

LEVERAGING MOBILE TO ACCELERATE DIGITAL IDENTITY ECOSYSTEMS: CONSIDERATIONS FOR POLICYMAKERS IN AFRICA

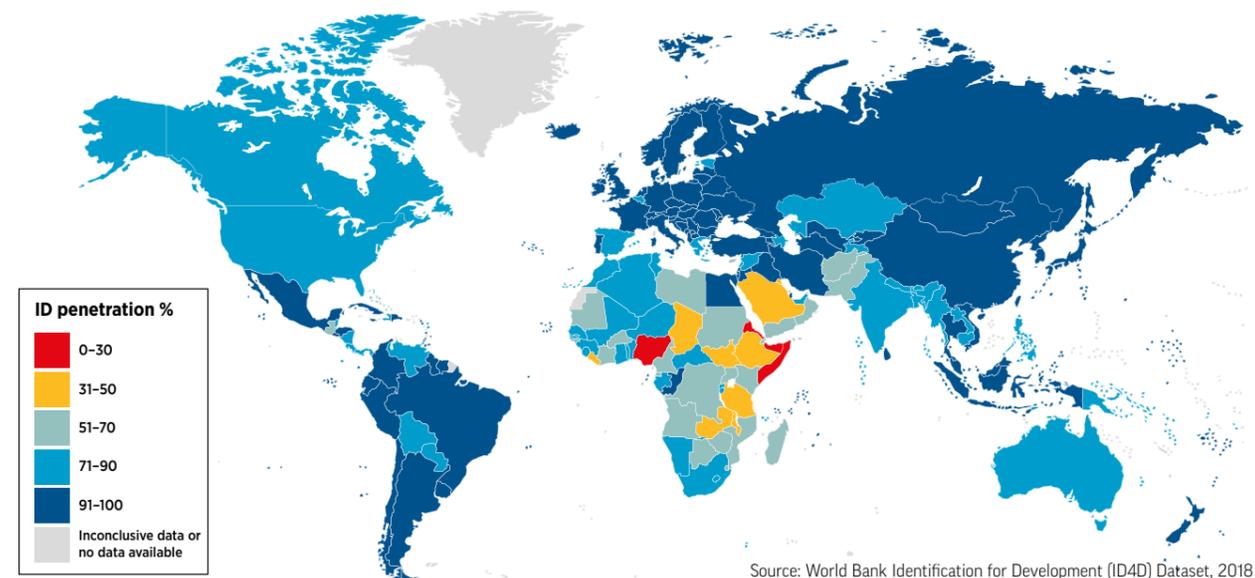
WRITTEN BY YIANNIS THEODOROU, DIRECTOR OF POLICY AND REGULATORY AFFAIRS, DIGITAL IDENTITY

As African countries continue their journeys towards 'digital transformation' of their economies, national identity authorities have a crucial role to play in ensuring that every single resident of Africa can actively participate in the new digital economy. For this to happen, building an inclusive and accessible digital identity ecosystem that also caters for the needs of Africa's underserved populations is a must. A digital identity is increasingly becoming a prerequisite to access a plethora of basic life-enhancing services including healthcare,

education, banking and exercising one's right to vote in a democratic election. Yet, according to the World Bank, an estimated one billion people around the world lack any legal (state-issued or recognised) identification and are arguably 'invisible' in many formal respects (figure 1). About half of these people live in Sub-Saharan Africa and most are likely to be women and/or forcibly displaced e.g. refugees or those affected by humanitarian crises.

Figure 1

Share of total population estimated to have an official form of identification (2018)



Proof of identity and access to mobile in one's own name

Access to formal identification is also—increasingly—a prerequisite for registering for a prepaid (or Pay-As-You-Go) mobile phone SIM card in one's own name. More than five billion unique individuals (figure 2) have a mobile subscription, with 3.6 billion having a mobile internet subscription. A mobile phone can be the primary medium through which we can assert our digital identity where appropriate. In many parts of Africa and developing markets, mobile is already playing a key role in unlocking access to several mobile-enabled services, such as mobile money accounts, Pay-As-You-

Go energy, water and sanitation services, educational, health and other digital services. For example, for many of the 690 million people who have a registered mobile money account, a mobile phone is their main, if not their only, means to receive, send and save money.

