanisms require owners, budgets, response times and evidence. 5. **Scale should follow measured performance.**

Governments need service-level evidence on completion, exclusion, correction, availability, cost and supplier substitutability before expanding a platform's mandate.

Why This Decision Matters Now

IN BRIEF

- The AU is moving from broad digital ambition towards specific continental DPI and digital-ID standards.
- National platforms are becoming shared dependencies across social protection, finance, health, licensing and civil registration.
- New investment will either preserve public choice or harden supplier and architecture decisions for a decade.

Digital public infrastructure usually refers to shared digital systems that allow people, governments and firms to identify, pay and exchange data. These functions are often described as a stack. The metaphor is useful if it encourages modularity, but misleading if it hides the institutions around the technology. A digital identity system needs enrolment channels, correction procedures and rules governing who may rely on a credential. A fast-payment system needs settlement, dispute resolution, fraud controls and viable participation by banks and non-banks. A data-exchange layer needs legal authority, purpose limitation, consent where appropriate, audit trails and accountability for errors in source records. None of those functions is solved by an application programming interface.

The World Bank's Global DPI programme now supports work in more than 80 countries. Its 2026 results report describes identity, payments and data systems as foundations for services and economic participation. UNDP's 2026 Africa policy paper and accelerator similarly emphasise trusted, interoperable and inclusive infrastructure. The convergence is important: the policy debate is moving beyond isolated e-government projects. Africa's access conditions make implementation choices especially consequential. ITU estimates that 36 per cent of people in Africa used the internet in 2025. A digital-only design can therefore transfer administrative cost to residents who lack connectivity, devices, digital skills or accessible interfaces. Physical service points, delegated assistance, low-bandwidth channels and a right to complete a service without surrendering unnecessary data are infrastructure features, not temporary outreach measures.

03 / ANALYSIS

From Platform Procurement To Service Procurement

IN BRIEF

- Define the public-service result and affected population before choosing architecture.
- Separate components that must interoperate, scale and be replaced on different cycles.
- Price operation, maintenance, security, correction and exit for the full service life.

Technology procurements often begin with a solution category: national identity platform, payment switch, data-exchange layer, cloud migration or citizen portal. The stronger starting point is the service journey. Which person is trying to do what? Which institution is accountable? What evidence is required? What is the consequence of a false rejection or an unauthorised disclosure? What alternatives exist when connectivity or a credential fails?

This changes the specification. Availability becomes a measure of successful service completion rather than server uptime alone. Performance includes correction time, agent reach and payment reversals. Security includes the ability to suspend a compromised relying party. Inclusion includes assisted and offline channels, accessible design and evidence on who drops out.

The World Bank's 2026 technical procurement guidance for DPI recommends openness, security, sustainability and social value throughout the procurement cycle. Its ID4D guidance also warns that weak internal technical capacity can allow vendors to shape requirements, increasing cost and lock-in risk. The implication is organisational: an independent, capable public buyer is part of the infrastructure.

A six-part procurement test

- 1. Service outcome.** Specify the completed public task, baseline performance and population segments. Include the journeys most likely to fail, not only the typical user.
- 2. Modular boundary.** Define components, interfaces and data responsibilities so that identity, payments, exchange, portals and sector systems can evolve without a full-platform replacement.
- 3. Operating capability.** Fund service management, security operations, data stewardship, user support and supplier oversight. Require a staged transfer of knowledge and operational control.

4. Rights and safeguards. Make lawful use, minimisation, security, assisted access, correction, redress and independent oversight measurable obligations.

5. Market and exit. Require open, documented interfaces; portable data; testing environments; source or escrow arrangements where appropriate; transition assistance; and realistic replacement tests.

6. Evidence gate. Link scale, renewal and payment to verified service performance, including outcomes for underserved users.

StoneComms original synthesis: The six-part test is a commissioning framework derived from the evidence in this paper. It is not a formal standard. Its purpose is to keep public value, operational resilience and future choice visible at procurement decision points.

04 / ANALYSIS

Interoperability Without A Megasystem

IN BRIEF

- A shared trust framework can connect systems without creating one continental identity or database.
- Technical compatibility must be matched by legal authority, liability and service ownership.
- Reusable credentials should disclose only what a transaction needs and leave an auditable record.

