GSMA Digital Identity Programme: Insights and Achievements (2016–2020)

Exploring the role of mobile platforms, conducive policies and business models in strengthening digital identity ecosystems

April 2020

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in **Barcelona**, **Los Angeles** and **Shanghai**, as well as the **Mobile 360 Series** of regional conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**

Follow the GSMA on Twitter: **@GSMA**

Digital Identity

The GSMA Digital Identity Programme is uniquely positioned to play a key role in advocating and raising awareness of the opportunity of mobile-enabled digital identity and life-enhancing services. Our programme works with mobile operators, governments and the development community to demonstrate the opportunities, address the barriers and highlight the value of mobile as an enabler of digital identification.

For more information, please visit the GSMA Digital Identity website at **www.gsma.com/digitalidentity**

Follow GSMA Mobile for Development on Twitter: **@GSMAm4d**

This document is an output of a project funded by UK aid from the Department for International Development (DFID), for the benefit of developing countries. The views expressed are not necessarily those of DFID.

Contents

Introduction

The mission of the GSMA's Digital Identity programme is to leverage mobile technology as an enabler of digital identity and services that provide social and commercial value in developing markets. A person's ability to prove their unique identity is key to their economic, financial and social development. Without proof of identity, they are less likely to be able to access services like healthcare and education, assert their rights, vote in elections or fully participate in the analogue or digital world. However, according to estimates from The World Bank, one billion people still lack formal identification, 80 per cent of whom are in either Sub-Saharan Africa or South Asia.[1] Globally, those in low-income countries are the least likely to have access to ID, often for reasons related to outdated paper-based identity systems, cultural norms, poor communication channels between rural areas and identity registry offices, cumbersome registration processes, prohibitive costs and lack of awareness of the importance of having official proof of identity.

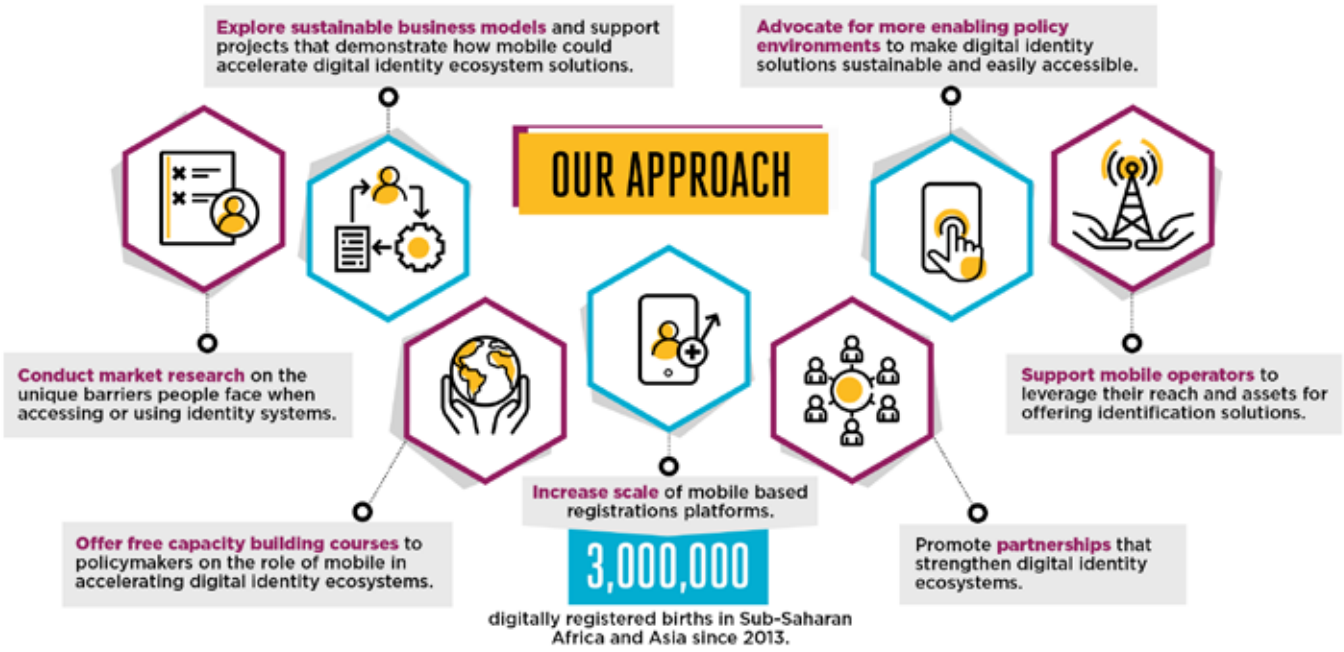
At the same time, the number of unique mobile subscribers has surpassed the five billion mark, highlighting the transformative potential of mobile technology to empower citizens, protect privacy and stimulate economic and social development through inclusive digital identity systems. No other technology has the reach, capability and integration in daily life to respond to this global challenge and provide public and private sector entities with efficient ways to reach the most underserved.

The GSMA Digital Identity programme is playing a key role in exploring, advocating and raising awareness of the opportunity mobile provides to improve access to official (foundational) identification (e.g. a national identity or birth certificate) and identity-linked services (e.g. access to mobile money, social payments or health services). The programme has worked with mobile network operators (MNOs), governments, intergovernmental organisations, private sector partners, non-governmental organisations (NGOs) and humanitarian agencies, to research and analyse the barriers vulnerable populations face in accessing or using ID; explore sustainable business models through pilots that demonstrate how mobile could accelerate digital identity solutions; and advocate for enabling policy environments and proportionate regulations that ensure digital identity ecosystems are inclusive and easily accessible.

1. See The World Bank, ID4D Data: Global Identification Challenge by the Numbers.

Figure 1

The GSMA's Digital Identity programme's approach to addressing the global identity gap challenge



Through these activities, which are described in detail in this report, we have identified opportunities for MNOs to:

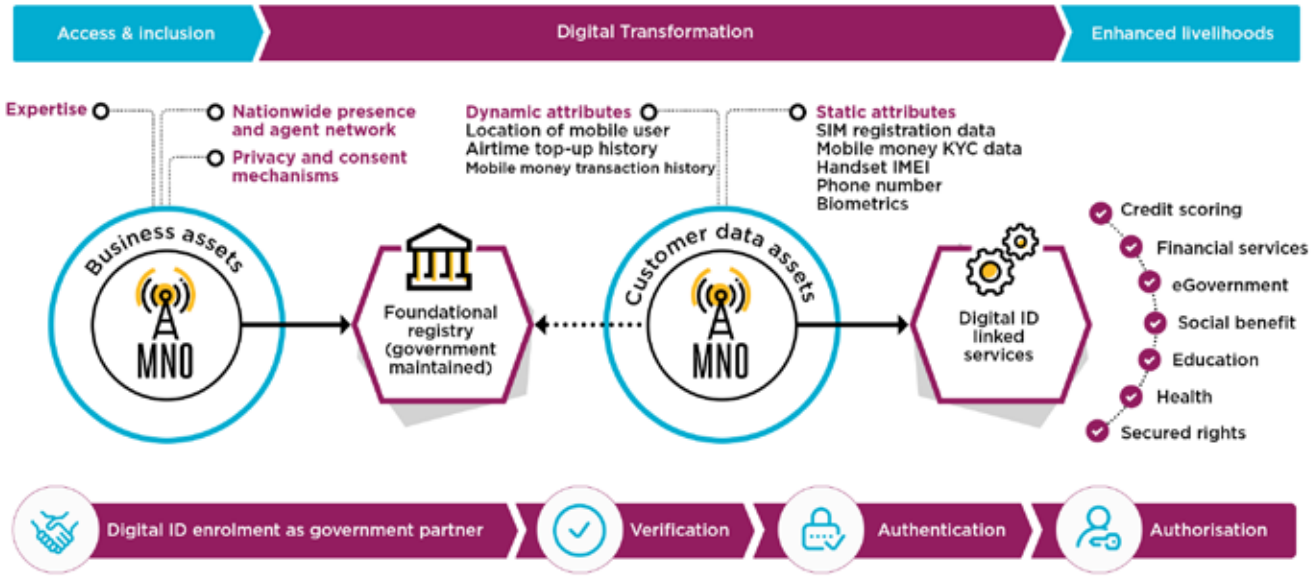
- Help **drive consumer demand** for official proof of identity through their customer relationship management channels, especially in the more than 150 countries where mobile SIM registration and Know Your Customer (KYC) processes are legally mandated to activate SIM cards and mobile money accounts. As the World Bank's latest Global Findex survey shows,[2] applying for a mobile SIM card or mobile service is the most prevalent use of identification in all countries for both men and women.
- **Leverage business assets to work with governments to improve access to foundational IDs.** Business assets, such as extensive agent and retail networks, established privacy practices and experience managing customers' personal data, can complement government efforts to enrol citizens in new or existing identity ecosystems with more efficient and inclusive methods. In Nigeria, for example, our Digital Identity programme has helped MNOs convene with the government and agree to partner with a view to accelerating enrolment in the country's new national digital identity ecosystem,[3] while digital birth registration projects in Pakistan and Tanzania have collectively registered the births of over four million children since 2013.[4]

2. World Bank (2018), Global ID Coverage by the Numbers: Insights from the ID4D-Findex Survey.
3. NIMC, The Digital Identity Ecosystem.
4. As of September 2019; figures were reported to GSMA by project partners.

- **Improve digital identity verification and unlock access to a wealth of digital or online services relevant to their customers' mobile use.** MNOs may be able to analyse customer data assets, including customer attributes that are either dynamic (e.g. call detail records, network mobility data, frequency of airtime top-ups, mobile money transactions, approximate geolocation) or static (e.g. KYC data, phone number or biometric information). This can allow them to improve the level of "identity assurance" for a mobile user attempting to access a digital service. It can also support the development of "functional" identities that would unlock access to certain services (e.g. improve the creditworthiness of an individual based on their mobile money transactional history and subsequent access to credit).
- Build on **established customer relationships and act as trusted partners** (to customers, governments, public sector organisations or other service providers) to enable access to a range of identity-enabled digital services, including credit scoring, mobile financial services (e.g. payments, savings, credit, insurance), e-government services, social payments and healthcare.

Figure 2

MNOs could play several roles in supporting a digital identity ecosystem



This report summarises the achievements and lessons of the Digital Identity team over the last four years, documenting how the programme has established the GSMA as a thought leader, convener and catalysing partner in digital identity for the underserved.

In section 1, we provide an overview of the various research reports, case studies and policy notes used to foster collaboration with key partners and other thought leaders, document specific examples of best practice and innovation in the digital identity space, or strengthen our ability to advocate for more inclusive and sustainable policy and regulatory environments. The programme has also helped address the "identity gap" by leveraging the value and reach of the mobile industry. **In section 2**, we outline how the team has built on momentum or stimulated new efforts to demonstrate how MNOs can work with partners to deliver innovative and secure digital identity solutions. These use cases include digital birth registration, identity for the forcibly displaced, understanding and mitigating identification barriers faced by women and girls, economic identities, identity verification in the context of social benefit disbursements, health identities and supporting identity enrollment and access to government services.

The most important lessons from this work are highlighted **in section 3**.

Background

In 2016, when GSMA Mobile for Development (M4D) launched its Digital Identity programme with the support of DFID, the role of identification (ID) in development was just beginning to gain traction. Despite being inextricably linked to other development priorities and outcomes, access to ID was often taken for granted. The UN Sustainable Development Goals (SDGs), specifically 16.9, "Legal identity for all, including birth registration, by 2030", focused the international community on the realities of the nearly one billion people who could not fully participate in either the analogue or digital world because they could not prove who they were.

Around the same time, the rapid scaling of the Aadhaar system in India, which provided all citizens with a 12-digit ID number and biometric authentication, shone a light on both the potential for, and challenges of, integrating technical solutions and private sector players in an official ID ecosystem. As our team was ramping up, it became obvious that a shared definition of "digital identity" did not yet exist. There was not sufficient evidence or consensus on the roles and responsibilities of the public and private sectors; what constitutes an inclusive and accessible ID ecosystem; what level of assurance different use cases would require; or what types of business models would have the greatest social and commercial impact.

Against this backdrop, the M4D Digital Identity programme focused its learning agenda on answering these questions and developing partnerships, such as with the World Bank's Identification for Development (ID4D) Initiative, that would help us forge a shared view of this nascent area of development.

Fast forward to 2020, and digital identity is booming, both in concept and in practice. Alliances have sprung up around the world to tackle different elements of the ecosystem, from technology to privacy and ethics. Governments, especially in countries with low ID penetration, are making reforms and investment in their identity infrastructure a priority, and are looking for new ways to work with the private sector and leverage technology to support these partnerships. Multistakeholder cooperation has led to shared principles and definitions, and there is early evidence that digital identity initiatives are having an impact and new business models are emerging.

1 Thought leadership

Since the launch of the Digital Identity programme in 2016, our team has published numerous research reports, case studies and policy recommendations that highlight the various roles of mobile in either closing the identity gap or providing digital identity solutions with a social and commercial impact. These activities have been designed to help the GSMA, our MNO members and development partners understand the scope and nature of the identity gap in developing countries; to identify possible use cases or business models for mobile industry engagement; and to educate policymakers and other stakeholders about the conditions that enable digital identity ecosystems to develop and scale.

The team has produced over 30 publications since 2016, most on digital identity use cases, such as digital birth registration or the development of mobile-derived identity profiles (these are discussed in more detail in section 2). Our other publications were designed to support our mission by fostering collaboration with key partners and thought leaders, such as the World Bank's Identification for Development (ID4D) team, UNICEF, UNHCR and a range of other public and private sector partners. Our research has also documented specific examples of best practices, innovations or digital trends related to digital identity, or supported the team's efforts to advocate for more inclusive and sustainable policy and regulatory environments.