However, having a unique mobile subscription in most countries is predicated on presenting proof of identity. A recent global study by the GSMA¹ found that governments in 150 countries (figure 3) require mobile users to present proof of identity when registering for a prepaid (Pay-As-You-Go) SIM card in their own name. This is the case in 50 countries in Africa who frequently cite 'security' concerns for

implementing mandatory SIM registration even though no empirical evidence yet exists to demonstrate a link between the introduction of this policy and a reduction in crimes involving mobile communications. Given that 94 per cent of all mobile SIM cards in Africa are prepaid (figure 4), it is crucial that such SIM registration policies are proportional and reflective of people's ability in each country to meet the identification requirements. Individuals who lack a proof of identity face a higher risk of social, digital and financial exclusion where they cannot meet mandatory identification requirements for registering a SIM card in their own name. It is important to recognise that when people lack such proof of identity they may well rely on friends and relatives to register a SIM card on their behalf, or seek to obtain activated SIM cards on 'black markets'. However, while such formal and informal 'work-arounds' may exist, the inability to access mobile services in one's own name could amount to a missed-opportunity for that individual to be properly digitally and financially included; As countries' digital transformation plans—including eGovernment services—are advancing it will become imperative that individuals are able to prove their identities both offline and online. Mobile may well be the medium through which one's digital identity could be asserted to access such services online.

Digital identity verification is still nascent in the context of mobile SIM registration

A number of studies by the World Bank suggest that an inclusive and robust² digital identity ecosystem can offer significant benefits to private³ and public⁴ sector entities by enabling strong, remote verification of individuals' identification credentials, which then unlocks access to a host of relevant services. Despite the high number of governments mandating mobile SIM card registration, only 11 per cent of these globally (and only six per cent of African countries – figure 5) enable mobile network operators (MNOs) to verify customers' identification credentials against an approved government database to facilitate the accuracy of the validation process. It is therefore not surprising that a number of ID authorities across Africa are now looking to offer online identity verification capabilities to selected public and private sector entities.

Millions of undocumented people are still financially excluded but mobile money offers a huge potential to bridge the gap

The impact of mobile money in supporting the financial inclusion of the world's underserved populations is well documented. Due to the convenience, safety and affordability of transacting via mobile money over traditional financial institutions, the industry will continue to play a key role in bringing the 1.7 billion people who remain financially excluded into the formal financial sector⁵ worldwide. However, while mobile money services are available in 90 countries worldwide,⁶ an estimated 456 million individuals across these countries (most of them in Africa) may be at risk of financial exclusion due to their inability to meet the identification/ Know Your Customer (KYC) requirements for opening mobile money accounts in their own names. This highlights an urgent need for identity authorities, central banks and Telecommunications Regulators to join forces in an effort to ensure consistency and proportionality across the various identity related policies under their respective mandates.

Lack of official identification is disproportionately impacting refugees and other forcibly displaced persons

The humanitarian community is increasingly focused on how to ensure those in need of assistance are equipped with acceptable forms of identification which would allow them to access mobile connectivity and mobile money services in their own name.⁷ One hundred and seventy three countries are hosts to 19.9 million refugees. Yet, 75 per cent of these countries legally require⁸ people to present an acceptable form of identification in order to register for a mobile SIM card. Similarly, 81 refugee-hosting countries offer mobile money services which could potentially be available to 54 per cent of all refugees (but for their ability to meet the KYC requirements for opening a mobile money account in their own name). A key policy consideration for host-country governments⁹ (in the context of addressing proof of identity barriers faced by refugees) is to understand and reflect what forms of identification most refugees have