The African Union's Interoperability Framework for Digital ID defines common requirements and minimum standards so different systems and relying parties can communicate. It explicitly does not propose one unified African identity system. That distinction protects institutional diversity while creating a path towards mutual recognition.

At national level, the same logic supports a federated architecture. A health service may need proof of eligibility, a bank may need identity evidence for customer due diligence, and a licensing authority may need confirmation of a business record. They do not all need copies of the same complete record. A trusted exchange can provide a verified attribute, record the request and keep responsibility for the source data visible.

Payment interoperability adds another layer. AfricaNenda and partners reported in March 2026 that nearly half of AU member states had a live instant-payment system. Their analysis shows that infrastructure alone does not ensure routine, inclusive use. Licensing, access to clearing and settlement, pricing, consultation, fraud management and dispute resolution shape who can participate and whether households and merchants keep using the rail.

The World Bank's ID Meets Instant work proposes portable payment identity credentials as a way to connect digital identity and fast payments without creating a single central wallet or identity database. The design lesson is broader than payments: interoperability should exchange the minimum verified information required for a transaction, under a clear trust and liability framework.

Four layers of interoperability

Technical: common interfaces, data formats, authentication patterns, cryptographic trust and conformance tests.

Semantic: shared meaning for attributes, status, timestamps, errors and service events.

Legal: authority to request and disclose data, privacy duties, retention, liability and cross-border recognition.

Operational: service ownership, incident response, correction, version management, onboarding and offboarding.

A procurement that covers only the technical layer creates an interface without an operating institution. A governance agreement without conformance testing creates a policy that suppliers interpret differently. Both are incomplete.

Country Evidence: Different Functions, Not A League Table

IN BRIEF

- Country examples show distinct institutional functions rather than one preferred model.
- Reported reach is useful evidence of adoption, but does not by itself prove inclusion or service quality.
- Transferability depends on law, administrative capability, connectivity and delivery channels.

Ethiopia: identity as an access layer. World Bank

implementation reporting states that Fayda registration exceeded 39 million by March 2026 and integration had reached more than 100 public and private institutions. The programme combines enrolment, legal foundations, data protection capacity and use cases. Its value lies in enabling verification across services, including for refugees and other groups historically excluded from formal records. The next evidence need is service-level: completion, correction and exclusion rates by population and channel.

Nigeria: scale and delivery reach. The World Bank reports more than 100 million National Identity Numbers issued. It also describes social-protection delivery reaching millions of households, with attention to cash-out distance. These are different evidence units. Identity issuance measures coverage; a payment reaching a household measures delivery; neither alone establishes affordability, control of personal data or ease of correction.

Rwanda: a reusable service gateway. Rwanda's Ministry of Local Government reported in 2026 that Irembo hosted more than 100 services from over 20 institutions and reduced bureaucracy. The platform illustrates the value of a recognisable, reusable service channel. Rwanda's physical Service Access Points also show why assisted access remains necessary. Government-reported assessments are useful operational signals, but independent outcome evidence and published service-level data would strengthen conclusions.

Zambia: procuring trust and authentication. Smart Zambia issued a March 2026 request for proposals for digital authentication and verification infrastructure. Zambia also launched national public-key infrastructure in October, while public statements acknowledged that sustained operation, skills, resources and institutional adoption would determine value. This sequence makes the operating model visible: authentication, signing and trust infrastructure need coordinated adoption by service owners.

Regional layer: common rules before mutual recognition. AU work on digital-ID interoperability and a DPI roadmap provides a framework for cross-border compatibility. Smart Africa reported on 20 October that Benin, Ghana and Rwanda had completed the first phase of a federated cross-border identity pilot using synthetic data in a controlled environment. The milestone shows that national systems can test trusted verification without centralising identity databases, but it is not evidence of live public use or service impact. Regional standards create an option to connect; national law, source-record quality, service ownership, security assessment and domestic redress determine whether that option becomes safe and useful.

06 / ANALYSIS

The Accountability Architecture

IN BRIEF

- Shared infrastructure needs a visible owner for every request, record and failure.
- People need a practical route to correct data and challenge a service decision.
- Independent oversight and public reporting should scale with system reach and consequence.

DPI concentrates dependencies. If an identity service fails, benefits, finance and licences may fail together. If a source record is wrong, interoperability can spread the error more efficiently. If a credential becomes a de facto condition for essential services, voluntary enrolment may cease to be meaningful in practice.