The publications outlined in this section were showcased at a variety of conferences and global events, including:

- GSMA MWC Barcelona (2017–2019)
- GSMA's Mobile 360 Africa conference (2016–2019)
- GSMA's Mobile 360 India conference (2016)
- ID4Africa conferences (2017–2020)
- World Bank annual meetings (2017–2019)
- World Bank ID4D conferences (2017–2019)
- Columbia University Blockchain and Development Roundtable (2018)
- The Kenyan Government ICT Taskforce
- Omidyar Network workshops on Good ID (2018–2019)
- K(no)w Identity Conference 2017
- Vodafone Foundation Americas 2017
- GIS/DFID Meetings in Bonn
- FIGI Symposium 2019
- Mobile Connect Summit
- Several ITU and UN-hosted events

Collaboration with partners

In 2016, the Digital Identity programme co-authored a joint discussion paper with the World Bank and the Secure Identity Alliance (SIA): Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. One of the main objectives of this paper was to build consensus among diverse stakeholder groups on shared language and principles, and to argue for the importance of public-private partnerships in (digital) ID systems of the future, particularly in developing countries. Using examples from countries that have adopted digital identity systems, the paper illustrates how digital identity can promote efficiency, financial savings, social inclusion and access to basic services and rights. It also outlines some of the key risks and challenges that must be overcome with political commitment, data protection and privacy, costs and sustainable business models.

The paper suggests models for private-sector participation in foundational digital ID systems, and common principles for maximising the potential of digital identity to contribute to sustainable development. Based on a series of consultations, broad multistakeholder discussions and earlier research, the paper identified three foundational principles for national digital identity systems:

- **Universal coverage:** An officially recognised form of identity should be accessible to all individuals from birth to death.
- **Appropriate and effective design:** Identity systems should be appropriate to the context and adaptable to long-term needs, including measures to ensure demand, robustness, integrity and resilience, interoperability, proportionality, vendor and technology neutrality, and fiscal and operational sustainability.
- **Building and sustaining trust:** Identity systems must be built on a legal and operational foundation of trust and accountability between public agencies, private sector actors and individuals, who must be assured their data is private and protected, and they can control and oversee how it is used.

Following the publication of this initial report, the GSMA continued to work closely with the World Bank's ID4D team as they led a global effort to develop shared principles on identification. In 2017, the GSMA joined many other organisations in developing and endorsing the Principles on Identification for Sustainable Development: Toward the Digital Age. This joint publication outlined 10 principles grouped into three overarching themes: Inclusion (universal coverage and accessibility), Design (robust, secure, responsive and sustainable) and Governance (building trust by protecting privacy and user rights).

The report recognises that in order for legal identification systems to be effective and available to all (i.e. to the individuals who must prove their identity to access rights and services), there must be a coordinated and sustained effort by key stakeholders involved in the provision and use of these systems, including government, the private sector, international organisations and development partners. By using these Principles to shape a common approach to identification, it is hoped that stakeholders will be better able to align and guide their support, facilitate discussions at country, regional and/or global levels, and work together to foster robust and inclusive identification systems that advance sustainable development.

As of late 2019, over 25 organisations have endorsed the Principles on Identification: African Development Bank, Asian Development Bank, The Bill & Melinda Gates Foundation, Center for Global Development, Digital Impact Alliance, the GSMA, FHI 360, ID4Africa, IOM, ITU, International Union of Notaries, Mastercard, Omidyar Network, Open Identity Exchange UK/Europe, Organization of American States, OSCE Office for Democratic Institutions and Human Rights, Plan International, Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK, Secure Identity Alliance, WFP, UNHCR, UNICEF, UNDP, UNECA and the World Bank Group.

Understanding end user perspectives on digital identity

To ensure that future digital identity solutions or services are inclusive, effective and relevant, a bottom-up approach to design and implementation is vital. This approach ensures that the requirements, needs and desires of consumers — or end users — are understood and met. Over the last three years, the GSMA Digital Identity programme's in-country research has helped address this critical knowledge gap by collecting a broad range of insights from end users, such as how they navigate day-to-day pain points related to identity; the short-term and long-term incentives that influence their decision to access and use identity credentials; and their preferences when using identity-linked services. We have also engaged with a wide range of stakeholders in the identity ecosystem (government representatives, identity experts, MNOs, international development practitioners and local service providers) to document their perspectives on the role mobile technology could play in closing the identity gap.

In 2017, we completed our first qualitative research project and published our findings in Driving Adoption of Digital Identity for Sustainable Development: An End-User Perspective Report. Our research in Tanzania, Côte d'Ivoire and Pakistan used a multi-methods approach to capture a range of perspectives on mobile and identity, and explore local identity "ecosystems" through a variety of lenses. The end users participating in our research were all in lower socio-economic groups, but represented a mix of ages, genders, locations (urban and rural), life stages, education and literacy levels. Although each country had its own unique context and challenges, a number of important cross-cutting themes emerged that we believe could shape digital identity opportunities in these and other emerging markets. The report also identified a range of considerations for MNOs at every stage of the design and implementation process to ensure that digital identity solutions have a social impact and include low-income consumers.

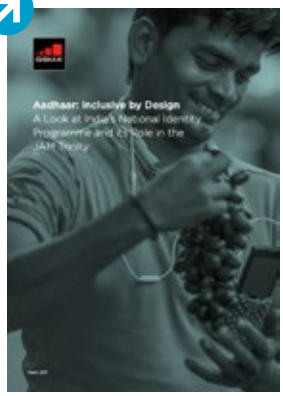
The team has conducted qualitative research on digital identity with stakeholders and end users in a total of eight countries: Tanzania, Rwanda, Nigeria, Ghana, Côte d'Ivoire, Pakistan, Bangladesh and Sri Lanka. A summary of key insights from this work can be found in our 2019 briefing paper, GSMA End-User Research: Our Top 5 Lessons. In short, these lessons were:

- **Identity documents have practical, aspirational and emotional value.** Above all, identity documents — especially official, government-recognised forms of identity — are appreciated by end users because of their practical value in everyday life. IDs open access to essential services, allow greater freedom of movement, provide a vital safeguard against various forms of exploitation and contribute to higher levels of social, economic and civic participation. However, IDs are also appreciated for their symbolic, emotional and aspirational value. Possessing an official document with a photo and signature that anchors you to your national identity can be valuable and exciting and, in some cases, can even confer status.
- **Many end users feel they can cope without an ID, but workarounds can be costly.** End users without IDs are adept at "working around" identity requirements to get the services they need, ultimately perceiving these processes as flexible and negotiable. This often includes borrowing a friend's or family member's ID, asking a trusted contact to provide a reference, using an expired or less official form of ID (such as a student card) or simply making excuses for not having the right documentation. However, this "flexibility" often weakens the perceived need for a national ID (NID) and, in cases where workarounds are not as effective, not having an ID has direct and negative costs.
- **There is a complex gender narrative associated with identity.** Nearly all research participants have asserted that women and men have an equal right to an NID. However, prevailing gender inequalities and social norms can reinforce a widely held assumption that women have less practical need for an ID than men. A lack of urgency to register can be further complicated by the fact that many women are unable to leave their home to travel to enrolment centres, or are less willing to navigate lengthy, complex and often arduous enrolment processes.
- **Relationships and trust are vital.** The relationships end users have with their government, local service providers and community members strongly influence their behaviour and attitudes about identity, as well as their willingness to share information about themselves. Where community relations are strong and trust among citizens is high, we have found that people tend to be happy to share personal information with service providers, and highly value less formal proof of identity that leverages personal relationships, for example, having a community leader vouch for you. Conversely, in instances where national security was a concern and trust among citizens was low, data privacy and access to government-issued proof of identity was a high priority.
- **Mobile is already being used in "identity journeys", but could be used even more effectively.** Mobile technology plays a significant role in many day-to-day identity journeys. For example, end users can call friends or family members to vouch for them; some services, such as e-government services in Rwanda, use two-factor authentication by linking national IDs to mobile numbers; and some end users rely on their mobile handsets and SIM cards to store important identity information or photographs of ID cards. Most end users could see clear benefits to using their phones in new ways to validate their identity when travelling or accessing identity-linked services, and welcomed digital identity solutions that were more accessible, easy to use and/or enabled them to better meet their daily needs.

Documenting innovation and best practices

Occasionally, the Digital Identity team publishes case studies that highlight innovative companies or technologies that are, or could be, leveraging mobile to provide underserved populations with better access to identity-related services. Our 2018 case study, Innovative Mobile Digital Identity Solutions, explores two emerging solutions that are using mobile technology to establish functional and foundational identities. The first case study features Juvo's Flow Lend solution, which is providing mobile phone customers in the Caribbean with a functional financial identity by analysing their mobile phone usage and top-up activity. This has provided predominantly pre-paid customers with a recognised credit score and access to mobile financial services for the first time, while also enabling a local MNO to understand the needs of these customers and significantly reduce churn rates (the numbers of customers switching between mobile providers). The second case study explores iCivil's partnership with the Government of Burkina Faso to use mobile technology to facilitate birth registration, particularly in rural areas where birth registration rates remain low.

Of all the emerging technologies likely to shape the future of international development, perhaps none is getting more attention than blockchain. However, for many MNOs and their partners in the development sector, it has been difficult to judge whether the significant hype around this technology is justified. In our most-downloaded report to date, Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid, we provide short case studies that showcase how four blockchain platforms are being used to improve people's access to self-sovereign identities, bring new levels of transparency to the distribution of international aid and improve the efficiency of humanitarian cash transfers. Although the platforms featured in the report are still in early stages of development, we were encouraged to see that they may soon provide opportunities for MNOs to support development partners in new ways, create new revenue streams, reduce KYC compliance costs and related barriers, and contribute to the SDGs.



Other stand-alone case studies published by the Digital Identity team include:

- Aadhaar: Inclusive by Design – A Look at India's National Identity Programme and its Role in the JAM Trinity. This report provides some context for the evolution and design of Aadhaar by exploring the identity landscape in India pre-2009, and examining two other Indian identity programmes that provided important lessons for the Unique Identification Authority of India (UIDAI), despite not reaching scale. The report then looks at Aadhaar through the lens of the Principles on Identification, highlighting how particular elements of Aadhaar have been designed and implemented to ensure it is inclusive, secure and trustworthy.

- Identity and the Urban Poor. In this case study, we consolidate a range of insights on the unique identity challenges faced by three types of urban dwellers: children born in urban areas, rural-urban migrants and those who have been forcibly displaced to cities (including internally displaced people and refugees). This high-level case study was developed through a review of external literature and by looking back at findings from our own end user research. While there is no single archetype for the urban poor, we suggest that those living in urban poverty share a handful of commonalities that shape the opportunity for mobile-enabled digital identity solutions. These include lower access to, and use of, official identity; lives marked by instability; high access to mobile; higher reliance on social connections; and less trust in government and government services.

- Understanding Capture and Validate KYC Processes. We conducted desk-based research and stakeholder interviews in nine countries implementing a Capture and Validate (C&V) Mobile SIM registration and KYC processes. We then visited five of these countries — Pakistan, Bangladesh, Peru, Uganda and Senegal — in person to conduct structured interviews with individuals particularly knowledgeable about, and experienced with, the local C&V system. Where possible, this included telecom regulators, national identity authorities and MNO representatives from numerous business functions. We found that where C&V systems are inclusive and easily accessible, they can offer clear benefits to MNOs. For example, where MNOs can validate a digital ID credential against a government database or token (such as a smartcard-based ID) they can streamline their SIM registration processes, offer a better onboarding experience for customers and reduce administrative, transactional and compliance costs. They could also leverage digital ID validation processes to provide access to new identity-linked services to vulnerable segments of the population, such as social cash disbursements delivered via mobile money, or targeted health services.

Supporting enabling policy and regulatory environments

The Digital Identity programme's policy and advocacy work has helped to promote enabling policy and regulatory environments that are focused on three key objectives:

1. Accelerating the enrolment of underserved groups on new foundational digital ID platforms (e.g. national IDs or birth certificates).

2. Facilitating the development of mobile-enabled digital identity services that drive demand and uptake of digital ID by individuals who were previously unable to access life-enhancing (digital) services.

3. Advocating for conducive policies and regulations that promote digital and financial inclusion via mobile, as well as trust in digital ecosystems. For example:
   - Where proof of identity is mandatory for registering a SIM card, policies must be proportionate to the market context, taking into account identity penetration, cost and ease of access, gender disparities and other considerations.
   - The harmonisation of proof of identity requirements imposed by different regulators, for example, KYC regulations imposed by central banks and SIM registration rules imposed by telecom regulatory authorities.
   - The development of strong legal frameworks for privacy and data protection relevant to a digital economy.

At the global level, the Digital Identity programme works with partners to advance a shared view of the key principles underpinning a digital identity ecosystem, and to educate policymakers and other stakeholders on the conditions that will enable it to develop. The programme also works at local and regional levels with MNO members to support in-country policy interventions. This involves exploring and sharing policy considerations with governments interested in updating their identity ecosystems.

The programme also offers a free capacity building course[5] for policymakers involved in a country's ID ecosystem. The course highlights the role of mobile in digital ID systems and how a digital identity can empower people to become "digital citizens" and fully participate in today's digital economies. It also highlights the impact government policies can have on the ability of marginalised groups to access official proof of identity and identity-linked services, and offers recommendations on how to remove barriers that lead to the digital or financial exclusion of marginalised groups.

In 2016, the Digital Identity team published a report, Regulatory and Policy Trends Impacting Digital Identity and the Role of Mobile. This report examines the momentum that digital identity programmes are gathering and the role of MNOs in enabling identity solutions. It shows there is considerable diversity in approaches to digital identity, making harmonisation, standardisation, federated approaches and interoperability particularly important. The report suggests that taking an integrated policy approach to these requirements would boost momentum for mobile-based digital identity and existing MNO activities, as well as develop models for MNO engagement, such as public-private partnerships.

The report also touches on the need for policymakers and MNOs to promote transparency and proper, lawful management of government access requests for mobile subscribers' communications data through digital platforms. Transparent, proportional and well-implemented legal frameworks are considered essential for building consumer trust in digital identity ecosystems, as is government leadership in developing these frameworks and convening key stakeholders for consultation. The report also highlights the need for MNOs to engage with governments, regulators, standard-setting bodies and others to demonstrate the opportunity of mobile-based digital identity services in support of the SDGs.

As of December 2019, an estimated 155 governments have imposed proof of identity requirements to use mobile services — a policy that requires MNOs to check and record their customers' identity documents before selling/activating their prepaid SIM cards. The Digital Identity programme has published a series of studies exploring the strong direct link between access to official identification and access to mobile, particularly in locations where prepaid SIM registration is mandated. These reports have been cited hundreds of times by news reports and publications, and the four report series (2016–2020) is considered the best source of information on this topic. The reports showcase insights and best practices from various countries that have introduced mandatory SIM registration policies, and provide recommendations for policymakers considering mandating or updating SIM registration policies.

