

Policy Briefing

282

November 2023



Digital identification and Biometrics In East Africa: Opportunities and Concerns

ISABEL BOSMAN

Recommendations

- Digital identification (ID) systems should be rolled out transparently, with public consultation, and take into consideration the sensitivity of collected data.
- Function creep (the use of data that has been collected for one purpose, for other purposes) is a real possibility in centralised shared databases between public and private sectors. Data protection and privacy should always be respected.
- It is advisable to maintain paper-based or analogue alternatives or alternative biometric options if registrants are not able to supply the necessary biometric data.
- A strong legal basis for the protection of data and privacy of the bearer is crucial to the functioning of any digital ID system.
- Cybersecurity and related legislation should be prioritised.

Executive summary

Possession of legal identity is a link between citizens and the myriad government services and social, economic and legal rights available to them. However, around 50% of Africa's population do not have a legal identity, making it increasingly difficult for people to access vital government services such as healthcare and social grants, and to set up bank accounts, register SIM cards, and apply for other important documents such as passports. The provision of legal identity is included in the UN's Sustainable Development Goals and is also regarded as important in attaining the objectives of the AU's 'Agenda 2063: The Africa We Want'. The roll-out of legal identity is moving away from traditional, paper-based systems to digital systems, which often include the collection of biometric data for additional security. This reduces the risk of identity theft and fraud, to some extent. However, without the proper legal framework guiding implementation, such programmes could significantly increase the risk both of certain members of the population being excluded and of collected data being abused. This policy briefing considers the implementation of digital identification programmes in two East African states – Ethiopia and Uganda. It explores the advantages and drawbacks of these systems and makes recommendations on how to mitigate the risks of such systems and ensure that their implementation considers the privacy and data protection of citizens.

Introduction

A national ID document is a primary vehicle for inclusion in and access to government services, as well as the exercise of social, economic and legal rights for millions of people across Africa. Possessing a legal identity, defined by the UN as 'the basic characteristics of an individual's identity... conferred through registration and the issuance of a certificate by an authorised civil registration authority following the occurrence of birth',¹ connects citizens with governments and the services they provide.

Yet, nearly half of Africa's population still go about their daily lives without any form of legal identification.² The most recent World Bank data indicates that one in four adults in sub-Saharan Africa does not have an ID.³ This lack of legal identity also has a gendered impact, with ID coverage among adult women found to be significantly lower than among men.⁴ Foundational identity management is defined by the World Bank as 'an identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of

1 UN, "UN Legal Identity Agenda", <https://unstats.un.org/legal-identity-agenda/>.

2 Anri van der Spuy et al., *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative Analysis of Findings from Ten Country Case Studies*, Report (Cape Town: Centre for Internet and Society and Research ICT Africa, November 2021).

3 World Bank, *ID4D Global Dataset: Volume 1 | 2021 Global ID Coverage Estimates* (Washington DC: World Bank Group, 2022), 23.

4 Van der Spuy et al., *Towards the Evaluation*.

public and private sector transactions and services'.⁵ The implementation of this also varies between African states, with some displaying higher levels of deployment than others.⁶

In their efforts to upscale the roll-out of national ID to meet the Sustainable Development Goals (SDGs), many African states have turned to digital options to facilitate foundational identity management. The term 'digital identification' refers to the process of 'converting paper-based legal identities into digital data which can be processed by machine systems'.⁷ But digital identification, while it has many benefits, comes with its own set of challenges.

If not implemented with care and impartiality, digital identification could lead to the exclusion and marginalisation of sections of the population in a more intense manner than with paper-based ID documents. This policy briefing explores the benefits and challenges related to the implementation of digital identification systems in Africa, drawing on the examples of Ethiopia and Uganda. It also looks at concerns around the types of data collected for these systems.

Why digital ID? And why now?