An accountability architecture therefore needs more than a privacy notice. It should define who controls each dataset; which institutions may query it; what evidence a request must carry; how the person is informed; how errors are corrected at source; how downstream systems receive corrections; how incidents are contained; and who can impose remedies.

The operational test is simple: a resident should be able to answer five questions.

1. What information was used? 2. Which institution requested it and for what purpose? 3. What decision or payment followed? 4. How can an error be corrected or a decision challenged? 5. What alternative exists while the issue is resolved?

Procurement can make these answers possible. Contracts can require transaction logs that public bodies can audit, service-level targets for correction and appeal, notification patterns, independent testing, incident reporting, vulnerability management and data deletion at contract end. They can also reserve government rights to inspect, export and transfer data without punitive fees.

Accountability also requires proportionality. A low-risk information service does not need the same controls as a system that determines access to income, movement or healthcare.

Governance should follow the consequence of the decision and the number of people affected, rather than the novelty of the technology.

07 / ANALYSIS

A Digital Public Infrastructure Scorecard

IN BRIEF

- Measure the public service, the shared infrastructure and the supplier market together.
- Disaggregate by gender, disability, geography, income proxy, language and assisted-access use where lawful.
- Publish trends and exceptions, not only national averages.

Dimension	Core question	Illustrative measures
Service completion	Can people finish the task?	completion rate, median time, repeat attempts, abandonment
Inclusion	Who is excluded or pays more?	assisted-access use, offline completion, rejection by group, travel and fee burden

Dimension	Core question	Illustrative measures
Accuracy and redress	Can errors be fixed?	false rejection, correction time, appeal resolution, downstream update
Availability and resilience	Does the service survive failure?	end-to-end availability, degraded-mode completion, recovery time, correlated outages
Privacy and security	Is use lawful and controlled?	unauthorised queries, high-risk findings, incident containment, deletion compliance
Interoperability	Can components and agencies connect safely?	conformance pass rate, onboarding time, version failures, minimum-data adherence
Market health	Can the state change supplier?	qualified suppliers, component replacement test, export time, switching cost
Public value	Is service improving at sustainable cost?	unit cost per completed journey, staff time saved, payment leakage or delay where evidenced

The scorecard deliberately separates inputs, operations and outcomes. Registrations, transactions and connected agencies are scale indicators. They are not proof that users experienced a better service. A procurement should state which measures trigger payment, remediation, expansion or pause.

StoneComms original synthesis: A useful evidence gate combines three thresholds: acceptable service performance for the overall population, no material deterioration for an underserved group, and a demonstrated ability to replace or isolate a component without losing the service. This prevents national averages from masking exclusion and prevents apparent performance from resting on an unchangeable supplier.

Implications For Policy, Capital And Implementation

IN BRIEF

- Governments should fund institutional capability with the platform.
- Development partners should finance evidence, safeguards and transition capacity, not only rollout.
- Suppliers should expect interoperability, auditability and exit to be evaluated as performance.

For governments

Create a senior service owner with authority across the participating agencies. Maintain an architecture authority that publishes standards and conformance tests, but keep delivery accountability with named service institutions. Build an independent procurement team able to challenge solution design, commercial assumptions and security claims.

Use staged contracting. Fund discovery and service mapping before committing to national scale. Pilot with difficult journeys and underserved groups. Release expansion funding only after public evidence shows acceptable completion, redress, resilience and inclusion.

Make assisted and offline access part of the core service. Physical enrolment and service points should be designed, costed and monitored as channels in the operating model. They should not become permanent places where residents pay intermediaries to compensate for poor digital design.

For development finance institutions and donors

Treat operations, cybersecurity, data protection, service design, independent evaluation and government technical capacity as investable components. A platform whose maintenance, incident response or helpdesk is unfunded is not sustainable infrastructure.

Use financing conditions to strengthen public ownership and future competition. Require open interfaces, data portability, transparent recurring costs, independent assurance and a funded transition plan. Avoid tying policy reform to a single proprietary architecture.

Coordinate regional and national support. Continental frameworks can reduce duplication, but country programmes need resources to translate standards into law, procurement documents, conformance tests, service operations and public communication.

