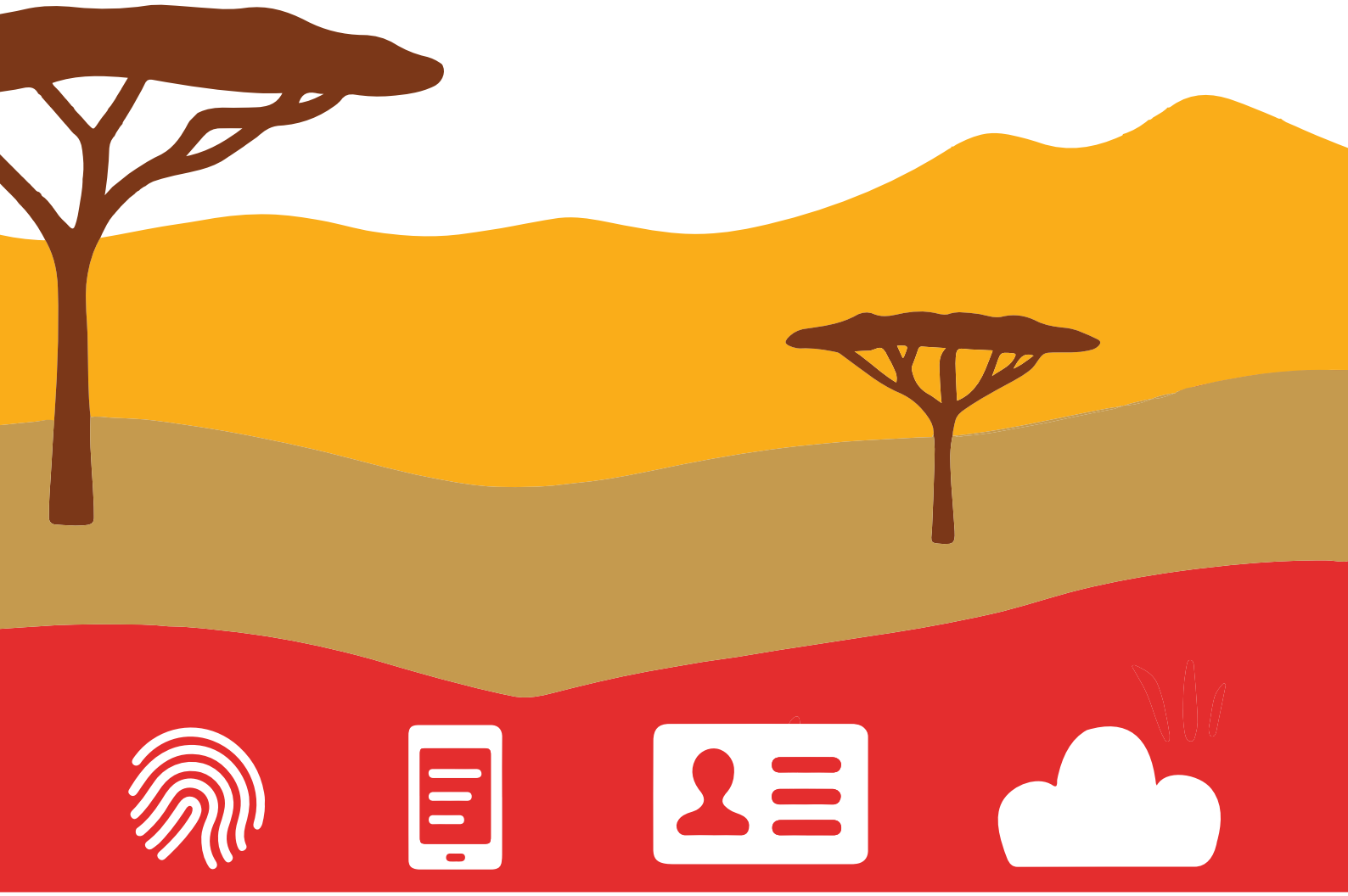
A Report on the Study of

Government Digital Services and Digital ID in Kenya and Zambia



Strathmore University

Centre for Intellectual Property and Information Technology Law

Introduction

How Africans engage with their governments is rapidly changing. Crucial services like tax filing, invoicing, and business registration, as well as applications for documents like driving licenses, birth certificates, passports and identity cards are increasingly tied to digital platforms. While this shift promises a new era of government efficiency, transparency, inclusion and unprecedented access to public services, these benefits are overshadowed by concerns over data privacy, data collection and centralisation, data sovereignty, increased marginalisation, and legal protections.