The provision and possession of a legal identity is recognised as important for promoting development and forms part of the UN's Sustainable Development Agenda and related SDGs. Under SDG 16.9, states have committed to provide 'legal identity for all, including birth registration', by 2030.⁸ The AU also considers this ideal important for achieving the objectives of Agenda 2063, its long-term development plan.⁹ In its Digital Transformation Strategy for Africa (2020–2030), the AU maintains that 'rapid modernisation and urbanisation', coupled with 'the increasing sophistication of commercial transactions', have reinforced the clear necessity of legal identity.¹⁰

The AU attributes the current push for digital identification to 'recognition of the fact that the economy in Africa must evolve or even transform in order to achieve sustainable, inclusive growth'.¹¹ More specifically, digital identification and a standards-based approach to govern it – what the AU's Digital Transformation Strategy aims to establish – are regarded as advantageous for the smooth functioning of the African Continental Free Trade Area and reaping its many hoped-for benefits.¹²

5 World Bank, "Practitioner's Guide: Identification for Development (ID4D)", [https://id4d.worldbank.org/guide/glossary#:~:text=Foundational%20identification%20\(ID\)%20system,private%20sector%20transactions%20and%20services](https://id4d.worldbank.org/guide/glossary#:~:text=Foundational%20identification%20(ID)%20system,private%20sector%20transactions%20and%20services).

6 Van der Spuy et al., *Towards the Evaluation*.

7 Kristophina Shilongo, "Digital ID 101: Making Sense of Key Terminology", Digital ID Dispatches from Africa, June 25, 2021.

8 The Global Goals, "Goal 16: Peace, Justice and Strong Institutions – Target 16.9", <https://www.globalgoals.org/goals/16-peace-justice-and-strong-institutions/>.

9 AU, "The Digital Transformation Strategy for Africa (2020–2030)", May 18, 2020.

10 AU, "The Digital Transformation Strategy", 41.

11 AU, "The Digital Transformation Strategy", 40.

12 AU, "The Digital Transformation Strategy"; Van der Spuy et al., *Towards the Evaluation*.

The drive for digital ID is part of a global shift towards the digital migration of traditionally analogue or paper-based systems. In Africa specifically, interest in digital identification grew as mobile technology became more widespread.¹³ Furthermore, digital ID is being rolled out precisely when digital infrastructure, which includes 'internet coverage, security, biometric technology, smart devices, and cloud services', is expanding.¹⁴

Paper-based identification documents are vulnerable to theft, damage and loss, placing their bearers at risk of identity theft and fraud. It has therefore become common for digital ID systems to include biometric data such as fingerprints or iris scans, alongside photos of the bearer. The inclusion of biometric data in ID documents is an extra layer of security and is more difficult for criminals to forge. Research has also indicated that digital identification has become an attractive option for African states as they embrace progress in the digital technology field and because of the 'relative ease, low cost, and convenience' of digital ID systems.¹⁵

But there are several concerns around the implementation of digital ID systems. Because they store sensitive and personal information, privacy should be paramount and breaches through cyberattacks are a major concern. Without safeguard mechanisms, especially in authoritarian contexts, state critics and members of the opposition are particularly vulnerable. The development of digital and information and communications technology infrastructure in Africa is also uneven. The precise use of the data collected and stored, whether it is shared between public and private entities, access to this data, the nature of its collection and criteria for inclusion are all risk factors that should carefully be considered before the roll-out of digital ID systems.¹⁶ It is also important that such systems are supported by strong legal mandates for data protection, privacy and transparency, clearly stating how data will be stored and collected and for what purpose.