For technology and service providers

Design for replacement. Document interfaces, events, data models and deployment dependencies. Provide automated conformance testing and realistic transition support. A supplier that can demonstrate safe component substitution offers greater public value than one that claims end-to-end indispensability.

Price the full operating service transparently. Separate licences, hosting, security, support, customisation, transaction charges and exit services. Make future volume bands and inflation assumptions visible so the public buyer can compare life-cycle cost.

Support local capability through accountable work packages.

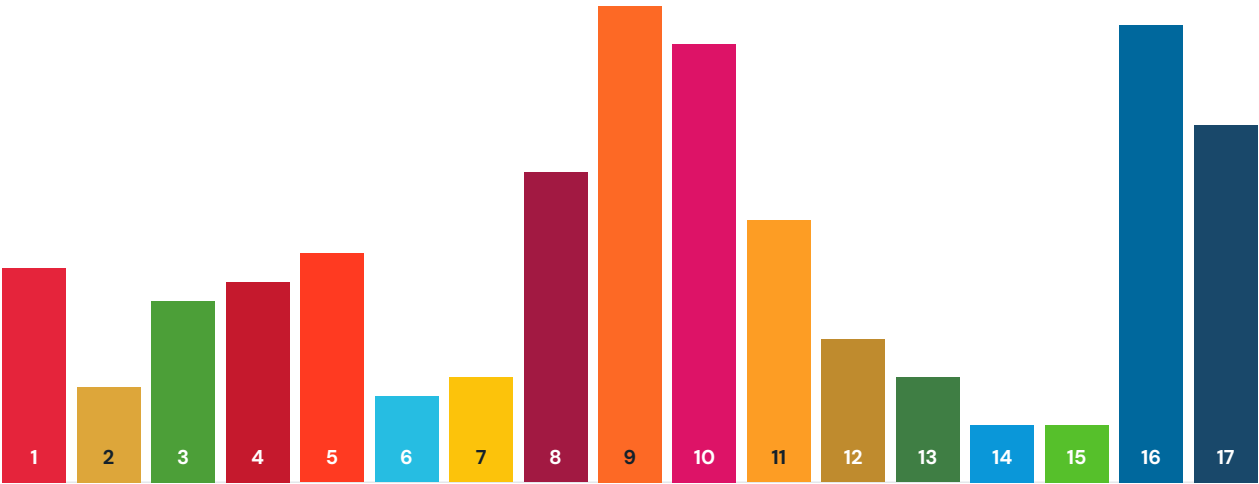
Knowledge transfer should be demonstrated through operational drills, runbooks, incident exercises and government-led releases, not counted as training days.

11 / CLASSIFICATION

Communities and the UN SDGs

IN BRIEF

- SDGs 9, 16 and 10 are the most direct classifications for this research.
- Other goals depend on the sector and service using the shared infrastructure.
- Relative prominence is qualitative interpretation, not impact measurement.



Lower bar: indirect or application-dependent relationship

Higher bar: direct relationship to this paper

Digital public infrastructure can reduce friction in services, payments and eligibility checks. It can also deepen exclusion when connectivity, enrolment, language, disability access or redress is weak. Communities therefore experience the infrastructure through service completion, cost, agency and remedy, not through platform deployment alone.

SDG relevance and relative prominence are StoneComms interpretations of issues and outcomes documented in this research. They are not formal impact measurements, and they do not imply endorsement by the United Nations.

12 / REFERENCE

Methodology

This paper is a public-source desk review completed on 29 October 2026. It combines current policy signals from the African Union, World Bank and UNDP with implementation evidence from Ethiopia, Nigeria, Rwanda and Zambia; a controlled cross-border interoperability milestone involving Benin, Ghana and Rwanda; specialist guidance on identity, payments, procurement and interoperability; and ITU connectivity data.

Sources were selected for institutional proximity to the underlying programme, publication date and relevance to procurement or service delivery. Government and programme reports are treated as evidence of policy, implementation status and reported reach. They are not treated as independent causal evaluations unless the source provides that design.

StoneComms compared cases by institutional function, not national ranking. The procurement test, interoperability layers, scorecard and evidence gate are original synthesis. They have not been validated as a formal standard and should be tested against local law, service data and procurement conditions.

13 / REFERENCE

Limitations

Public reporting is richer on registrations, system launches and connected services than on failed transactions, user cost, correction, appeals and independent security performance.