1. GSMA (2018-2019). 'Access to Mobile Services and Proof of Identity'. See: www.gsma.com/mobilefordevelopment/resources/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks
 2. World Bank (2018). 'G20 Digital Identity Onboarding'. See: www.gpfi.org/sites/default/files/documents/G20_Digital_Identity_Onboarding.pdf
 3. World Bank (2018). 'Private Sector Economic Impacts from Identification Systems'. See: <http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpactsIDSystems-Web.pdf>
 4. Ibid.
 5. World Bank Group (2018). 'The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution'. See: https://globalfindex.worldbank.org/sites/globalfindex/files/2018-04/2017%20Findex%20Full%20Report_0.pdf
 6. GSMA. 'State of the Industry Report on Mobile Money 2018'. See: www.gsma.com/mobilefordevelopment/sotir/
 7. UNHCR (2019). 'Displaced and Disconnected'. See: www.unhcr.org/innovation/displaced-and-disconnected/
 8. GSMA (2018-2019). 'Access to Mobile Services and Proof of Identity'. See: www.gsma.com/mobilefordevelopment/resources/access-mobile-services-proof-identity-global-policy-trends-dependencies-risks
 9. GSMA (2017). 'Enabling Access to Mobile Services for the Forcibly Displaced'. See: www.gsma.com/mobilefordevelopment/resources/enabling-access-mobile-services-forcibly-displaced



access to, which could be deemed acceptable for meeting such proof of identity requirements in the immediate aftermath of their displacement. A new research report¹⁰ by the UNHCR, supported by the GSMA, looks into the identification requirements that forcibly displaced persons face in the context of accessing mobile services, across 20 host-countries. For example, the research found that in Zambia refugees can use their Proof of Registration, Refugee Certificates and Refugee Cards as valid proof of identity to complete SIM registration and mobile money registration. Such interim policies¹¹ could be put in place until official recognition of a refugee's status is complete—a process that can take months or years.¹²

Privacy frameworks can encourage uptake of digital identity and adoption of identity linked mobile services

Linking their identity data with their mobile SIM card may raise another question for many mobile users: *Will this impact my privacy?* Actual or perceived risks to people's privacy may adversely affect their willingness to register a SIM card or sign up to identity linked mobile services in their own names. GSMA research has found that only 61 per cent of the countries mandating prepaid SIM registration have a privacy/data protection framework in place.¹³ This is also true for 54 per cent of all African countries (figure 6).

Figure 2

Unique mobile subscribers as a proportion of total population (2018)