Ethiopia: Fayda

Fayda ('value' in Amharic) is the name of the biometric digital ID programme introduced in Ethiopia, where the government plans to enrol all eligible adults in the system by 2025.¹⁷ A pilot project was announced for the roll-out of the ID in 2021 and completed in 2022, culminating in the first 100 000 registrations.¹⁸ Yodahe Zemichael, Executive Director of the National Identity Program (NIDP), says that the pilot project delivered many lessons on the implementation of the digital ID system. Most importantly, Zemichael says, the national ID authority should not be regarded as 'a one-stop shop where all the data about

13 Van der Spuy et al., *Towards the Evaluation*.

14 AU, "The Digital Transformation Strategy", 40.

15 Van der Spuy et al., *Towards the Evaluation*, 3; AU, "The Digital Transformation Strategy".

16 Anri van der Spuy, "Introducing the Digital ID Dispatches from Africa Series", Centre for Internet and Society, India, June 18, 2021.

17 Zecharias Zelalem, "Ethiopia's New Biometric ID System Raises Concerns of Deadly Ethnic Profiling", *Business Day*, February 1, 2023.

18 Ayang Macdonald, "Ethiopia Plans Upgrades to Meet 10m Digital IDs Target by 2023, Draft Law Approved", *Biometric Update.com*, August 15, 2022.

an individual, resident or citizen is found'.¹⁹ Rather, such bodies should restrict the amount of data collected from their subjects and prioritise transparency, so registrants are always informed about when and how their data is being used.²⁰

According to the NIDP, there are currently 1 438 351 registrations and counting.²¹ The NIDP aims to register and issue digital IDs to 10 million people in 2023.²² Those 18 years and older make up 54.1% of the country's total population of nearly 120 million.²³ Fayda is envisioned to become the primary foundational ID management system in the country and will take over several functional ID tasks, as it is incorporated into the financial sector for 'Know Your Customer' (KYC) purposes, the civil registry, and overall plans for Ethiopia's digital economic transformation.²⁴ Functional ID is sector-specific, for example, voter identification cards or, in the case of Ethiopia, the kebele (Amharic for 'ward') residence card,²⁵ whereas foundational ID has a more general use and can be applied universally.²⁶ Fingerprints and iris scan biometrics are collected for the Fayda digital ID system in addition to facial biometrics for authentication and KYC purposes specifically.²⁷

Teferei Fikre, Chief of Staff in the Office of the Prime Minister, has said that Fayda will²⁸

guarantee citizens' right to recognition, expand the opportunities to use various social and economic rights, foster trust in the relationship between the service provider and recipient, and establish a system of transparency, accountability, and streamlined operation at the national level.

Apart from certain functional ID documents such as the kebele card, Ethiopia did not have a foundational legal identity system in place prior to Fayda.²⁹ Kebele cards are identification documents issued by authorities at the ward (kebele) level to residents of that area over the age of 18. In the absence of a national foundational ID system, these documents have fulfilled many such functions in the country.³⁰ By introducing a foundational ID system, Ethiopia's citizens will be able to fully access the multitude of social, economic, legal and political rights to which they are entitled, and which have rightly been acknowledged by key officials.

19 Quoted in Chris Burt, "Ethiopia's National Digital ID Prepares Foundation Ahead of Scale-up", Biometric Update.com, October 3, 2022.

20 Burt, "Ethiopia's National Digital ID".

21 NIDP, "Fayda for Ethiopia", <https://id.gov.et/>.

22 Macdonald, "Ethiopia Plans Upgrades".

23 Simon Kemp, "Digital 2022: Ethiopia", Datereportal, February 15, 2022.

24 Burt, "Ethiopia's National Digital ID".

25 Lucas Kitzmüller, "Let's Get Digital? Policy Options for Ethiopia's ID System", *Medium*, December 12, 2020.

26 World Bank Group, "Practitioner's Guide: Types of ID Systems – Identification for Development (ID4D)", <https://id4d.worldbank.org/guide/types-id-systems>.