The report examines the current landscape of government digital services and digital identity systems in Kenya and Zambia. Through surveys with civil society organisations (CSOs), the private sector and government agencies, extensive literature review and legal analysis, the study seeks to identify governance frameworks and implementation strategies for digital ID and government digital services, assess institutional and regulatory gaps, and propose strategies for collaborative engagement among governments, CSOs, and the private sector.

The overarching research question is:

> What governance design and implementation mechanisms are needed to address the existing regulatory, institutional and capacity gaps that inhibit the establishment of democratic, just and rights-preserving data systems in the provision of government digital services and digital ID in Kenya and Zambia?

Findings reveal that both Kenya and Zambia have made significant investments in digital ID and digital government services. Kenya has introduced Maisha Namba, eCitizen, and the Huduma Kenya Service Delivery Programme. Zambia is deploying biometric IDs through its Integrated National Registration Information System (INRIS) and Electronic National Registration Cards (eNRC), while also expanding rural access via Smart Village and the Digital Zambia Acceleration Project.

Despite existing legal frameworks, such as Kenya's Data Protection Act of 2019 and Zambia's Data Protection Act of 2021, enforcement remains weak. Regulatory bodies lack sufficient resources, technical capacity, and autonomy, undermining the effective protection of personal data. Moreover, the legislative environment has not adequately addressed the risks posed by overcollection of biometric data, opaque data-sharing practices, or the lack of informed consent.

These challenges are particularly acute for marginalised communities such as refugees, women, and rural populations, who often face discriminatory vetting procedures, poor access to documentation, or limited digital literacy.

CSOs play a critical role in addressing these gaps. They are engaged in legal empowerment, policy advocacy, public awareness campaigns, and digital rights training, helping communities navigate complex identification systems and hold institutions accountable. The private sector, while instrumental in deploying infrastructure and services, has called for clearer regulatory guidance and improved collaboration with oversight agencies. Government stakeholders acknowledge challenges related to data security, capacity gaps, and service delivery inefficiencies, particularly in rural areas.

Summary of Findings from Kenya

A significant concern across all surveyed sectors in Kenya is the persistent exclusion of marginalised communities from accessing government digital services. CSOs highlight bureaucratic hurdles faced by refugee populations in registering for digital IDs. They report that ethnic minorities and indigenous communities frequently struggle to obtain official identification. These groups also struggle to access digital services. Beyond documentation, CSOs point to digital illiteracy and infrastructural limitations as exacerbating these challenges, impeding rural communities' ability to interact with online government services.

The private sector corroborates these observations, identifying limited digital literacy, the lack of proper identification, and inadequate infrastructure in remote areas as key barriers. Likewise, government agencies acknowledge similar barriers.

The consistent mention across all three stakeholder groups of the lack of foundational identity documents as a primary barrier to digital access reveals a deeply rooted systemic issue. This suggests that digital exclusion in Kenya is not solely a technological or educational gap but is profoundly rooted in traditional administrative and legal identity systems.

The integration of biometric ID systems into government digital services has introduced both opportunities and significant challenges. CSOs report that biometric data, such as fingerprints and facial recognition, is widely required for accessing key services, including national identification, health insurance, and voter registration. However, concerns persist regarding the risk of exclusion due to technical errors, the absence of clear regulations, and gaps in oversight mechanisms. The centralisation of biometric data particularly in systems like Maisha Namba, without adequate transparency, is highlighted as a major issue.

Kenya has a robust legal framework governing digital services and biometric ID data, but key issues arise across civil society, the private sector, and government. CSOs point to weak enforcement, regulatory gaps, limited transparency in government data practices such as the non-disclosure of DPIAs, and insufficient public participation, which contribute to low trust and potential exclusion. The private sector highlights overlapping regulations, frequent legal changes, and inconsistent enforcement, all of which create uncertainty and complicate compliance efforts. Further, government agencies report challenges related to limited technical infrastructure, low awareness of data protection obligations, inadequate staffing, financial constraints, and fragmented systems, which collectively undermine the effective implementation of data governance frameworks.