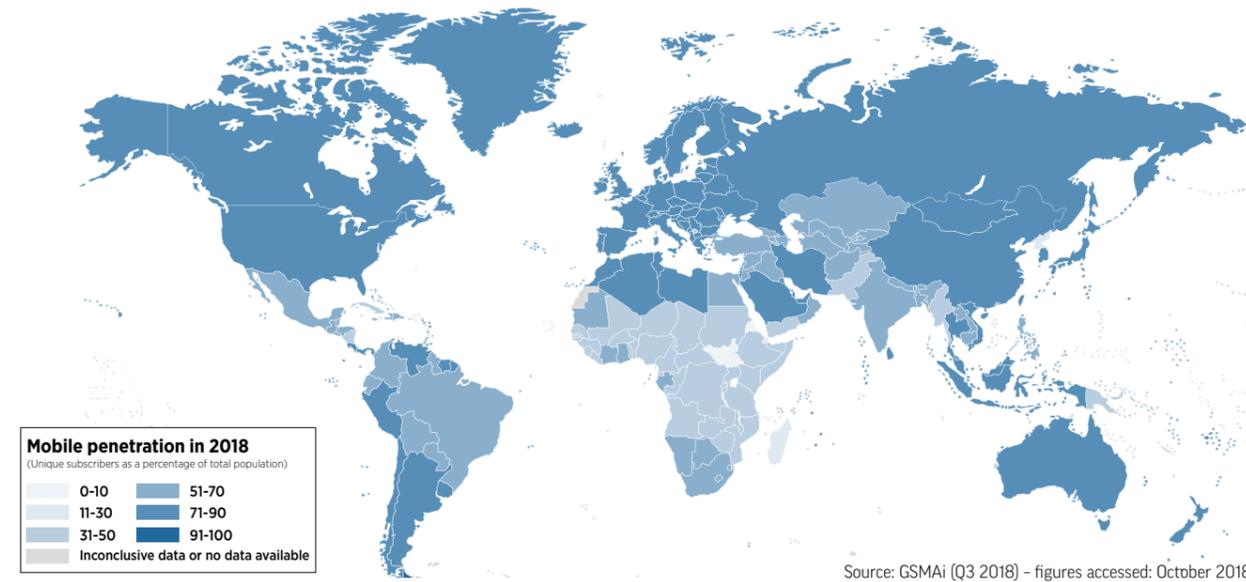
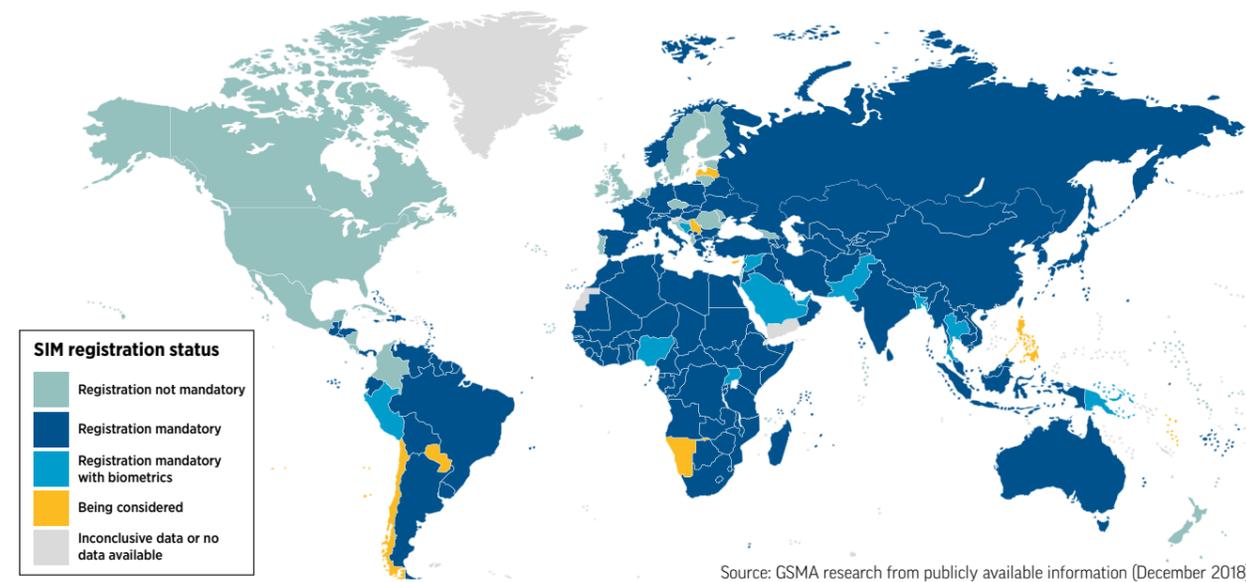


Figure 3

Status of SIM registration policies (2018)



10. UNHCR (2019). 'Displaced and Disconnected'. See: www.unhcr.org/innovation/displaced-and-disconnected/

11. GSMA (2019). 'Overcoming the Know Your Customer hurdle: Innovative solutions for the mobile money sector'. See: www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/01/Overcoming-the-KYC-hurdle-Innovative-solutions-for-the-mobile-money-sector.pdf

Figure 4

Share of prepaid connections as a percentage of total mobile subscriptions, Africa