27 Macdonald, "Ethiopia Plans Upgrades".

28 Quoted in Burt, "Ethiopia's National Digital ID".

29 Kitzmüller, "Let's Get Digital?".

30 Kitzmüller, "Let's Get Digital?".

Registration for the Fayda system is not mandatory, and citizens will be allowed to continue using their kebele cards.³¹ But the kebele system, when compared with a sophisticated system such as Fayda, is unreliable, as there are no centralised backups of the records. Damage to or loss of this document are therefore legitimate concerns.³² By continuing to use the kebele card and not registering for the digital ID, citizens could also risk exclusion from certain services and sectors that rely on the functionalities digital identification will enable. Indeed, as argued in an analysis of Ethiopia's Draft Digital Identification Proclamation (presented to the country's federal parliament in 2022), 'government or private entities may condition provision of services on possession of digital identity'.³³ In addition, 'if the provision of a public or private service relies on biometrics verification, possession of digital identity will be mandatory'.³⁴

Civil society activists and other experts have also raised several concerns about the Fayda system being used in a discriminatory fashion and for ethnic profiling. While the Fayda ID will not capture someone's ethnicity, experts warn that this may still be deduced from that person's name – information that will form part of the ID – and that ethnic profiling could be enabled in this way. Several legal routes have been proposed to ensure personal data protection, but activists fear that 'enforcement is not assured'.³⁵ This fear may have grown out of the identification system in place at the ward level, where registrants' religion and ethnicity are recorded. Although not present on ID cards, this data is still stored in administrative databases.³⁶ There are also growing fears that the adoption of digital ID might see human rights defenders and state critics come under increasing scrutiny and possible surveillance. Such tactics were used against the so-called 'Zone 9 bloggers' – state critics charged with terrorism in 2014.³⁷

Experts and activists are concerned that the personal data collected for the digital ID system may be 'misused', and that 'the benefits promised by a digital ID system are outweighed by the potential risks'.³⁸ This is a common critique of digital ID systems. Organisations such as the World Bank and the UN have in the past been accused of deploying digital ID systems in 'conflict-prone regions without adequate safeguards to prevent data misuse or rights abuses'.³⁹

Concerns about the implementation of the Fayda system in Ethiopia are also tied to the fact that the country has no data protection laws, despite several attempts at adopting such legislation.⁴⁰ There is also an 'overall apathy towards privacy and data protection in

31 Zelalem, "Ethiopia's New Biometric ID".

32 Kitzmüller, "Let's Get Digital?".

33 Kinfe Yilma, "On Ethiopia's Digital ID Bill, Data Privacy, Warts and All", *Mizan Law Review* 16, no. 2 (2022): 456.

34 Yilma, "On Ethiopia's Digital ID Bill", 456.

35 Zelalem, "Ethiopia's New Biometric ID".

36 Yilma, "On Ethiopia's Digital Bill".

37 "Ethiopia Zone 9 Bloggers Charged with Terrorism", *BBC News*, July 18, 2014.

38 Zelalem, "Ethiopia's New Biometric ID".

39 Zelalem, "Ethiopia's New Biometric ID".

40 Yilma, "On Ethiopia's Digital ID Bill".

the country'.⁴¹ Furthermore, Ethiopia has neither signed nor ratified the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention), adopted in 2014 and in force since 8 June 2023.⁴² Implementation of the digital ID programme and related data collection is therefore going ahead without a legislative framework governing data protection.

Finally, the act of capturing biometrics itself can be exclusionary, especially in cases where a registrant is unable to present fingerprints, as is often the case with manual labourers, persons living with disabilities and the elderly.⁴³ However, an official from the Ministry of Justice in Ethiopia has said that alternatives to fingerprint biometrics will be available to accommodate such persons.⁴⁴

Uganda: Ndaga Muntu

Uganda's national biometric digital ID, Ndaga Muntu, was introduced in 2015 as mandatory for all citizens. Ndaga Muntu, which means 'identity card' in Luganda, refers to 'the physical ID card... and to the system itself'.⁴⁵ The project arose out of a national security initiative, the National Security Information System (NSIS) launched in 2014 to 'reform civil registration and identification ahead of the 2016 elections'.⁴⁶ Without the digital ID, Ugandans are unable to access public services such as healthcare and social grants. It is also necessary for private services such as 'opening a bank account, buying a mobile SIM card, enrolling in college, gaining formal employment and getting a passport'.⁴⁷