Commercial contracts, life-cycle cost models, incident logs and supplier performance data were generally unavailable.

National averages can obscure differences by gender, disability, rurality, income, displacement status and language. Some country evidence comes from implementing institutions and therefore requires independent verification before causal conclusions are drawn.

Technology, policy and programmes are changing quickly. This paper describes evidence available by 29 October 2026 and does not constitute legal, cybersecurity or procurement advice.

14 / REFERENCE

Source Note

All figures and implementation claims are attributed to the publishing institution. Phrases such as "the World Bank reports" or "the ministry reported" distinguish reported programme evidence from StoneComms interpretation. No proprietary datasets, source code, system audit, user research or confidential contracts were reviewed.

15 / REFERENCE

Sources

1. African Union, "6th Ordinary Session of the Specialised Technical Committee on Communication and ICT", 26–29 October 2026. <https://au.int/en/newsevents/20261026/au-innovation-festival-au-innofest26-theme-vibrant-youth-ecosystems-ai-and>
2. African Union, "AU Interoperability Framework for Digital ID", 11 December 2023. <https://au.int/en/documents/20231211/au-interoperability-framework-digital-id>
3. World Bank, "Global Digital Public Infrastructure Program: From Foundations to Scale", 6 May 2026. <https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program>
4. World Bank, "Technical Procurement Guidance for DPI and Integral Digital Service", 24 April 2026. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099042426124014450>
5. World Bank ID4D, "Procurement" and "Standards" practitioner guidance, accessed 29 October 2026. <https://id4d.worldbank.org/guide/4-procurement> and <https://id4d.worldbank.org/guide/standards>
6. World Bank, "ID Meets Instant: Enabling Trusted, Inclusive Fast Payments through Digital Identity", February 2026. <https://fastpayments.worldbank.org/resources>
7. UNDP Africa, "Digital public infrastructure in Africa: A leapfrog catalyst for inclusive growth", 26 June 2026. <https://www.undp.org/africa/publications/digital-public-infrastructure-africa-leapfrog-catalyst-inclusive-growth>
8. AfricaNenda Foundation, Arab Monetary Fund, Better Than Cash Alliance and World Bank, "Scaling Instant Payments in Africa: Policy Choices for Central Banks", 9 March 2026. <https://africanenda.org/resource/scaling-instant-payments-in-africa-policy-choices-for-central-banks>
9. ITU, "Facts and Figures 2026: Internet use", 13 October 2026. <https://www.itu.int/itu-d/reports/statistics/2026/10/13/ff26-internet-use/>
10. World Bank, "Ethiopia Digital ID for Inclusion and Services Project: Implementation Status and Results Report", May 2026. <https://documents1.worldbank.org/curated/en/099051826153515642/pdf/P179040-74a164c1-0bb2-49b6-8b5f-2da36395da02.pdf>
11. Rwanda Ministry of Local Government, "Rwanda's Digital Transformation Strengthens Local Government Service Delivery", 2026. <https://www.minaloc.gov.rw/news-detail/rwandas-digital-transformation-strengthens-local-government-service-delivery-study-reveals>
12. Rwanda Ministry of ICT and Innovation, "Service Access Points", accessed 29 October 2026. <https://www.minict.gov.rw/projects/service-access-points>
13. Smart Zambia Institute, "Implementation and Roll-out of a Digital Public Infrastructure for Digital Authentication and Verification", 26 March 2026. <https://www.szi.gov.zm/?p=6592>
14. Zambia Ministry of Technology and Science, "Launch of the National Public Key Infrastructure", 7 October 2026. <https://www.mots.gov.zm/?p=7728>
15. World Bank Group, "World Bank Group Launches First Digital Strategy to Expand Access and Create Jobs", 20 October 2026. <https://www.worldbank.org/en/news/press-release/2026/10/20/world-bank-group-launches-first-digital-strategy-to-expand-access-and-create-jobs>
16. Smart Africa, "Benin, Ghana and Rwanda Take Major Step Towards Africa's Single Digital Market Through Cross-Border Digital Identity Interoperability", 20 October 2026. <https://smartafrica.org/benin-ghana-and-rwanda-take-major-step-towards-africas-single-digital-market-through-cross-border-digital-identity-interoperability/>