5. GSMA capacity building course: Digital identity for the underserved and the role of mobile.

Our 2016 report, Mandatory Registration of Prepaid SIM Cards, reviews recent requirements for mandatory SIM registration in various markets, reflects on best practices, highlights potential issues and suggests recommendations for policymakers introducing or revising a mandatory SIM registration policy. The report concludes that any decision to implement or change a SIM registration policy should only be taken after consultation with all stakeholders and the completion of a comprehensive impact assessment that reviews all possible options to address specific concerns in the market, including consumers' privacy concerns and expectations. These decisions should consider the costs and benefits of mandating (as opposed to encouraging voluntary) registration; ensure the proposed registration solutions take a long-term view and consider local market conditions; and ensure the proposed solution maximises value for society.

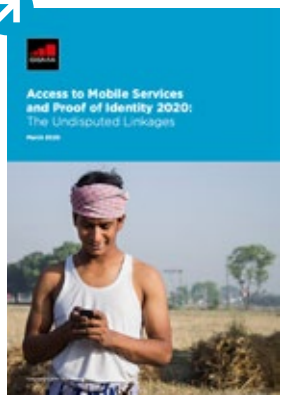
Our programme's expertise in SIM registration enabled us to actively engage in several countries, particularly in Africa, where the SIM registration policy environment has been challenging and either deactivated or threatened to deactivate the SIMs of millions of mobile users who could not meet proof of identity requirements.

Condusive regulatory policies in Uganda to enable access to mobile services by refugee populations

In early 2017, Uganda's telecom regulator, the UCC, issued a decree following pressure from the government, requiring all MNOs to deactivate all "unidentified" (unregistered) mobile SIM cards overnight. The UCC was able to reach an agreement to extend the deadline to one week, but would then have to proceed with disconnections.

Colleagues from the GSMA held a series of meetings with the industry and convened MNOs to draft a letter to the Government of Uganda asking for the deadline to be extended further. These engagements, as well as subsequent communications between the GSMA and the UCC, heavily referenced best practices and global insights from the Digital Identity team's reports, which strengthened arguments for granting the extension and minimising the risk of leaving people without access to mobile communications. A longer deadline extension was granted after these engagements, but the issue was escalated to the High Court when consumer groups sought an injunction against the UCC-ordered SIM card deactivation, which was later dismissed.

While MNOs ramped up efforts to raise consumer awareness of how to comply with SIM registration processes to avoid deactivation, the GSMA Digital Identity team continued to engage with the government, strongly advocating for the expansion of a national ID before enforcing strict SIM deactivations. This would ensure that a larger proportion of the population would have access to a national ID, be able to register their SIM cards in their own names and avoid being cut off from mobile communications.



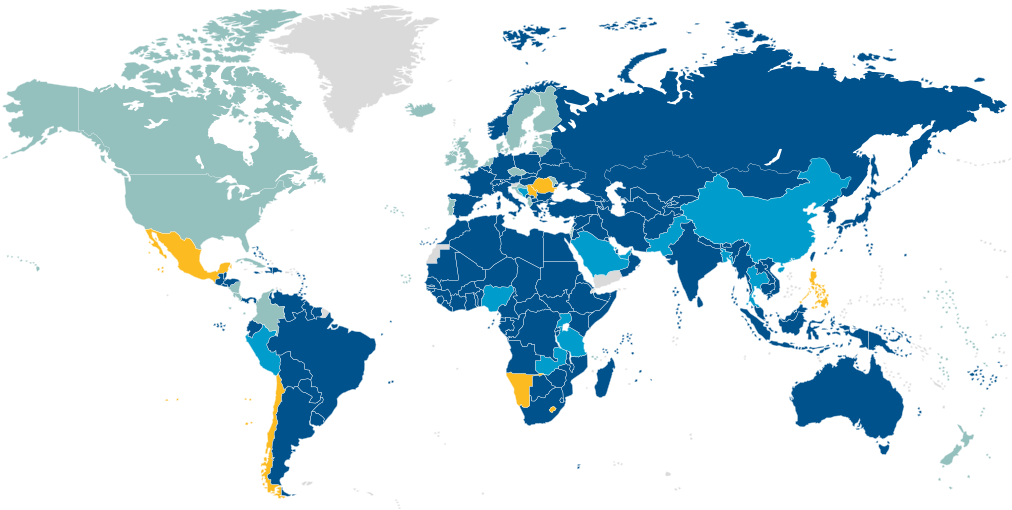
Our programme demonstrated a direct relationship between access to official ID and access to mobile

In Access to Mobile Services and Proof of Identity, first published in 2018 and updated in 2019 and 2020, we examined SIM registration policies globally and found, among other things, that the majority of markets with low mobile penetration also have low levels of registered populations. This suggests a direct relationship between people's ability to access government-recognised proof of identity and the level of mobile penetration in that market. The reports also highlight that robust identity verification is still nascent in the context of mobile SIM registration: just 12 per cent of countries mandating SIM registration enable MNOs to verify the accuracy of customers' identification credentials against an approved government database.

These reports also found that a significant number of countries lack a comprehensive privacy framework, which in turn affects trust in the digital ID ecosystem. The GSMA discovered that only 59 per cent of countries mandating SIM registration have a privacy and/or data protection framework in place, and the same applies to 41 per cent of all African countries. While these legal frameworks seek to meet the privacy needs and expectations of mobile users, the scope varies from country to country (Figure 3).

Figure 3

Proof of identity requirements to access mobile, by country (SIM registration)



SIM registration status

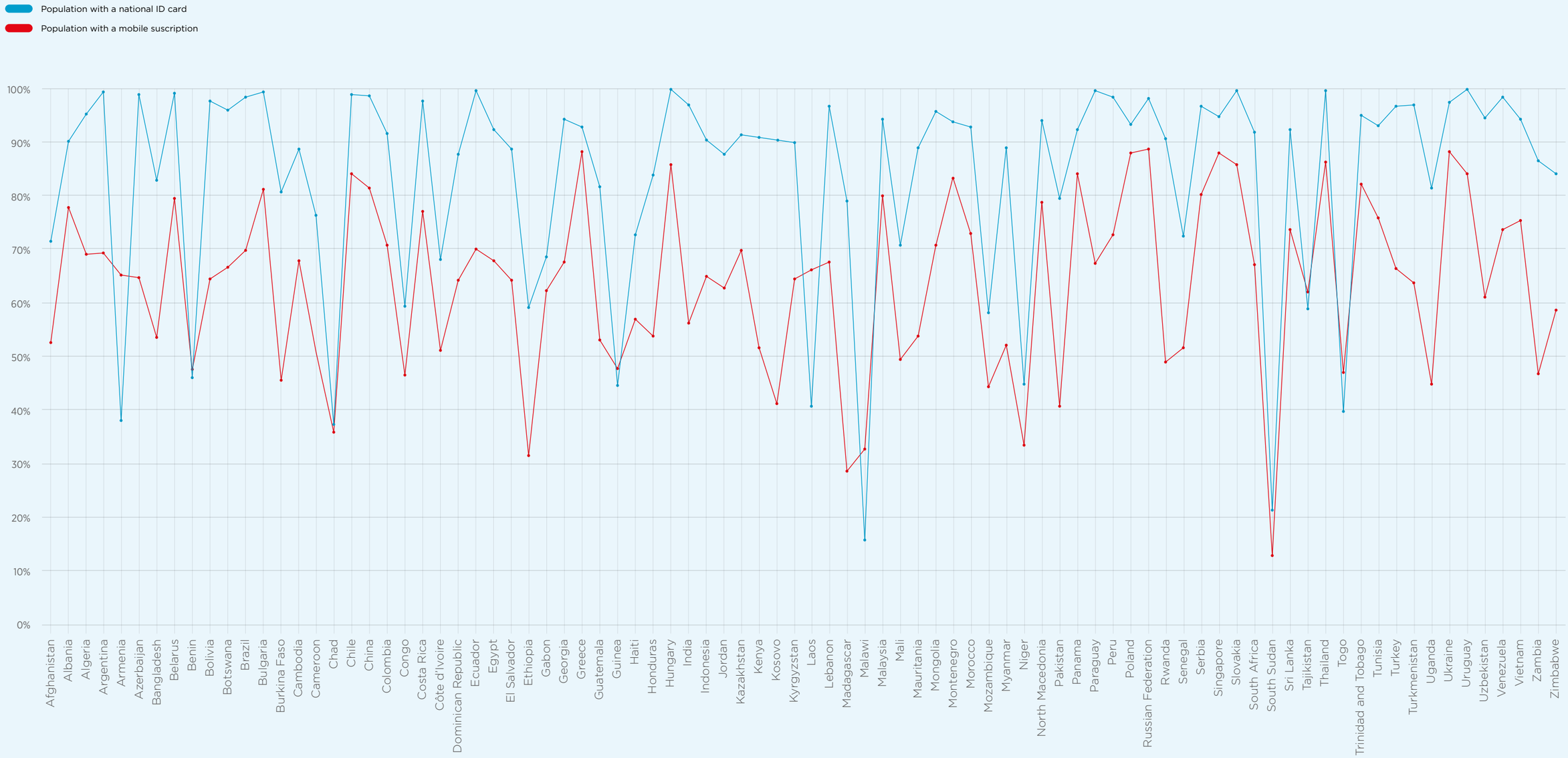
Registration not mandatory | Registration mandatory | Registration mandatory with biometrics | Being considered | Inconclusive data or no data available

GSMA Digital Identity Programme:
Insights and Achievements (2016–2020)

Figure 8

The link between access to ID and access to a unique mobile subscription

Source: GSMA Intelligence, Market Penetration - Unique Mobile Subscribers Q3 2019 and The World Bank, 2017 FINDEX dataset



Selection of countries where SIM registration is mandatory from World Bank Findex dataset 2017

In addition to being able to prove one's identity digitally, successful digital economies must also have a high level of consumer trust in the digital ecosystem. However, many countries around the world do not have comprehensive legal privacy and data frameworks. With this in mind, the GSMA recently conducted end user research in Sub-Saharan Africa to explore attitudes about privacy and trust, both in the presence and absence of comprehensive data protection frameworks, as well as consumers' willingness to access digital services that are linked to their identity details.

Interestingly, the research showed that many consumers could not correctly identify whether their country had data protection and privacy laws in place. The research also showed that vulnerable consumers, particularly those in rural environments with lower levels of education and more basic handsets, tended to be less aware of the risks associated with sharing data. In fact, 94 per cent of those surveyed in Mozambique and Rwanda (countries without comprehensive privacy frameworks) were willing to share personal identifiable information, such as their address, compared to 78 per cent in Ghana and Zambia (where privacy frameworks are more comprehensive).

Women in particular expressed concerns about safety and potential harassment, lack of digital literacy and were less convinced that redress for data breaches would be successful. However, previous GSMA research has shown that MNOs are already addressing some of these issues with women-focused initiatives, such as female-friendly distribution models, anonymous top-ups and educational initiatives.

Overall, the research showed that in markets with legal frameworks for privacy and data protection, people felt more informed, supported or confident in managing their privacy. It also showed a universally high appetite for accessing identity-linked services, regardless of the presence of legal frameworks, particularly if consumers perceive a clear benefit and the service is provided by a sufficiently trusted entity. Further research in additional countries is needed to substantiate these initial findings, but this research has highlighted the need for MNOs to be transparent about how consumers' data is used, to clearly articulate how identity-linked services can provide tangible benefits for consumers and to consider ways to build and retain consumer trust.

Overall, our research related to policy and regulation has helped provide more evidence and recommendations on how governments could create effective digital identity ecosystems, and leverage the power of mobile to increase digital, social and financial inclusion, drive economic growth and prevent fraud.

Our main recommendations to policymakers include:

1. **Partner with the private sector, MNOs in particular, to implement national (digital) identity enrolment.** The mobile platform, with its reach and operator assets, can help governments leapfrog traditional paper-based ID systems and facilitate the roll-out of digital national IDs. Such public-private partnerships could help achieve SDG 16.9: "By 2030, provide legal identity for all, including birth registration".

2. **Promote e-government and other identity-linked services to drive demand for identification.** These services provide incentives for adoption and support the growth of a robust digital identity ecosystem. For example, tax declaration, voting, health systems and educational registration. These can help make governments much more financially and politically efficient while also having a positive socio-economic impact on citizens.

3. **Harmonise regulations that impose identity requirements on industry.** In some countries, MNOs are already subject to identity-related requirements, such as mandatory SIM registration and KYC requirements for mobile financial services. These obligations are often imposed by at least two different regulatory authorities, typically telecom regulators and central banks. Taking an integrated policy approach to proof of identity requirements would facilitate a seamless customer experience, from registering a SIM card to accessing other identity-linked services like mobile money, credit, healthcare and education. It is also important to consider the timing of regulation enforcement to ensure that a critical mass of citizens have the opportunity to obtain an acceptable form of ID to access these services, and to minimise exclusion.

4. **Encourage best practices in privacy and consumer protection.** Data protection and privacy laws, as well as industry best practices on handling personal data, must be aligned with consumer expectations. Having this "trust framework" in place would not only encourage adoption of mobile-based identity services, but also support operational effectiveness and provide clarity on each party's responsibilities for data collection and use. Growing reports of government requests to access communications threaten consumer trust and perceptions of digital identity solutions. Regulators and policymakers must promote transparency and proper, lawful management of government access requests.

2

Exploring digital identity use cases

To contribute to a tangible body of evidence on the role of mobile in the creation and growth of digital identity ecosystems, the Digital Identity programme has spent the last four years working with member operators and development partners to test and develop mobile-enabled digital identity platforms that bring our insights and advocacy work to life. Without a compelling business case, MNOs' appetite and prospects for scaled end user adoption and mobile-enabled digital identity platforms may be limited in reach, overly dependent on short-term donor funding (and associated challenges) and ultimately unable to have the transformational impact the Digital Identity programme believes is possible.

Given that digital identity is still a fairly fragmented concept, we aim to find solutions that could demonstrate a viable business case and provide early insights into the operational, technical and commercial considerations in the development and design of scalable and sustainable mobile-enabled digital identity services. It is important to note that the use cases we explored fall along a spectrum of business cases and partnership models. Some use cases we tested were a reflection of where the sector was at the time or where we saw it going in the near future. Others, such as those involving the creation of economic identities by analysing mobile data assets, explored an area where we saw opportunities for MNOs to have a unique impact. Furthermore, some business cases addressed challenges that were a priority in the digital identity ecosystem and we wanted to test what the role of an MNO would be. Finally, use cases such as digital birth registration are key to achieving development goals, but may not have an obvious commercially viable model, and we saw these cases as opportunities to explore new models for shared-value partnerships and collaboration.