The research also identified gaps in training, ranging from knowledge of the laws and best practices of data protection and inclusion, that could be solved through regular staff capacity-building. Most of the institutions interviewed did not indicate that they were trained on the new laws on data protection nor were they aware of the need for data protection impact assessments. Government acknowledgments of human resource constraints and limited awareness of data protection obligations, alongside reports of internal misconduct and data breaches, point to human capacity as a key factor in successful digital governance.

Summary of Findings from Zambia

The assessment of digital governance in Zambia is primarily informed by the perspectives of CSOs because of the absence of data from key state and commercial actors.

A key theme emerging from Zambian CSOs is the persistent challenge of digital exclusion, particularly among marginalised groups such as refugees, asylum seekers, women and girls, PWDs, and underserved communities.

The use of biometric data in accessing government digital services is another area of diverse experiences among Zambian CSOs. Most respondents confirmed that biometric authentication, including fingerprints, facial recognition, and iris scans, are required for certain services. However, concerns were raised by some CSOs regarding a lack of government communication about the purpose of data collection and concerns about data-sharing practices. The inconsistency in service requirements, with some organisations not being required to submit biometric data, also indicates a lack of uniformity.

Capacity-building emerged as a strong focus for several Zambian CSOs, with some organisations investing in community-based training on digital safety, ethical data use, and cybersecurity. Other organisations also reported organising public forums and awareness sessions on digital rights. However, this momentum is not shared across all actors, with some CSOs indicating limited or no biometric-specific training programmes, or a general lack of internal technical capacity. Internal governance mechanisms also varied considerably among CSOs, ranging from comprehensive systems with encryption and audits to informal practices like basic password hygiene or policies still under development.

While some CSOs show robust interaction with regulators, others exhibit vague or incomplete responses and a lack of internal technical capacity. This points to a significant disparity in the institutional capacity of CSOs themselves to effectively engage with complex digital governance issues, understand nuanced legal frameworks, and advocate for policy changes.

Summarised Recommendations

The study recommends the following courses of action:

Legislative reforms and effective enforcement in response to discriminatory digital ID legislation, non-implementation of data protection legislation, a lack of capacity to enforce laws, and political interference in

legislation and enforcement.

Enhancing data governance and data protection to remedy the lack of transparency in data collection, sharing and overall governance practices as well as stronger cybersecurity enforcement, capacity-building programmes, and increased investment in secure data storage infrastructure.

Digital access and inclusion as a means to address the persistent exclusion of marginalised communities from digital services, with CSOs urging governments to adopt a rights-based approach to digital governance.

Addressing systemic inequalities such as gender inequality and access to mobile technology through inclusive design principles, capacity-building initiatives, and robust regulatory frameworks.

Building capacity and resource allocation in response to limited technical infrastructure, human resources, and financial investment with the aim of empowering communities to engage with digital government platforms effectively.

Improving collaboration between CSOs, private sector and government agencies to resolve regulatory ambiguities and improve cybersecurity practices.

Ethical guidelines for digital technologies that empower data protection agencies to better address key concerns like informed consent, data minimisation, and safeguards against misuse, with the guidelines mandating transparency in data practices, prohibiting discrimination, and countering risks such as mass surveillance and unauthorised data sharing.

Decentralised citizen feedback and redress mechanisms to strengthen accountability and cultivate trust in digital governance by creating secure and anonymous reporting channels in addition to empowering local CSOs and community groups to act as independent observers.

Advancing interoperability for inclusive digital services in response to fragmented service delivery and silos that limit governments' ability to build a holistic view of citizen needs, hindering effective access to services particularly for marginalised communities.

Summarised Conclusion

While both countries have made concerted efforts to digitise government services, there are persisting gaps and challenges in the rollout and implementation that ought to be addressed. It is also important for governments to have proper policies in place to anchor digital identity regimes and implement proper safeguards for data protection and safety. It also takes a multi-stakeholder approach to fully address the gaps and challenges impacting the implementation of existing frameworks on government digital services.

This study was made possible by a grant provided by the International Development Research Center (IDRC). We thank the organization for their continued support.

IDRC · CRDI
International Development Research Centre
Centre de recherches pour le développement international

Canada