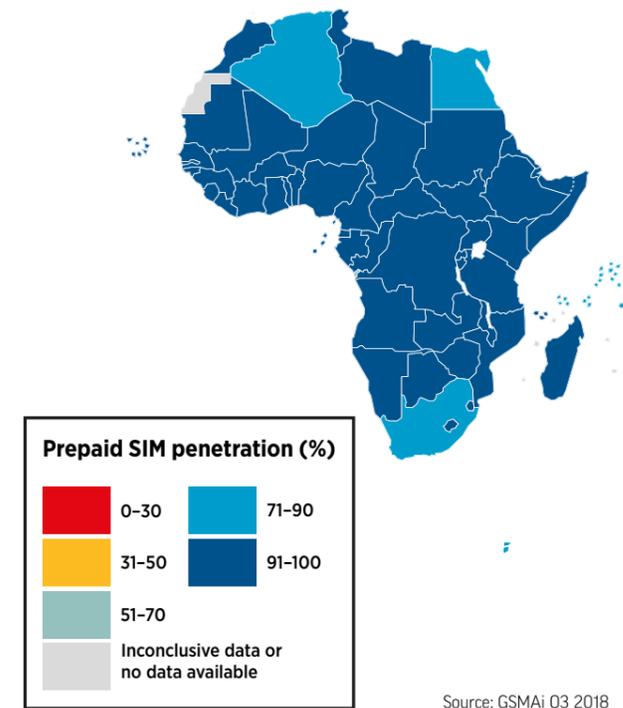


Figure 5

Type of mandatory SIM registration policy, by country in Africa

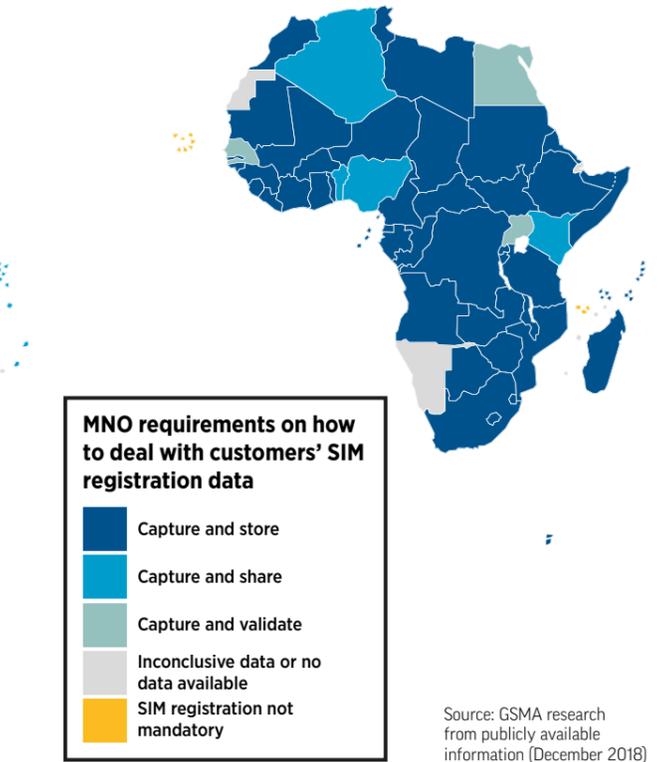
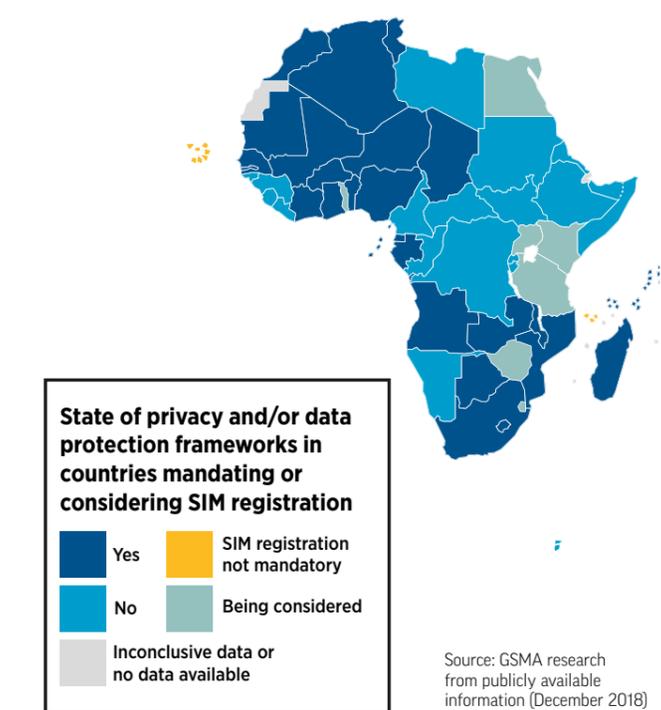


Figure 6

State of privacy/data protection frameworks in countries mandating SIM registration, Africa



As the world's economies increasingly 'go digital', governments carry a responsibility to foster and help create a trusted environment where consumers' privacy is respected and their privacy expectations are met. Mobile network operators are often subject to a range of laws and/or licence conditions that require them to support law enforcement and security activities in countries where they operate. These requirements vary from country to country and may have an impact on the privacy of mobile customers. The retention and disclosure of data and the interception of communications for law enforcement or security purposes should take place only under a clear legal framework and using the proper process and authorisation specified by that framework. Given the expanding range of communications services, the legal framework should be technology neutral. Proportionate and clear data protection and privacy frameworks, which are based on international best practices, are likely to encourage user adoption of digital identity-linked services, support transparency and operational effectiveness. Ultimately, having effective and sector-agnostic privacy frameworks is about building and maintaining high levels of trust in digital and mobile ecosystems.