Digital birth registration

As an official and permanent record of a child's identity, birth registration can bestow access to a number of vital services, including healthcare and immunisations, education and social protections. As a child grows, birth certificates — as official proof of age — can act as a vital safeguard against child labour, early marriage or recruitment into the military. Later in life, it can enable young adults to acquire national identity documents, vote in elections, gain formal employment, own property or access formal financial services. For national governments, birth registration is an essential tool for planning and monitoring the delivery of public services, development policies and infrastructure programmes. For these reasons, the United Nations Convention on the Rights of the Child, as well as a number of international treaties, guarantees every child the right to be registered at birth, and the right to a name and nationality.

It is increasingly evident that in the world's hardest to reach areas, mobile technology is well-placed to provide national governments and other ecosystem players the opportunity to leapfrog outdated, paper-based birth registration systems and offer more children a foundation for full participation in society. In 2016, the GSMA began tracking and reporting on a number of innovative digital birth registration (DBR) initiatives supported by MNOs in Pakistan, Tanzania, Ghana, Belize, Senegal and Uganda, to learn how these projects successfully delivered measurable and significant improvements in local birth registration rates.

These lessons were captured in two reports: Birth Registration in Tanzania: Tigo's Support of the New Mobile Birth Registration System and Innovations in Mobile Birth Registration: Insights from Tigo Tanzania and Telenor Pakistan. Insights from these early reports were shared at multi-stakeholder workshops at GSMA's Mobile World Congress (2017 and 2018) and the Mobile 360 Africa Conference (2016 and 2018). The Tigo-supported DBR programme in Ghana was showcased by the Digital Identity team to then-President Dramani Mahama of Ghana at the UN General Assembly's "Every Women, Every Child" lunch in 2016. They were also shared at the Fifth Conference of African Ministers Responsible for Civil Registration and Vital Statistics, held in Lusaka in October 2019, and with civil registration officials in Zambia, who are beginning the journey of digitising and reforming their civil registration and vital statistics (CRVS) systems.

GSMA's Director General, Mats Granryd, visited a hospital outside Dar es Salaam to see and help raise awareness of the digital birth registration (DBR) service supported by Tigo Tanzania.

In 2017, the GSMA's Director General, Mats Granryd, visited a hospital outside Dar es Salaam to see and help raise awareness of the digital birth registration (DBR) service supported by Tigo Tanzania. The initiative is implemented by Registration Insolvency and Trusteeship Agency (RITA) and UNICEF, with funding from the Government of Canada and in partnership with Tigo. As of mid-2019, over 3.6 million children under five had been registered and issued a birth certificate under this initiative. Across the 13 regions where the project is delivered, registration and certification levels have increased from less than 10 per cent in 2012 (according to a nationwide census) to over 80 per cent by 2019. Over a million more children are expected to register using the digital birth registration service by mid-2020, which is planned to be rolled out in every region of mainland Tanzania by 2022.

In 2016, UNICEF, Telenor Pakistan and the provincial governments of Sindh and Punjab, renewed and expanded their commitment to testing how mobile technology could augment Pakistan's traditional paper-based birth registration process. This followed a successful four-month pilot that saw registration rates in targeted districts increase by an average of 200 per cent over the previous year. Since the new phase of this project began, over 770,000 new births have been registered through the new DBR system and, impressively, an estimated 40 per cent of children registered are girls. In some of the project locations, Telenor's mobile agents were introduced as official DBR registrars. The project has proven that these agents are extremely effective at facilitating birth registration due to their proficiency with relevant administrative procedures, such as issuing mobile phone SIM cards, collecting customer data and verifying NADRA's National Identity Card information. Telenor agents also tend to be more familiar and comfortable with using mobile technology to register customer details.

While this project was being implemented, the Digital Identity programme worked with Telenor Group and Telenor Pakistan to investigate how MNOs could support future DBR projects in a commercialy sustainable way. For instance, by developing additional revenue streams through data, disbursements and links with other value-added services, such as maternal and child health advisory services. In 2018, we produced the Roadmap for Digital Birth Registration as a guide for MNOs and their partners to have a greater impact and improve the efficiency and efficacy of digital birth registration. The Roadmap draws on lessons from, and our recommendations for, the Telenor-supported DBR project in Pakistan. It provides a number of insights, examples of best practice and recommendations for MNOs and their partners at all stages of a DBR project. While many of the insights and recommendations are specific to Pakistan, they should also be very relevant and applicable to birth registration stakeholders in other developing markets.

In particular, the report provides recommendations on designing a below-the-line (BTL) communications strategy for the DBR initiative in Pakistan, and proposes a cost-effective communications plan. The strategy focuses on creating communications messaging and materials that encourage behavioural change by helping new parents understand why birth registration is important, the benefits of using the new digital service and the practicalities of registering through local registrars (or "gatekeepers"). The Roadmap also reinforces Telenor's assertion that there was a need for a more sustainable gatekeeper incentive model, based on rewarding DBR registrars for every successful registration rather than a flat monthly rate. Through interviews with DBR gatekeepers, the GSMA confirmed that monthly disbursements based on actual registrations would be more motivating, and would also allow gatekeepers to better manage associated travel and administrative costs.

The Digital Identity team has also worked with Plan International, Smart Zambia and Zambian MNOs to explore how mobile can support the digitisation of Zambia's CRVS system. Platforms such as OpenCRVS offer a standardised, but adaptable and modular, alternative to the current partially decentralised analogue system. This is a different approach to digital CRVS than has been taken in countries like Pakistan, Ghana and Tanzania, where MNOs worked in partnership with UNICEF to develop bespoke, country-specific platforms. Feedback from many development stakeholders indicated that a more standardised but modular approach may be worth considering from a sustainability and scalability perspective. In July 2019, our programme joined Plan International on a proof of concept visit to Zambia, which aimed to examine the country's current manual and paper-based CRVS system and map out a path to a more effective digitised system.

After meeting with registration officials (including healthcare workers, district registrars and officials from Zambia's Department of National Registration, Passport and Citizenship – DNRPC) to conduct primary research on the existing birth and death registration process, our programme hosted a workshop with a range of CRVS stakeholders to identify pain points and bottlenecks in the birth registration process. This consultative approach was helpful in understanding the immediate opportunities to improve the system. The workshop concluded by working with stakeholders to understand what an ideal CRVS ecosystem would look like and integrating this feedback in Zambia's CRVS digitisation process.

The OpenCRVS platform, adapted to Zambia's CRVS requirements, was demonstrated at the Fifth Conference of African Ministers Responsible for Civil Registration in October 2019 in Lusaka. As the Zambian Government considers its options for platform architecture and vendor selection, the Digital Identity programme has brought together MNOs and CRVS officials in Zambia to understand the added value mobile could bring to the digitisation of the national registration system. In October 2019, Zamtel publicly committed to supporting the DNRPC in its efforts to digitise the country's births, deaths, marriage and divorce registration processes, regardless of the digital platform the government selected. Zamtel is exploring how connectivity and bulk notification services could be provided on a commercial basis to support the deployment of such a solution in the last mile.

July 2019 workshop in Lusaka with Plan, DNRPC, National Registration Office, Department of Health, Dept of Home Affairs, Department of Education, National Police, Central Statistics Office, Smart Zambia and UNICEF in attendance. GSMA represented MNOs and fed back – Zamtel committed to supporting the government in its reform and digitisation efforts after this workshop.

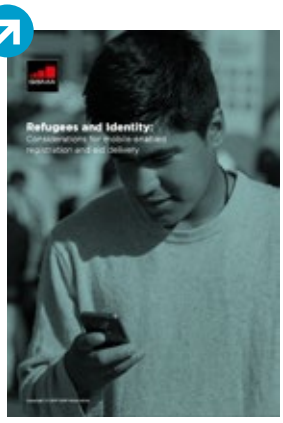
Zamtel mobile agents have also participated in field testing of the OpenCRVS platform, generating many valuable insights that were presented to the Zambian Government. As we saw in the Pakistan DBR model, agents demonstrated high levels of technical literacy, strong relationships with local communities, and knowledge and experience working with end user data through their existing KYC activities. The Zambian Government could effectively leverage Zamtel's network as an additional registration channel to achieve universal birth registration, as existing channels have thus far struggled to raise the national birth registration rate above 14 per cent. In December 2019, the DNRPC confirmed their intention to work with Zamtel to accelerate the digitisation of Zambia's civil registration system.

These first two photos show the manual birth and death registration process at Chongwe District Registry office.

Photos from the OpenCRVS field testing where Zamtel agents were involved in digitally registering births.

Identity for the forcibly displaced

Due to the extreme circumstances under which they are forced to flee their homes, forcibly displaced persons (FDPs) often relocate within their own country or across international borders without any form of legal identification. Identity documents can be forgotten, lost, destroyed or stolen during their journey, and those who are fleeing persecution based on some aspect of their identity (e.g. nationality, religion, ethnic group or political affiliation) might find it safer to travel without documentation. In many cases, FDPs from poor, vulnerable or disconnected segments of society have never owned identity documents. Meanwhile, the top 10 refugee-hosting countries (in terms of volume) all have mandatory SIM registration policies that require customers to present a valid form of ID before a SIM can be activated or a mobile money account can be opened. Many FDPs are unable, at least in the short term, to meet these requirements, and therefore risk being excluded from basic mobile connectivity, mobile internet and a variety of mobile financial services.



An area of increasing focus, therefore, is the opportunity for mobile and digital technology to play a role in establishing unique digital identities for FDPs, particularly refugees. In our 2017 report, Refugees and Identity: Considerations for Mobile-Enabled Registration and Aid Delivery, we shone a light on the fact that displaced populations may, especially when they are first displaced, lack the identity documents required to meet MNOs' KYC criteria. This means that in markets where humanitarian-issued IDs are not accepted for KYC purposes, and asylum seekers and refugees face challenges or delays obtaining a government-issued ID, opportunities for MNOs to offer both basic and value-added mobile services can be restricted. Our report is one of the first to explore the issue of mobile KYC in refugee areas in detail, showcasing how contrasting regulatory environments in Kenya and Iraq have shaped the types of mobile financial services provided by MNOs and humanitarian organisations.

One of the most significant barriers to the digital and financial inclusion of FDPs, as identified by all our humanitarian partners, is a lack of official identification documents and consequent inability to access SIM cards and mobile money wallets in their own name. In 2017, we published Enabling Access to Mobile Services for the Forcibly Displaced, a policy note that brought even more focus to the identity-related barriers preventing FDPs, including refugees, from accessing mobile connectivity and mobile financial services. This report, which was the subject of a consultation and peer review by several humanitarian and UN organisations our programme convened in New York City, offered seven key policy considerations for host country governments and regulators to address these barriers. The report noted that the responsibility for issuing identification credentials to FDPs usually rests with different entities depending on one's forced displacement status (i.e. whether one is an asylum seeker, refugee, stateless person, internally displaced person, etc.). Finally, the note outlined several benefits — for host countries, local communities and the humanitarian aid sector — of making identity-linked mobile services, including mobile money accounts, readily accessible to FDPs.

In 2017, we also embarked on a successful collaboration with UNHCR – the UN Refugee Agency, to elevate policy considerations at global forums between 2017 and 2020, such as the World Economic Forum in Davos, the ITU, the Global Refugee Forum and the GSMA's Mobile World Congress. The GSMA also collaborated with UNHCR on an in-depth research study of 20 countries to understand the legal barriers refugees face when attempting to access mobile connectivity and mobile financial services. The study, Displaced and Disconnected, provided a basis for the Digital Identity programme's joint advocacy engagements in selected host countries.

Our growing expertise in the area of refugees and identity provided an opportunity to lead an in-country workshop in Amman, Jordan in February 2018. The objectives of the workshop were to facilitate better coordination among MNOs and humanitarian organisations, to learn from each other and brainstorm ways in which mobile could help reduce some of the identity-related barriers refugees were facing in Jordan and Lebanon. Organisations participating in the workshop included Zain, UNHCR Jordan, MercyCorp Jordan, UNRWA, MicroFund for Women, Norwegian Refugee Council, World Food Programme, World Economic Forum and Souktel. There was consensus that better coordination was needed in the humanitarian community on approaches to data sharing, data protection and privacy standards, and would be critical to the implementation and adoption of digital identity. Participants also identified the need for clearly articulated requirements, from both humanitarian organisations and MNO partners, for designing and implementing robust digital identity solutions, including clarity on roles and commercially sustainable business models.

Following this workshop, the GSMA agreed to conduct further research to help interested MNOs define a digital identity use case in a humanitarian context and identify technical, advocacy and partnership requirements. Many of the lessons from this research have been published in Recognising Urban Refugees in Jordan: Opportunities for Mobile-Enabled Identity Solutions. The report brings fresh focus to the complex identity-related challenges faced by urban refugees in Jordan, the tenth largest refugee-hosting nation in the world, and illustrates how MNOs and humanitarian organisations can collaborate to provide urban refugees with greater and more inclusive access to digital identity and identity-linked mobile services. The digital identity needs and opportunities revealed through this research included: enabling refugees to digitally register life events and vulnerabilities with humanitarian agencies and other service providers; providing greater access to identity-linked mobile financial services; and delivering more relevant and targeted information to refugees (including guidance on how to register for official forms of identity).

Identity solutions for women and girls

Although there is currently a deficit of gender-disaggregated data on access to identification, it is presumed that of the billion people in the world unable to prove their identity, a disproportionate number are women and girls. In many countries, women and girls remain particularly vulnerable, and socially, politically and financially excluded. Expanding access to identity will help the international community effectively address SDG 5, which aims to eliminate gender-specific challenges, such as poverty, inequality and violence against women.

Empowering a woman with official and recognised forms of identification not only strengthens her individually, it also fortifies her family and contributes to the social and economic welfare of her wider community. Surveys in Pakistan, for instance, have helped to highlight the critical role Computerised National Identity Cards (CNICs) have played in empowering women: those with CNICs felt a stronger sense of identity than ever before, were eager to vote and know their rights as citizens, were given more respect within their families and their increased self-confidence emboldened them to share their opinions on household matters. The McKinsey Global Institute has also recently estimated that if women were able to participate in the economy to the same extent as men, it would add up to USD 28 trillion to global GDP by 2025.