Eight years after its introduction, around one-third of the country's population reportedly still do not have the digital ID.⁴⁸ A study conducted on the project by the Centre for Human Rights and Global Justice, Initiative for Social and Economic Rights and Unwanted Witness confirms this finding. It further notes that 'Ndaga Muntu has led to mass exclusion... and has become a barrier for women and older persons, as well as many other marginalised individuals, to access their human rights'.⁴⁹

Failure to register under the digital ID system has been tied to unsuccessful ID applications because of the inability to present documentation proving citizenship, such as a birth

41 Yilma, "On Ethiopia's Digital ID Bill", 465-466.

42 AU, "Convention on Cyber Security and Personal Data Protection", <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

43 Zelalem, "Ethiopia's New Biometric ID".

44 Burt, "Ethiopia's National Digital ID".

45 Centre for Human Rights and Global Justice, Initiative for Social and Economic Rights and Unwanted Witness, *Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons* (New York and Kampala: CHR&GJ, ISER and Unwanted Witness, June 8, 2021), 78.

46 Neema Iyer, *Digital Identity in Uganda: Case Study Conducted as Part of a Ten-Country Exploration of Socio-Digital ID Systems in Parts of Africa* (Cape Town: CIS and RIA, 2021), 11; see also CHR&GJ, ISER and Unwanted Witness, *Chased Away and Left to Die*.

47 Nita Bhalla, "Uganda Sued Over Digital ID System that Excludes Millions", *Reuters*, May 16, 2022.

48 Bhalla, "Uganda Sued Over Digital".

49 CHR&GJ, ISER and Unwanted Witness, *Chased Away and Left to Die*, 8.

certificate or a marriage certificate. This has had a particularly negative impact on those married in traditional wedding ceremonies or who were born at home or in rural areas.⁵⁰ The digital ID was also made a requirement for receiving a COVID-19 vaccine in 2021. However, the intervention of civil society organisations saw this exclusionary requirement overturned.⁵¹ As part of the registration process for the ID card, those enrolling must also provide fingerprints and facial biometrics.

The Ndaga Muntu system has received widespread criticism for errors made by officials at registration, such as incorrect spelling of the bearer's name and dates of birth being mis-recorded. In one notorious example, a senior citizen could not claim a monthly welfare grant for two years owing to his date of birth being recorded incorrectly at the time of registration.⁵² The system has also been called over-dependent on manual or paper-based documentation processes and criticised for failing to present alternatives for those registrants unable to present fingerprint and facial biometrics.⁵³ As one critic put it, these shortcomings have led to 'a situation that has all the negatives and none of the positives' of digital identification.⁵⁴

The Ugandan digital ID system collects a large amount of personal data: 'name, date of birth, gender, information on citizenship, place of birth, details of parents, clan, tribe, ethnicity, spouse, education, tax information, personal biometrics information... as well as any other information as may be required'.⁵⁵ Capturing all this data opposes the 'principles of data minimisation' often associated with digital ID.⁵⁶ It also heightens the risk of ethnic profiling and surveillance. This becomes especially evident when considering that the Ndaga Muntu ID will become the only valid method of identification for accessing public and private services in Uganda.⁵⁷

Unlike Ethiopia, Uganda does have a legal framework governing data privacy, which is provided for under Article 27 of the country's constitution.⁵⁸ The Data Protection and Privacy Act was passed in May 2019, while the Data Protection and Privacy Regulations took effect in March 2021. This framework places several restrictions on the collection, transfer and processing of personal data.⁵⁹ But, like Ethiopia, Uganda is yet to sign and ratify the Malabo Convention.⁶⁰