It is also not surprising that the World Bank's first 'Mission Billion Challenge'¹⁴ was focused on inviting innovative ideas from all over the world on how to operationalise 'Privacy-by-Design' principles in digital identity applications.

12. GSMA (2017). 'Refugees and Identity: Considerations for Mobile-Enabled Registration'. See: www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/08/TWP81_1_DigitalIdentityProgrammeReport_WebSingles_R.pdf

13. While national legal frameworks generally seek to meet mobile users' privacy needs and expectations, their actual scope varies from country to country.

14. World Bank ID4D, Mission Billion. See: <http://id4d.worldbank.org/missionbillion>

Role of mobile in facilitating identity enrolment through Public-Private-Partnerships

Mobile continues to connect more people than any other communications platform. By the end of 2018, 67 per cent of the total population had a mobile subscription, with 49 per cent of Africans having a unique mobile subscription. The World Bank's latest global FINDEX survey¹⁵ found that registering for a mobile SIM card is the most prevalent use of identification across all countries surveyed, for both men and women. This also suggests that the willingness to register a SIM card in one's own name is driving demand for acquiring a digital identity. For such demand to be met, people who currently lack a digital identity need to be able to easily sign up for one. Given the wide reach of mobile network operators (MNOs) through their nationwide retail presence and agent network, African governments have an opportunity to partner with them and leverage their capabilities to enrol millions of hard-to-reach and vulnerable groups of people who currently lack formal identification.

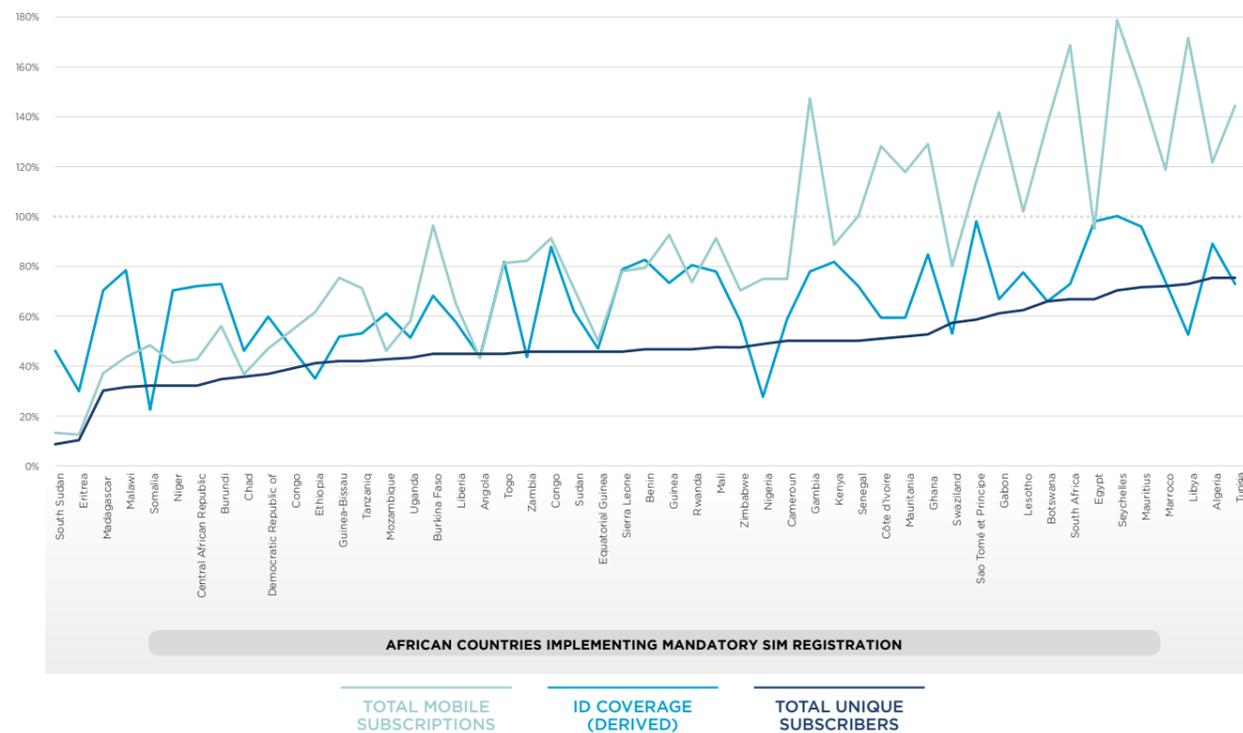
This model is currently being explored in Nigeria and could be particularly effective in other markets such as Somalia, Ethiopia, Swaziland, Zambia and Angola, (figure 7) where it appears there are more people with a unique mobile subscription than an official proof of identity.