We began our 2017 report, Understanding the Identity Gender Gap: Insights and Opportunities for Mobile Operators to Help Close the Divide, by exploring the gender gap in birth registration, highlighting how mobile technology can be used to help parents overcome the barriers preventing them from registering the birth of their daughters. We then examined the institutional and cultural barriers that can influence whether a woman is able or incentivised to obtain national identity documents. Short case studies on India and Pakistan are included, alongside gender-specific insights from the Digital Identity team's end user research in Tanzania, Côte d'Ivoire and Pakistan. The report helped identify several barriers that must be addressed to ensure digital identification systems include and cater to the needs of women and girls. These barriers are:

- A lack of gender-disaggregated data on the identity gap and how this can help inform and measure the design and impact of digital identity solutions;
- Cultural and social factors that have an impact on the gender divide in mobile access and ownership;
- Policy and regulatory barriers that have a disproportionate impact on women's ability to either access an official identity or be digitally and financially included via mobile platforms in their own right;
- Nascent digital identity ecosystems and a lack of relevant identity-linked services that encourage women to register for digital identities; and
- Untested business models for identity-linked services aimed specifically at women.

Through the work of the Digital Identity and Connected Women teams, the GSMA has established itself as a thought leader, convener and catalysing partner, both in digital identity and the gender gap in mobile access, mobile money and mobile broadband. In 2018, we began to build on our experience across these two thematic areas by supporting the Commonwealth Digital Identity Initiative, which aims to drive progress in providing a digital identity for every girl in the Commonwealth by 2030.

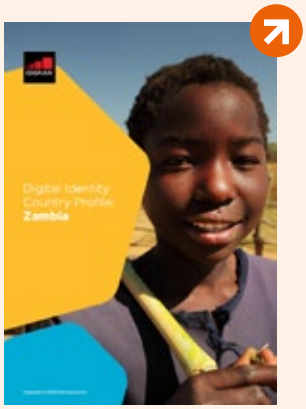
Spotlight On The Commonwealth Digital Identity Initiative

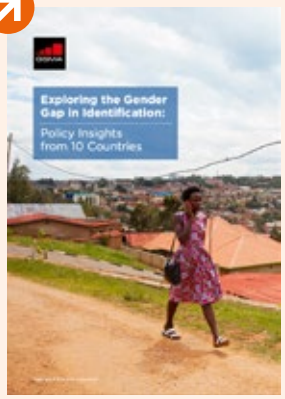
The Commonwealth Digital Identity Initiative (CDII) is supported by the UK's Department for International Development (DFID) and the Australian Department of Foreign Affairs and Trade (DFAT), in partnership with the GSMA's Digital Identity programme, the World Bank ID4D programme and Caribou Digital. The two-year programme is nestled between the 2018 Commonwealth Heads of Government Meeting (CHOGM) in London, where the programme was announced, and CHOGM 2020 in Kigali, Rwanda, where the programme will report on its achievements and outcomes, and recommend where the Commonwealth can continue to take a leading role in developing digital identity programmes.

In June 2018, we developed our (unpublished) Commonwealth Identity Database, which collated data on key metrics related to national identity coverage, mobile phone access and use, and other relevant social and gender development indicators. The database allowed the Digital Identity team and our CDII partners to make more informed and objective decisions about which Commonwealth countries should be prioritised for future research projects, technical support or in-country demonstration projects. Using data from the World Bank's ID4D database and the 2017 Global Findex Surveys, we developed key communications messages for the CDII, including the headline statistic that 230 million women and girls in the Commonwealth lack official ID.

Since the launch of the initiative, the Digital Identity team has produced several important pieces of research that explore the barriers preventing women and girls from adopting or using digital identities. Insights from our various CDII research projects have been shared with a wide variety of stakeholders at Mobile World Congress (2019) and Mobile 360 Africa (2019), as well as an ICT Roundtable event in London and a Mastercard event in Oslo.

Recognising that mobile technology and MNOs are well positioned to tackle this issue, we explored the identity and mobile landscapes in Malawi, Sri Lanka, Uganda and Zambia — four countries at distinct stages in their journey towards full national identity coverage, and with contrasting rates of mobile ownership and use among men and women. Although each country has its own unique identity context, the research also identified a range of insights — seen across all four countries — that are important considerations in developing, implementing and embedding digital identity solutions

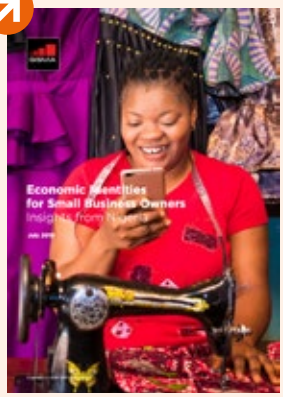




Aware that policy, regulatory and cultural factors contribute to the identity gender gap, our study, Exploring the Gender Gap in Identification: Policy Insights from 10 Countries, provides an overview of national identity ecosystems and related policies in 10 Commonwealth countries: Bangladesh, Botswana, Malawi, Nigeria, Papua New Guinea, Rwanda, Sri Lanka, Uganda, Zambia and Zimbabwe (while Zimbabwe is no longer a Commonwealth country, it is included in our report as an ex-Commonwealth country that has applied to re-join). The report identifies the unique barriers women face when accessing and using official identification, and explores government-led initiatives that are already in place or can be introduced to address these barriers. The key identity credentials explored in this study are birth certificates and national identity documents.

Insights gathered through the policy report were used to develop the GSMA's new capacity building course, "Digital Identity for the Underserved and the Role of Mobile". The course highlights the role of mobile in digital identification systems and how digital identity can empower people, especially women, to become digital citizens fully able to participate in today's digital economy. It further highlights the impact that certain government policies can have on the ability of marginalised groups to access official proof of identity and identity-linked services. The course has been designed for a broad range of policymakers and regulators, such as national identity authorities, central banks, ICT regulators, gender ministries, social affairs ministries and privacy regulators. Participants of the course are also invited to participate in a field-focus session in another country, as this further advances their knowledge and understanding of the role of mobile in digital identification systems. To date, the GSMA has delivered the course to 15 participants in Rwanda. The course was delivered to policymakers from at least seven Pacific countries at the end of 2019.

One of our most in-depth CDII studies to date, Digital Identity Opportunities for Women: Insights from Nigeria, Bangladesh and Rwanda, draws on in-country qualitative research to explore the specific incentives, challenges, preferences and benefits that women and girls encounter, compared to men, when engaging with digital identity systems or services. In addition to providing the GSMA, MNOs and the broader development sector with an extensive understanding of the identity and mobile contexts in Nigeria, Bangladesh and Rwanda, the report identifies how both men and women navigate day-to-day identity-related pain points, as well as the short-term and long-term incentives that influence their decision to access and use identification. It also provides recommendations on how mobile could be leveraged to increase adoption and use of identification and identity-linked services, especially among women and girls, as well as considerations for organisations working on, or interested in developing, digital identity solutions. The report highlights several important cross-cutting themes shaping this area, namely that identity documents are highly valued; there is a complex gender narrative associated with identity; the ability to register for mobile services in one's own name is increasingly important; mobile is already playing a significant role in many day-to-day identity journeys; and engaging with customer trust and data security is essential.



More specifically, the research highlighted that the owners of small and medium enterprises (SMEs) in Nigeria, many of whom are women, often struggle to demonstrate their personal and business credentials to their customers, suppliers and service providers. As a result, they often lack access to market information and support, pay more for financial services (such as business loans or capital), experience inequitable business relationships with suppliers and struggle to distinguish their business from less reliable or fraudulent enterprises. In March 2019, our team explored these challenges in more detail through a research project designed to improve our understanding of the identity-related needs and pain points faced by SME owners in Nigeria, and whether digital identities could improve access to new value-added mobile services. In particular, the research aimed to inform the development of a product or service that prioritises the needs and requirements of women. More details on the findings of this research can be found in our 2019 report, Economic Identities for Small Business Owners: Insights from Nigeria.

The report provides a clear roadmap for developing a minimum viable product (MVP) for an SME-focused economic identity (a concept discussed in more detail in the next section of this report). The roadmap suggests that, as a first step, the new service should test how MNOs can provide broader access to financial services through a data-sharing agreement with a local financial services provider. Following the publication of the report, the GSMA received a commitment from a Nigerian MNO to pilot this concept, and the service was launched in March 2020 with a subset of small business owners in Nigeria. The GSMA has supported this work through a series of workshops, journey mapping, human-centered product design and wireframing, and user testing ahead of a live service deployment. The following is a summary of the project.

9mobile's 9ID: an economic identity platform for small business owners in Nigeria

A GSMA partnership with 9mobile in Nigeria has led to the development and deployment of an economic identity service, 9ID. Research conducted by the GSMA indicated that MNOs are well positioned to develop an economic ID for small business owners in Nigeria. Small business owners, particularly women, struggle to demonstrate their value and build trust among customers, suppliers and service providers. As a result, they face challenges expanding their business and accessing financial services that would enable their business to grow.

An economic ID is especially important for women business owners in Nigeria as there is a misconception that women have less need for identification due to their perceived economic position. However, businesswomen must prove their credibility and value for all the same reasons as businessmen, and may have an even greater need for ID to access services from biased providers.

9ID is a small business economic ID that verifies the identity of a business and demonstrates trustworthiness to customers, suppliers and service providers. 9mobile seized this business opportunity to develop a minimum viable product, which will be piloted in March 2020. The aim of the product is to initially allow small businesses the chance to prove their value to service providers, build the trust of potential customers and, perhaps most importantly, get access to credit to grow their businesses. It is hoped that the information gathered from the pilot will enable 9mobile to offer additional business services to these customers on the 9ID platform, including insurance and even investment opportunities.

The service will be launched to a subset of existing 9mobile customers via a combination of SMS and phone calls that will encourage users to sign up to the service. Call centre staff will be trained to answer questions about the service, and a website is being developed for the product with a full FAQ section.

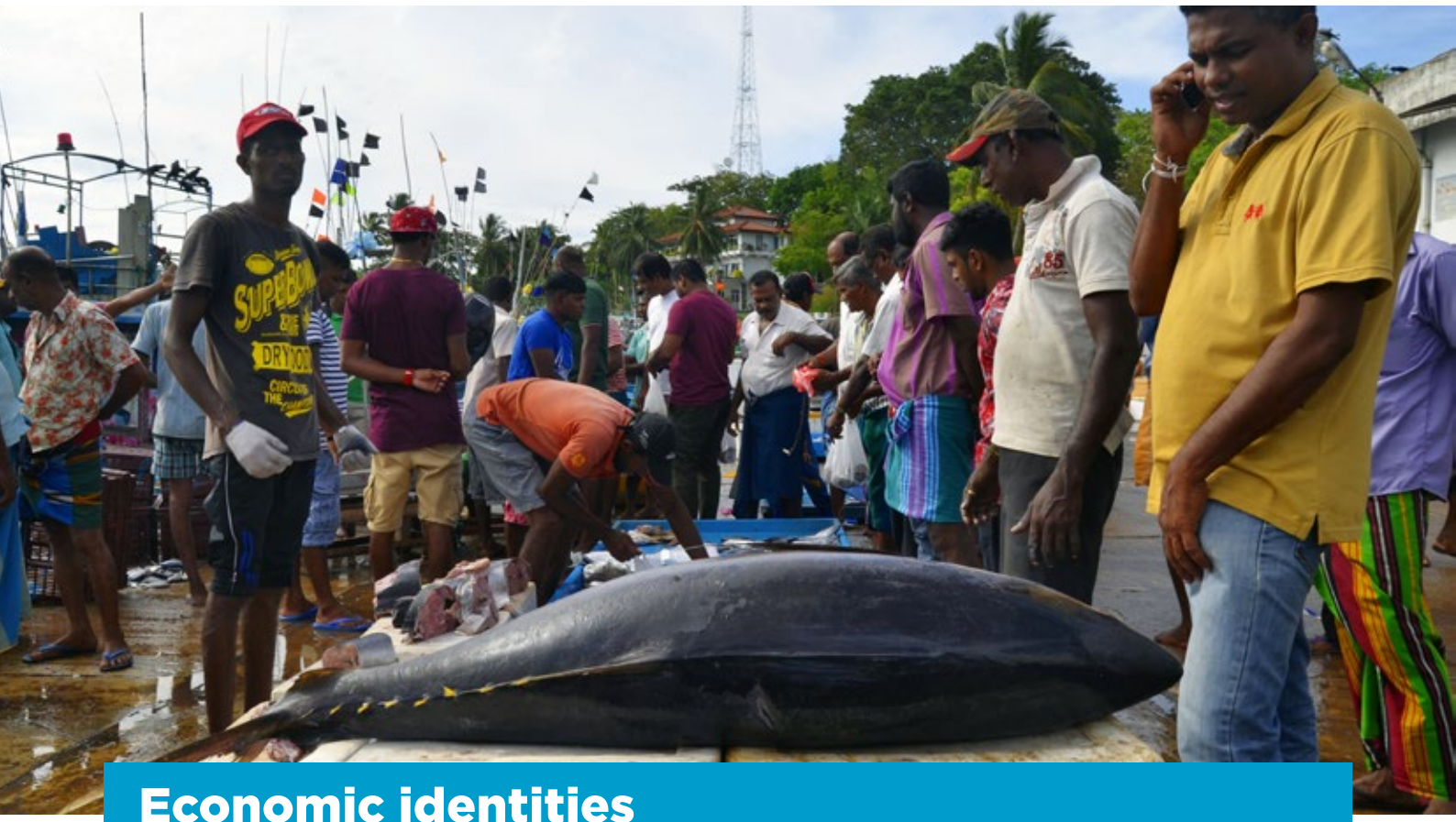
Finally, as part of the CDII, our Advocacy team developed and delivered a capacity building course for policymakers on Digital Identity for the Underserved and the Role of Mobile. As of February 2020, the one-day in-depth course had been delivered four times to about 100 policymakers (ICT regulators and ministries, national ID authorities, central banks, etc.) from over 20 countries.

The course:

Highlights the role of mobile in digital identification systems, and how digital identity can empower people to become fully participating digital citizens in today's digital economy;

Highlights the impact certain government policies can have on the ability of marginalised groups to access both official proof of identity and identity-linked services; and

Focuses on identity-related policy areas, such as government incentives for birth registration and national ID application processes, and features case studies and examples on how government policies can both support and hinder marginalised populations from accessing identity.