50 Iyer, *Digital Identity in Uganda*, 11.

51 Iyer, *Digital Identity in Uganda*.

52 Bhalla, "Uganda Sued Over Digital".

53 Iyer, *Digital Identity in Uganda*, 18; see also CHR&GJ, ISER and Unwanted Witness, *Chased Away and Left to Die*.

54 Iyer, *Digital Identity in Uganda*, 18.

55 Iyer, *Digital Identity in Uganda*, 19.

56 Iyer, *Digital Identity in Uganda*, 19.

57 Iyer, *Digital Identity in Uganda*.

58 DLA Piper, *Data Protection Laws of the world: Uganda*, 2022.

59 DLA Piper, "Data Protection Laws".

60 AU, "Convention on Cyber Security".

Section 66 of the Registration of Persons Act (ROPA) of 2015 mandates the ID as a requirement to access basic services.⁶¹ In one critic's view, this is evidence of an undeniable 'imbalance in the benefits accruable to citizens under the scheme'.⁶²

[It] strips away several of the fundamental rights already afforded to Ugandan citizens under the Constitution, while demanding an extreme amount of information, to grant them – again – access to those very rights and risks fomenting exclusion against persons unwilling or unable to register.

A consortium of civil society and rights organisations in Uganda sued the government in April 2022 because of the exclusionary elements of the digital ID programme. More concerns were raised recently when reports surfaced that the next iteration of the digital ID in Uganda, to be introduced in 2024, will also capture DNA biometrics.⁶³

Conclusion

The implementation of digital ID is a development likely to stay once in place. As cases of fraud and identity theft increase across the globe, additional modes of security are often incorporated. Including biometrics in the digital ID system is a good way of ensuring authenticity, but these systems are susceptible to human error, technical glitches and possible hacking. Additionally, while inclusion is often cited as a primary reason for introducing biometric digital ID, the examples of Ethiopia and Uganda both illustrate the exclusionary possibilities of such systems. Increasing the amount of information held in state ID databases could also hold potential danger, especially in contexts susceptible to ethnic conflict.

While it is important that citizens and the state are connected in this manner, implementing authorities should safeguard the personal data gathered. Handling sensitive information requires a strong legal framework that will ensure that privacy and data protection laws are enforced and oversight mechanisms implemented. The AU, in working towards a standardised framework for incorporating digital technology in governance practices, also has a responsibility to the citizens of African states to ensure that their governments implement ID projects that are truly inclusionary and mindful of the protection of their citizens.

61 Iyer, *Digital Identity in Uganda*, 32.

62 Iyer, *Digital Identity in Uganda*, 32.

63 Tyler Choi, "Concerns Raised as Uganda Plans DNA Upgrade for Biometric ID Cards", *Biometric Update.com*, May 17, 2022.

Author

Isabel Bosman

is a Researcher in the African Governance and Diplomacy Programme at SAIIA. She holds an MA in Political Studies from the University of the Witwatersrand. Her research focuses on the nexus between technology and politics, with particular interest in biometrics and electronic voting. She also studies African elections, democracy, and nuclear energy governance.

Acknowledgement

SAIIA gratefully acknowledges the support of SIDA for this publication.

About SAIIA

SAIIA is an independent, non-government think tank whose key strategic objectives are to make effective input into public policy, and to encourage wider and more informed debate on international affairs, with particular emphasis on African issues and concerns.

SAIIA's policy briefings are intended for use by policymakers, whether in government or business. They are concise, providing a brief analysis of the issue at hand, and make policy recommendations.

Cover image

Vertigo3d/Getty Images

All rights reserved. Copyright is vested in the South African Institute of International Affairs and the authors, and no part may be reproduced in whole or in part without the express permission, in writing, of the publisher. The views expressed in this publication are those of the author/s and do not necessarily reflect the views of SAIIA.

Please note that all currencies are in US\$ unless otherwise indicated.



Jan Smuts House, East Campus, University of the Witwatersrand
PO Box 31596, Braamfontein 2017, Johannesburg, South Africa
Tel +27 (0)11 339-2021 · Fax +27 (0)11 339-2154
www.saiia.org.za · info@saiia.org.za