Public-Private-Partnerships between MNOs and governments have also been successfully tested in the context of digital birth registration in countries such as Pakistan, Tanzania and Ghana.¹⁶

Figure 7

Identification coverage and mobile penetration across African countries where mobile SIM registration is mandatory

Percentage of population



Source: GSMA Intelligence, Market Penetration - Q3 2018 (accessed November 2018) and World Bank ID4D 2018 (number of registered individuals as a % of the population, taken as a proxy for identity penetration)

So what does this mean for policymakers working on their digital transformation strategies?

To improve social, political and economic inclusion, as well as engender trust in the digital ecosystem, an enabling policy and regulatory environment is essential. Elements of such an environment may include:

- Enabling all individuals to access formal identification;
- Coordination between government and sectoral regulators to ensure that the identity ecosystem can cater for the respective needs of each sector (financial, telecoms, health etc.), but also the specific needs of various consumer groups—including those marginalised and underserved;
- Ensuring proof of identity requirements when accessing mobile and digital services are:
 - clear and as harmonised as possible;
 - proportionate to people's ability to access an acceptable form of identification;
 - reflective of the risk of harm in a given context; and
 - sufficiently flexible to adapt to market developments.
- Fostering trust in mobile and digital identity ecosystems e.g. by establishing or maintaining privacy and data protection frameworks;
- Maintaining robust identification databases and empowering mobile operators to query these when validating customers' identification credentials at the point of SIM registration (where this is mandatory);
- Partnering with mobile operators, key stakeholders and the wider identification ecosystem to help drive identity

enrolment and access to innovative and interoperable solutions; and

- Encouraging adoption and usage of digital identity linked services (e.g. by investing in eGovernment and digital social protection portals for beneficiaries)

Given the vast reach of mobile technology, mobile platforms are uniquely placed to offer the most widespread and inclusive means of accessing the internet and digital technologies. The missing component to achieve this is access to official identification.

With just 11 years to meet the 2030 United Nations' Sustainable Development Goals (SDGs) and in particular SDG 16.9 of providing 'legal identity for all', there is a clear need for concerted action; governments, the development community, the mobile and financial services sectors and stakeholders from the wider identification ecosystem need to do their part to jointly address the proof of identity barriers preventing millions of people from accessing life-enhancing mobile services in their own name.

The GSMA's Digital Identity Programme is committed to supporting dialogue between these stakeholders in an effort to create more enabling environments where the needs of underserved groups are better catered for. This also involves advocating for and exploring various unique roles that its mobile operator members can play in bringing the benefits of digital identity to many of the poorest and hardest to reach individuals around the world.

If you would like to learn more about how we could work together please visit www.gsma.com/digitalidentity



15. World Bank ID4D, Global Dataset. See: <http://id4d.worldbank.org/global-dataset>

16. GSMA (2017), 'Innovations in Mobile Birth Registration: Insights from Tigo Tanzania and Telenor Pakistan'. See: www.gsma.com/mobilefordevelopment/resources/innovations-in-mobile-birth-registration-insights-from-tigo-tanzania-and-telenor-pakistan/