Economic identities

For the purposes of the Digital Identity programme, an "economic identity" is a dynamic digital profile based on an analysis of attributes gathered from an individual's mobile subscription and usage. For example, location data, call data records, airtime top-up and mobile money transaction history. One of the key objectives of a mobile-derived economic identity is to provide better access to targeted services, such as information and advice, financial services (e.g. savings, insurance or credit) or to verify eligibility for government subsidies. While our exploration of this concept began with a focus on smallholder farmers, we have also been working with MNO partners to test how it could be used to benefit specific underserved segments of the population, such as small business owners in Nigeria or fishing communities in Sri Lanka.

Economic identities for farmers

Increasing the productivity and profitability of farmers, and the agricultural industry at large, is a significant opportunity for MNOs in many developing countries. As the most ubiquitous technology in rural communities, mobile is uniquely positioned to deliver the critical services and information farmers need to make better-informed decisions, manage their day-to-day finances and improve their livelihoods. However, the rural poor are one of the least likely demographics to have access to official proof of identity. Even where identity coverage is widespread, there can be tension between a smallholder farmer's "fixed identity" (i.e. the demographic and biometric details recorded on their official identity document) and their more fluid "economic identity", which helps explain their shifting and dynamic social and economic circumstances. Farmers who are unable to prove their creditworthiness or validate other vital credentials (e.g. income and transaction histories, land ownership, crop types, geolocation or farm size) are more likely to face barriers accessing formal services or connecting to the global economy. For this reason, the GSMA's mAgri programme has identified "digital profiles" as a key bottleneck in digitising the agricultural value chain, and one of the best opportunities to demonstrate the value of the mobile platform in this effort.

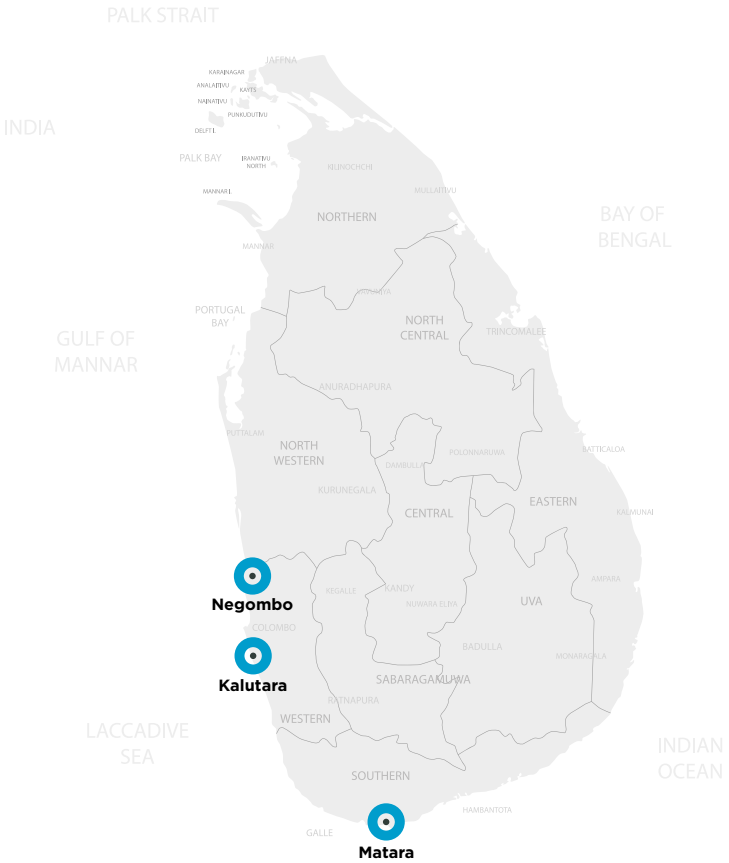
Our 2018 report, Digital Identity for Smallholder Farmers, highlights key findings from our qualitative research in Sri Lanka, which helped create a more detailed picture of the needs, opportunities and use cases for mobile-enabled digital identity solutions among smallholder farmers. The research made clear that digital economic identities have the potential to help farmers take pride in their profession, feel more informed, connect to new markets or buyers, access digital financial services and reduce their financial risks. In the long term, this will lead to better farming practices, greater digital and financial inclusion and higher productivity. For MNOs, digital identities could enable the digitisation of the agricultural value chain and extend a wide range of services to rural users and enterprise customers.

Through our research, we also learned it is vital that MNOs not treat farmers as a homogenous group. A range of factors influence an individual's identity-related needs and priorities, and MNOs and their partners should take a targeted approach to designing and marketing identity-based solutions. Farmers are also more likely to trust and act on information that comes from someone they know. For this reason, MNOs should consider creating partnerships with agribusiness as they build credibility in the agricultural sector, and explore opportunities to leverage the rich data agribusinesses have on the farmers that supply their crops. In the long term, our research suggests that placing more emphasis on digital identity could help MNOs boost revenues and brand awareness in rural areas, reduce churn, establish positive relationships with local government and enterprise clients, and help expand the country's mobile money ecosystem.

Lessons from this research were shared with Vodafone Ghana at a multi-day workshop in January 2018. The workshop brought together several Vodafone teams and external partners to discuss how the research findings from Sri Lanka could be used to inform a local economic ID project targeting smallholder cocoa farmers. The workshop validated a key assumption of our research in Sri Lanka: that even in different contexts, smallholder farmers share many of the same identity-related needs and pain points, including inadequate information and training on new farming methods; lack of market information and market access; climate change-related impacts like drought; inadequate support from government; limited access to credit; lack of farming tools and inputs; lack of insurance coverage; and low levels of productivity. Consensus was reached that an economic ID solution could help address most of these challenges while also bringing commercial value to Vodafone. To inform the design of this solution, the GSMA returned to Ghana to conduct further research to investigate the financial and identity needs of local farmers. Many of the insights collected through this work were published in our 2019 report, Mobile-Enabled Economic Identities for Smallholder Farmers in Ghana.

Sri Lanka: creating economic identities for fishermen

Lessons from our engagement in Ghana are also informing our work with Mobitel Sri Lanka, which is building and piloting an economic identity platform that consolidates various end user data (on an opt-in basis) to generate an economic ID for people working in the country's coastal small-scale fishing sector. This project was supported through identity landscaping and field research our programme conducted in March 2019 in three coastal districts of Sri Lanka (Negombo, Matara and Kalutara). The focus was on communities where small-scale fishing is the main source of economic livelihood. The research showed that many small-scale fishermen[6] struggled to access finance from traditional financial services providers and banks because they were daily wage earners and repayment terms were not aligned with their economic behaviours. Fishermen also struggled to physically access financial services in some instances, due to their daily schedules (most fishing activities took place between 3am and 7am, with the daytime reserved for processing and resting) and the expense of travelling to a main town to reach a bank.



Location of field research plus images of round table discussions as part of the field research.

6. Research was also conducted among women in small-scaling fishing communities. However, a key finding was that men tended to take part in daily fishing activities (e.g. going to sea to fish and/or working as deckhands on a boat) while women tended to be involved in processing. Research did not include the fishing activities of industrial-scale trawlers. Given this reality and for the sake of brevity, the term "fishermen" is used throughout this report, although a small number of women do travel to sea to fish.

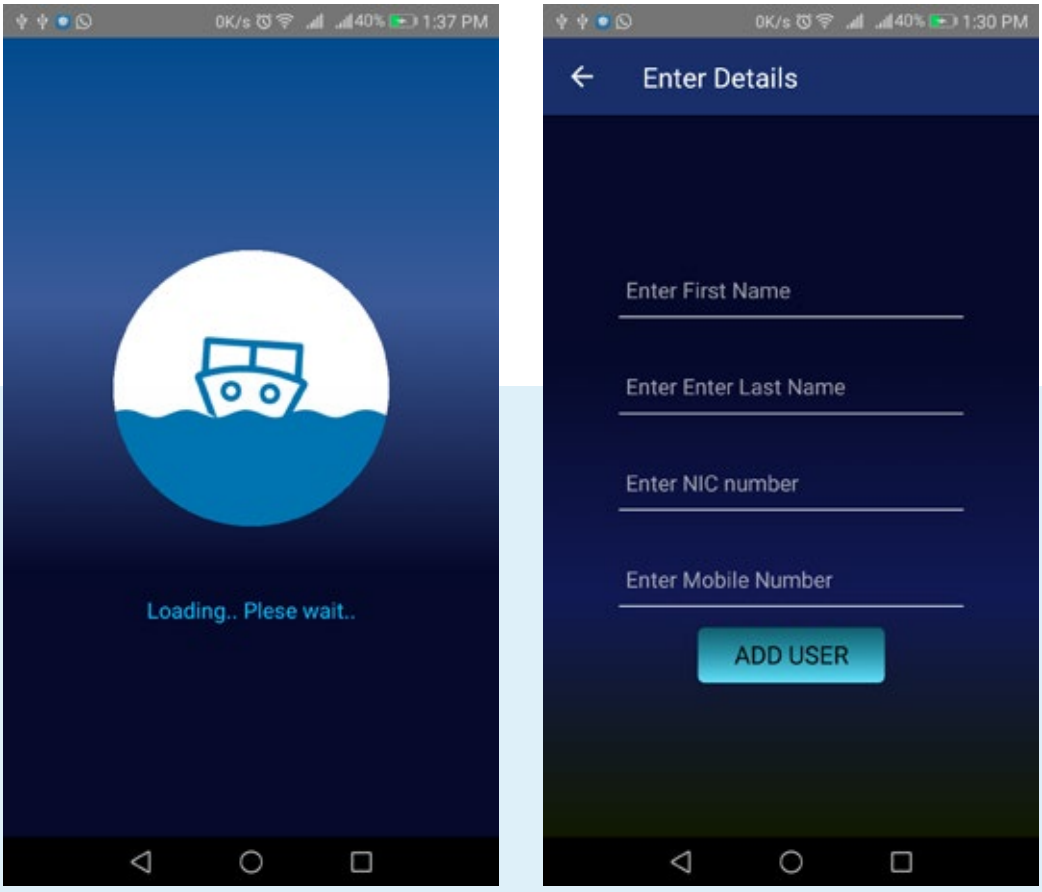
The economic identity platform has been designed with user consent at its core. After a person is onboarded to the platform, it brings together various data points (some of which are already captured through standard KYC processes while others are generated as a user engages with mobile financial services and other value-added services). The platform's ability to provide a holistic view of a user's economic behaviour and financial patterns over time (e.g. receiving payment for fish via a mobile money platform or using this platform to save regularly, pay bills or manage small loans) will help both Mobitel and financial services providers paint a more accurate picture of an end user. This is particularly valuable if that end user falls within an historically unbanked or underbanked demographic due to a lack of formal and documented economic activity.

A Mobitel agent in Matara participating in the field research and explaining how SIM and mCash KYC processes work in practice.

A typical day's catch for a fisherman in the village of Gandara.

The Digital Identity team worked closely with Mobitel until the technical development of the platform was complete and live testing began in late 2019. After completing the field research, the programme worked with Mobitel's Mobile Financial Services team to secure investment to develop an economic identity platform, map out a customer journey and identify the various data sources and internal Mobitel systems that would need to be integrated to maximise the utility of the platform and develop the necessary outputs.

From December 2019 to February 2020, the economic identity platform was piloted in three districts of Sri Lanka: Matara, Kalutara and Negombo. For Mobitel, the main business objectives of the pilot were to identify what data inputs would be required to create a customer's economic identity; to engage with stakeholders across the value chain to determine which data inputs might already be digitised; to assess the demand-side requirements of financial services providers in Sri Lanka (which would be relying on economic identities to de-risk this market segment); and to assess the demand for microloans (and possibly other financial services) within the small-scale fisheries industry.



(Screenshots of the economic identity platform)

The following recommendations were made to deploy the project:

- Gain important insights into the economic behaviours, needs and challenges of those working in Sri Lanka's small-scale fisheries sector;
- Drive financial inclusion in the small-scale fisheries industry through better-targeted mobile money offerings;
- Expand the microloans market in the fisheries sector; and
- Promote the use of Mobitel's mCash platform as a valid and acceptable form of day-to-day financial activity among a population that has traditionally been financially excluded.

Over 300 fisherman were registered on Mobitel's platform by regional Mobitel teams. The fishermen who were onboarded represented a range of ages and income levels (Table 1). Lessons from this pilot have strengthened Mobitel's understanding of identity-linked financial services, and will ultimately be used to tailor the economic identity platform to address the specific financial needs of other unbanked populations in Sri Lanka (e.g. widows, rural residents). Mobitel will analyse the data, spending patterns and behavioural trends captured by the pilot before deciding how and when to scale the platform, and release it to a larger audience and other unbanked populations.

Table 1:

Age and income levels of fishermen on Mobitel's economic identity platform

Income range (Rs)	Matara	Kalutara	Negombo
Below 25,000	26%	23%	35%
25,000–50,000	60%	67%	34%
50,000–100,000	32%	7%	10%
100,000–200,000	1%	1%	1%
Above 200,000	0%	1%	19%

Age	Matara	Kalutara	Negombo
Under 25	3%	11%	11%
25–30	6%	10%	4%
30–40	20%	35%	18%
40–50	29%	31%	34%
50–60	27%	11%	24%
60 and older	14%	2%	9%

The fishing harbour at Gandara (Matara District). This area was hit quite badly by the tsunami in 2004, and many fishing families still receive tsunami recovery subsidies from the government.

Social benefit payments

Social protection systems are designed to help individuals and their families cope with financial crises and shocks, find jobs, improve productivity, invest in the health and education of their children and remain financially secure in old age.[7] Social cash transfers (SCT) are one component of social protection systems, and are used to provide regular and predictable support to the poor and vulnerable.[8] To implement social benefit payments programmes efficiently, institutions are required to carefully manage the selection and enrolment of beneficiaries, the targeted and transparent delivery of funds, and the provision of ongoing communication and support. Effective and widespread identification methods are essential to these processes, but several issues are likely to hinder them.

In areas where identity coverage is low, SCT programmes are likely to face challenges as they often require beneficiaries to validate their identity in person as part of the cash disbursement process. These processes are typically more expensive and less efficient than digital methods of identity verification, for both the beneficiary and the organisation delivering the cash transfer. However, when cash transfer programmes become digitised, it can be more difficult for organisations to accurately confirm whether a specific beneficiary has received and used their cash. For example, it might be difficult to recognise whether a cash disbursement aimed at a woman is delivered to a bank account or mobile money wallet controlled by a husband or older family member. Digital approaches to identification could enable individuals to unlock greater value and benefit as they interact with government and other organisations, while also helping to streamline and add transparency to social benefit payments.

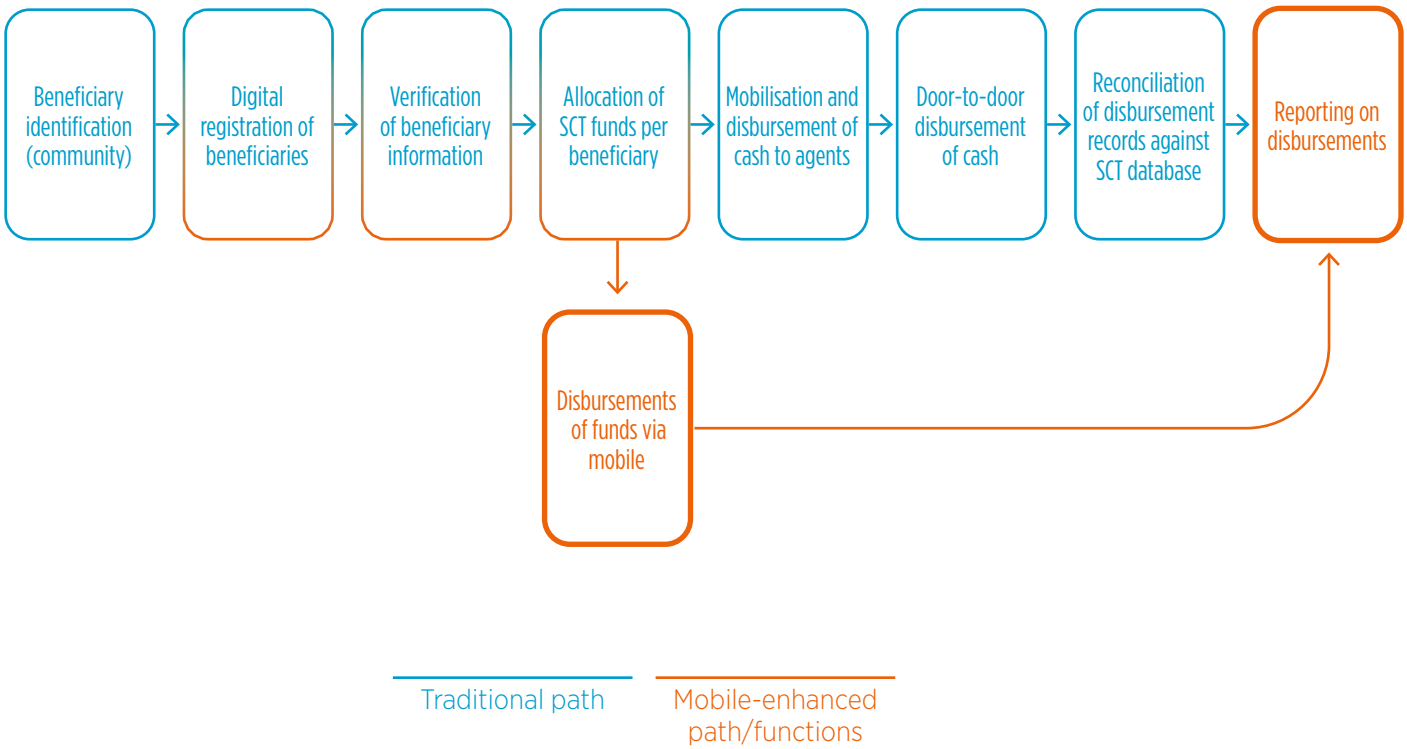
7. https://www.worldbank.org/en/topic/socialprotection/overview
8. World Bank (2015), The State of Social Safety Nets 2015.

In Zambia, the GSMA is exploring how MNOs can support the delivery of SCTs initially by developing an API[9] that allows social benefit programmes to verify a beneficiary's mobile number by matching a unique identifier (such as their national ID number) with information held in the MNO's KYC database. This makes a mobile number a more robust and reliable way to reach the intended beneficiary, and a more efficient way to disburse benefits (e.g. cash or vouchers delivered via mobile money). However, one of the next steps being discussed is developing a business model for MNOs to provide Verification as a Service (VAAS) using voice. Our programme sees great promise in voice biometrics, not only to verify that benefits have been received by the intended beneficiary, but also to provide a better customer experience, especially for vulnerable or disabled populations. Considering the growing number of social benefit programmes that rely on mobile to identify and deliver social benefits to vulnerable citizens, there is significant potential for MNOs to offer VAAS. The ability to verify a beneficiary's identity remotely will allow social programmes to reach greater scale, and will also be relevant in commercial applications, such as banking, insurance and health. The GSMA has engaged with local stakeholders in Zambia, including government, donors and implementation partners, to explore the opportunity, validate the hypothesis and examine the role that mobile-enabled digital identity could play in SCT programmes (Figure 4).

As a result of these engagements, technical integration between the disbursement authority and the mobile money provider's platforms has been completed (at the end of 2019), and the next phase of the project will focus on live verification of beneficiaries in a pilot of planned disbursements (planned in 2020).

Figure 4

The role of mobile in social cash transfer programmes



9. An API, or Application Programming Interface, is what allows software programmes to "talk" to one another. Operator APIs make it possible for third parties to use certain mobile network functions within their applications.

GSMA-hosted workshop, Lusaka, Zambia

GSMA convening, Chirundu, Zambia

Research: improving beneficiary identification in SCT programmes

Building on our experience in Zambia, in late 2019 the GSMA conducted research to further explore the opportunity for MNOs to support SCT programmes in the disbursement process, with a focus on the steps involved in identifying and verifying beneficiaries. The study focused primarily on government-to-person (G2P) cash transfer programmes as these are of particular interest to MNOs, due to their relatively large scale and often long-term, reliable nature.

Based on insights from primary research in Kenya and Malawi, the study explores:

- The potential size of the opportunity for MNOs;
- The identity-related constraints experienced by SCT programme stakeholders and the beneficiaries of these programmes; and
- Commercially viable opportunities for MNOs to support SCT programme stakeholders in overcoming these identity-related challenges.

Despite the differences between the country programmes, beneficiaries in both Kenya and Malawi experienced challenges related to when and where they could cash-out and how their identities were verified.

Kenya has a large-scale, relatively uniform and coordinated government SCT programme. The National Safety Net Programme (NSNP) has high levels of digitisation, widespread foundational ID coverage (a national ID) and high mobile and mobile money penetration. In this context, there is an immediate market opportunity as MNOs have a variety of assets already in place, including mobile money services, mobile agent networks and verification services. These assets could be leveraged to help NSNP providers make SCTs more accessible to end users, particularly at the point of disbursement and/or cash-out.

In contrast, Malawi's government programme has low levels of digitisation and a fragmented approach to implementation, combined with relatively low mobile penetration and low mobile money adoption. However, following the recent and rapid increase in national ID coverage in Malawi, together with a drive to streamline and digitise the SCT sector, there are emerging opportunities for MNOs to engage with SCT providers and support the payment delivery process. One possibility is offering verification services at the point of disbursement and/or payment collection.

MNOs are well positioned to support government stakeholders in overcoming these challenges. For example, by developing identity verification solutions to complement their payment platforms and leveraging the various attributes they have gathered on customers, including national identity numbers and mobile phone numbers. Other mobile services, such as SMS prompts, one-time passwords (OTP) and voice or facial recognition, could be introduced to provide the disbursing entity with higher levels of assurance that funds reach the intended beneficiary. These mobile-enabled verification options could also support payment collection by a proxy in instances where the registered beneficiary is unable to appear in person. It is important to note that MNO stakeholders felt strongly that it would only be in their interest to offer mobile-enabled verification services to SCT programme stakeholders if they were also the payment provider, as this was identified as the primary commercial opportunity.

Health identities

SDG 3 aims to “ensure healthy lives and promote well-being for all at all ages”, yet according to the World Health Organisation (WHO), at least half the world’s population still lacks access to essential health services, with almost 100 million people annually pushed into extreme poverty due to out-of-pocket health expenses. For the one billion people who are unable to access proof of identity, it remains particularly difficult to access financial aid, prove their eligibility for treatment and be included in government healthcare plans.

In our 2019 case study, Innovative Mobile Solutions Linking Health and Identity, we examine four mobile-enabled platforms that are helping to create unique health identities in low-income countries across Asia and Sub-Saharan Africa. These, in turn, are helping patients access timely, consistent and more affordable health services; expanding access to low-cost health insurance; and improving the way patient information is shared and used. Although these platforms are still in the early stages of development, early evidence suggests that digital heath identification platforms are creating new opportunities for MNOs to develop cross-sector partnerships; deliver social impact and generate new revenue through subscription and service fees (from patients, doctors and health centres); and introduce customers to new life-changing, value-added services, such as mobile money and remote healthcare.

The platforms showcased in the report include:

- **Element**, which develops and distributes a mobile-based, software-only platform for biometric identity. Its end-to-end biometric solutions are being used to build global immunisation platforms, enable connected diagnostics, provide a digital identity resource for healthcare providers and open access to financial services, among other services.
- **Kea Medical's** Hospital Information System was developed in 2017 with the aim to connect hospitals in Benin, and eventually across Africa, through a single database of patients' medical information. The platform creates universal medical identities for patients that are then linked to a mobile scannable QR code, enabling access to a patient's medical history at any time, from any location.
- **Dialog Sri Lanka's Doc990 platform** enables patients to digitally book and pay for appointments with doctors and health specialists. It has also expanded to include several complementary services, including teledoctor services, virtual pharmacies and the ability to access remote consultations and lab reports. In addition, Dialog is developing a centralised online portal that allows patients to securely access and store their health records.
- **Vodacom Lesotho** has worked with a number of partners to design and launch the Mobilising HIV Identification and Treatment Initiative, which aims to increase the number of HIV-positive children being tested and accessing antiretroviral treatment over a three-year period. The initiative raises awareness, improves access and makes the service more efficient through the use of mobile technology. The solution was designed to be deployed nationally and to reach remote mountainous regions.

In 2019, the GSMA supported a Kenyan MNO to explore and develop a digital health ID platform. The MNO aims to leverage its KYC data to enable patients to access portable medical records on one secure platform, unlike the current system in which paper records are held at disparate health facilities. Patients provide consent digitally and can share their medical profile or history with their doctor. For the MNO, value-added opportunities could include the development of a full-service health app; access to financial services (such as small loans or bill payments); revenue sharing with health facilities; or upselling health insurance products. The importance of strong partnerships cannot be stressed enough, and MNOs should collaborate with experienced players in health information systems to ensure the health ID platform is useful in both private and public sector health facilities, which will be key to ensuring reliability and achieving scale.

The role of mobile in bridging the identity gap and enabling access to government services

The most significant identity gaps are in areas where mobile connectivity and mobile agent networks continue to scale, which means MNOs are well placed to provide national governments and other ecosystem players the opportunity to leapfrog inefficient, paper-based registration systems and offer more inclusive ways to provide unique identities to the underserved. Governments could also leverage the extensive reach and network assets of MNOs to strengthen existing identity enrolment, verification or authentication processes, or to enable secure access to e-government services (which may also incentivise uptake of digital identities). Through our Policy and Advocacy workstream, we have engaged with a number of governments to explore how MNOs could support efforts to bridge the identity gap, and to share best practices in creating more enabling policy environments for digital and financial inclusion via mobile.

A few of the engagements we have supported include:

Tanzania: Through a series of workshops and engagements we held in 2016, the Telecoms Authority (TCRA) and Tanzanian National Identity Authority (NIDA) came to recognise the constructive role MNOs could play in the roll-out of a national ID through their retail network and supporting consumer awareness campaigns on how to register for the national ID. Our engagement also resulted in an agreement that TCRA would re-establish a steering committee of MNOs, NIDA and other strategic partners to work on a clear and milestone-driven approach to expedite the roll-out of national IDs. The TCRA also recognised it was important to ensure, in the interim, that consumers could access mobile services with other forms of acceptable identification.

Uganda: In early 2018, the Ugandan Government, through its National Identification and Registration Authority (NIRA), began investigating how to develop a mobile ID platform. Although there are over 100 e-government services available to the public, they are not interoperable or accessible via the same portal, and citizens must register with different usernames and passwords. NIRA therefore wanted to explore how the e-government platform could be linked to a mobile ID that people could use once their mobile SIM card had been registered and validated against their biometric ID card. Following a series of engagements between the GSMA Digital Identity team, NIRA and NITA (and in close collaboration with the World Bank's ID4D team), NITA hosted a workshop to allow all MNOs in the country to provide suggestions and discuss how the mobile ID could be rolled out. Positive feedback from NITA indicated this was the start of a fruitful consultation exercise in which MNOs had (and will continue to have) an opportunity to help shape the emerging mobile ID ecosystem (noting that a number of parameters are beyond their control). Once rolled out, this platform would be an example of a government policy (and investment) putting mobile at the centre of a digital transformation strategy.

Nigeria: Following a series of preparatory meetings, the GSMA Digital Identity team hosted a workshop in Abuja, Nigeria, in April 2018 that convened all government bodies involved in the development of the country's new digital ID ecosystem, as well as representatives from the World Bank and all MNOs in Nigeria. This workshop was the first time policymakers and MNOs had come together, and it led to the first official acknowledgement by the government that partnerships with MNOs in the nationwide ID enrolment effort would be extremely beneficial, not least because the four largest MNOs have over 70 million unique mobile subscribers between them while fewer than 40 million Nigerians had registered for an official national ID by early 2018. The GSMA's workshop concluded with all parties agreeing to work together to achieve the same goal: a ubiquitous, robust and inclusive national ID database for all Nigerians. There was consensus that a practical partnership model had to be developed for MNOs to support the National Identity Management Commission's (NIMC) enrolment strategy, while also ensuring seamless SIM registration for end users, in collaboration with the Nigerian Communications Commission (NCC).

In March 2019, the NIMC published an advertisement inviting private sector entities to formally express their interest in becoming licensed partners to support citizen enrolment in the new digital ID programme. This paved the way for MNOs in Nigeria, and hopefully elsewhere, to play a much more hands-on role in the digital ID ecosystem and offering other services to their (newly identified) customers, which may be as many as 100 million. As of January 2020, it is the GSMA's understanding that discussions are continuing between the government and MNOs on the details of the public-private partnership.

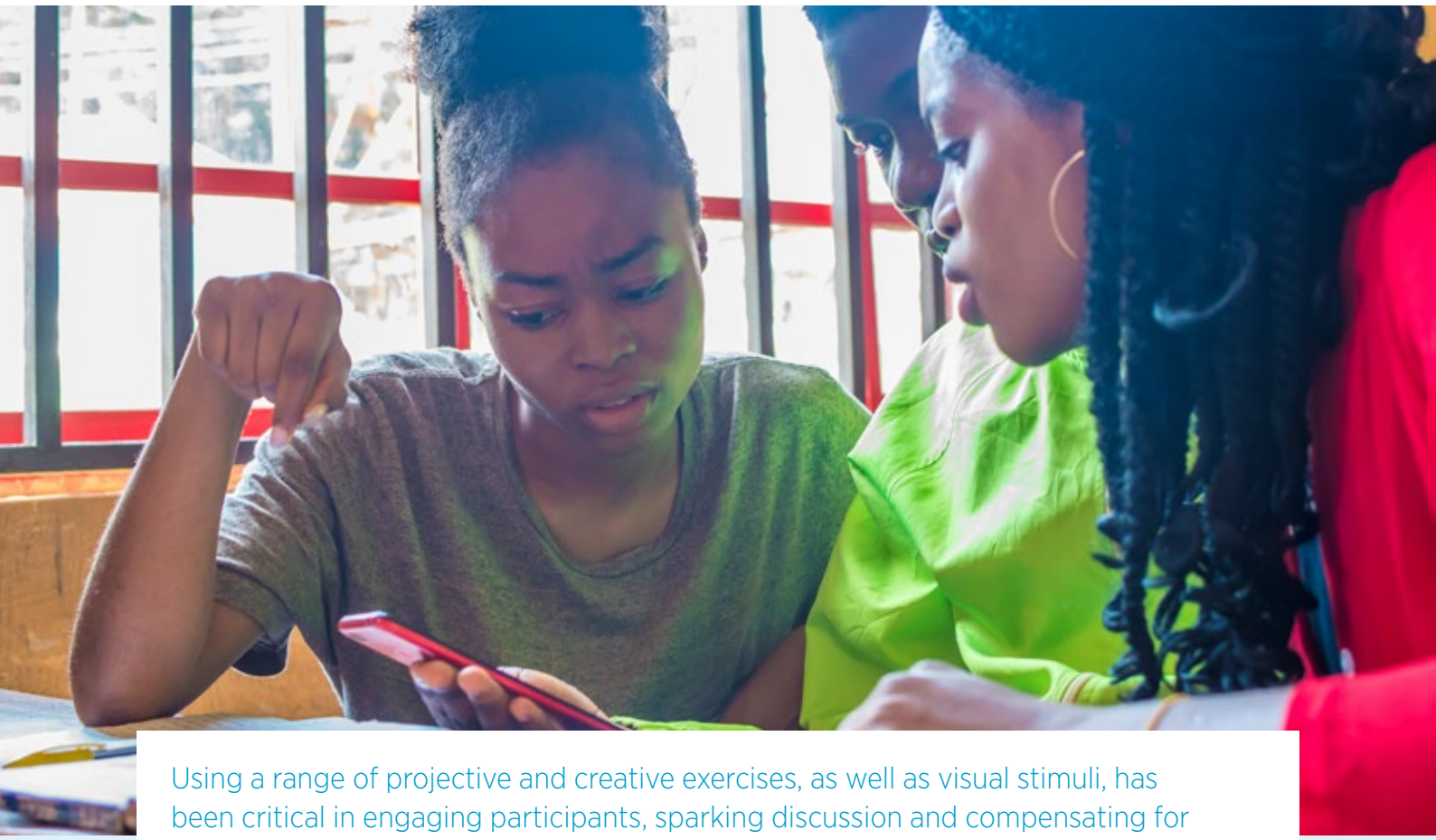
3

Key lessons learned

Research and insights

Our research with end users has highlighted the complexity of investigating individual perceptions of, and attitudes towards, identity. Our discussions often explored questions about identity (one's status as a unique individual in society), identification (the process by which one proves their specific identity) and the identity document/credential (or ID) that one uses as proof of identity. These distinctions become more complicated in the interplay between mobile phones and identification. Participants identified a range of overt identification processes related to mobile, including compliance with SIM registration and KYC regulations, but also more informal and intangible roles, such as end users calling friends or family members to vouch for them; services like e-government services in Rwanda using two-factor authentication by linking national IDs to mobile numbers; and people relying on their mobile handsets and SIM cards to store important identity information or photographs of ID cards.

We've learned that people's understanding of identity is often unique to where they live, and that participants' ability to discuss, interrogate and critique digital ID concepts can be influenced by a range of contextual and cultural factors. For example, how individuals operate within and outside their local community; how terms related to "identity" and "identification" are translated into local languages; the kinds of identity documents an individual already owns, uses or is aware of; how easy it is to access services without any form of identity; one's level of digital literacy; the role women play in the household; the political and national security landscape; and even the way in which the researcher and interviewee choose to introduce themselves. When participants are asked too early in a discussion to list the different kinds of identity documents they own, it can be difficult for them to think about identity as more than physical documentation, or to consider how new identity solutions could help them adopt new identity-related behaviours. Conversely, introductory questions, such as "What do you take pride in?", "How do you introduce yourself?", and "What do other people know about you?", are insightful and helpful primers.



Using a range of projective and creative exercises, as well as visual stimuli, has been critical in engaging participants, sparking discussion and compensating for low literacy, shyness and unease about sensitive topics. When pitching new digital identity concepts to end users, it has been helpful to explain how the concept is both use case-driven ("This is the problem it could solve") and process-driven ("This is how it would work"), but only to the extent that individuals feel reassured about the reliability and security of a service (data privacy is an increasingly emotive topic), and feel informed enough to explain why the concept would or would not meet their personal needs. It has also proven helpful to introduce concepts by inviting the respondent to play an active role in the design process; for instance, by saying, "We have an idea, but we need your help making this better." Prompts such as this encourage respondents to think creatively about how to improve the utility of the concept, rather than politely agreeing that it is a "good idea".

It is vital that any research project investigates stakeholder perceptions and attitudes about the identity-related needs and barriers faced by end users, particularly women. Our projects typically begin by engaging MNOs and other key stakeholders in a country's identity ecosystem to build a simple vision of what stakeholders would like to achieve through digital approaches to identity, and identify how they would like to partner with MNOs to achieve this vision. The conjectures and recommendations made in this phase of the research were used to tailor our approach to the end user research, and to develop early prototypes and ideas on how identity solutions or identity-linked services could work in reality. Allowing stakeholders to be actively engaged in, or even co-design, the research helps ensure it is meaningful for everyone. This is particularly important when researching identity because it does not exist in isolation; it is an essential process, component or aspect of many other topics, products and services.

Our research has also helped us consider the design principles that should be followed when developing digital identity products and services that are inclusive, user friendly and encourage uptake.

For instance, low-income consumers often use basic handsets with limited functionality and tend to have low levels of digital literacy; therefore, digital identity solutions must be functional on the most basic handset and easy for customers to use without support from others. Furthermore, behaviours, attitudes and habits around existing forms of identification are easily entrenched, which means even the most inconvenient workarounds, such as borrowing an ID card or avoiding a service altogether, can seem safer and easier than using new identity solutions. To be perceived as "better" than these workarounds, digital identity solutions should be easily accessible and offer additional value or convenience, for example, turning a cumbersome manual "registration" process into a simple "digital" process. Providers of new digital identity-linked services can also encourage new habits by communicating the benefits of registering for mobile services in one's own name, or supporting frequent, simple and repetitive use of ID, perhaps by developing ID-linked services that offer small financial incentives for frequent use, or even non-financial "rewards" in the form of praise or recognition.

Finally, it is vital to remember that segments of the population without a form of official identification are not a homogenous group, and several factors influence an individual's identity-related needs and priorities. For instance, our research has found that compared to older participants, younger end users tend to be more digitally literate; better connected to, and more aware of, the outside world; more willing to use digital channels to access information, advice and support; and more concerned about how their personal data is used. The same could be said about functional identities created to access a specific service/function. For example, in Sri Lanka and Ghana, we found that a farmer's needs and potential use of a functional digital identity can be influenced by their age, social capital, digital literacy, ability to manage uncertainty, perception of themselves and even the types of crops they grow.

When designing services and marketing them to specific target groups, MNOs and their partners should therefore balance the development of scalable and generic functional digital identity services with customisable interfaces.

Policy and advocacy

Through our programme's policy and advocacy engagements, we have learned several lessons about the role of policy and regulation in strengthening mobile-enabled digital identity ecosystems, for example:

- **There is inadequate appreciation of how proof of identity requirements can lead to digital and financial exclusion, especially in countries where official identity penetration is low.** With over 155 governments mandating mobile SIM registration and all (90+) central banks enforcing KYC requirements on mobile money providers, the ability of an individual to access mobile communications and mobile financial services in one's own name is wholly dependent on having an official, government-recognised form of identification. A number of governments we engaged with are enforcing these requirements to drive demand for (new) digital ID enrolment without due regard for the needs of vulnerable people, who may not be able to register for an ID and link it with their MNO or mobile money subscription by the government's deadline.
- **Demand is high for government capacity building on the role of public-private partnerships with MNOs.** When engaging with governments in countries where identity penetration is low, we have seen high demand for understanding how mobile can bridge the identity gap by supporting enrolment, and how to leverage the mobile (internet) platform to offer access to new digital services (such as e-government portals) that would, in turn, incentivise people to register for a (digital) ID. Trust between the government and the mobile industry is key, as is the ability to see SIM registration and KYC as an opportunity rather than a compliance burden.
- **Appropriate privacy and data protection frameworks are needed to build trust in the ecosystem.** Innovations in the analysis of personal data are only possible if people trust the various stakeholders and give consent for their data to be used in the context of digital identity solutions. A country's legal framework must also confer rights and liabilities around privacy and data protection, and have checks and balances providing clarity and limits on a government's power to access data on an individual's use of mobile communications.
- **Coordination is needed among government stakeholders (and the private sector) when designing digital identity ecosystems.** Authorities in charge of developing or updating a country's ID ecosystem may fail to consult with other public sector bodies that have an active interest in a well-functioning and robust identification structure (e.g. central banks, telecom regulators, ICT, finance and agricultural ministries, tax authorities, CRVS, electoral commissions). Proactive coordination between these actors, as well as the private sector (e.g. MNOs and banks), is therefore needed to ensure the design of a digital ID ecosystem is inclusive, efficient and effective.
- **Digital ID enrolment processes must be inclusive, accessible and future-proofed.** Governments designing digital ID processes should consider adopting technical standards rather than proprietary solutions that would lead to vendor lock-in. Policy frameworks should also be revisited to ensure they do not include discriminatory or exclusionary provisions that would have a negative impact on vulnerable populations.

Market engagement

Over the last four years, we have seen that the GSMA has a critical role to play in bringing together MNOs, development partners and public sector stakeholders to address some of the identity-related challenges faced by end users, governments and development agencies. Presenting lessons learned through research or market engagement activities has helped development partners better understand the roles MNOs can play in addressing these challenges, as well as the need to consider appropriate commercial incentives and cost implications for MNOs.

The concept of digital identity is still new to many stakeholders. Our programme's work with MNOs has also made it clear that digital identity should not be viewed as a vertical, but rather horizontal enabler that supports the provision of, and access to, a wealth of other services in a digitally transformed economy. In many countries, MNOs are engaged in a range of activities that are either enabling a foundational digital identity ecosystem or could be considered a form of functional digital identity in certain contexts, such as health, education or agriculture. A number of MNOs are already engaged in activities that involve digital identity, for example, analysing mobile money transactions or microloan repayment data for credit-scoring purposes, or offering value-added services (VAS) to customers.

The deployment of scalable, mobile-enabled digital identity platforms often depends heavily on a government's commitment to building digital, secure and verifiable foundational forms of identity. Government leadership in creating digital identity ecosystems can also be a motivating factor for MNOs to leverage their infrastructure to support such efforts. For example, the Zambian Government, through its Smart Zambia division, has openly and enthusiastically worked in consultation with MNOs to address some of the identity challenges that the government and local development partners face, such as the digitisation of CRVS systems, and effective and secure verification of Zambians who receive payments through social benefit programmes.

Finally, in the absence of a digital identity strategy (which only large multinational MNOs tend to have), a hands-on approach is necessary when engaging with smaller, local MNOs. This will help to determine how a digital identity use case fits into an MNO's commercial objectives and the added value it can offer to the development and deployment of a digital identity platform. For example, when the customer journey for Nigeria's economic identity platform was being developed, our programme held a workshop and tested assumptions with end users before 9mobile embarked on the design and technical development of the platform.

For an MNO, it is critical to look at digital identity through a commercial lens, since buy-in depends on the business case and scalability of a digital ID initiative. There are many interesting use cases and applications for digital identity, but the deployment of these platforms must be aligned with the MNO's commercial incentives and regulatory reality. As we have seen across the mobile for development arena, commitment from the highest levels of management is critical to ensuring that digital identity use cases can be viably researched and tested in market.

4

Looking ahead

Reflecting on the lessons and insights from the first phase of the Digital Identity programme, our next phase will focus on addressing specific digital identity challenges in selected countries where mobile platforms can offer socially impactful solutions in commercially sustainable ways. To achieve this, the programme will:

- **Promote the role of mobile in digital ID ecosystems,** for example, by facilitating strategic partnerships between public sector bodies, NGOs and MNOs to improve access to digital identity solutions via mobile platforms (e.g. improved verification of beneficiaries in social cash transfer programmes).
- **Support the development of enabling policy and regulatory environments**, for example, by sharing best practices, delivering capacity building courses and/or convening workshops with representatives from various public authorities with a stake in a country's digital identity ecosystem.
- **Participate in relevant global forums, engage with and continue partnerships** with key international, regional and national bodies to influence emerging principles and standards, and to disseminate programme messaging and best practices.
- **Conduct original research, generate insights and capture best practices.** The programme will continue to provide intelligence and analysis that position the GSMA as a thought leader in digital identity, and showcase the role of mobile and MNOs in strengthening digital identity ecosystems, including through effective public-private partnerships.

gsma.com

For more information, please visit the
GSMA website at www.gsma.com

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601