Mobile for Development

M4D Impact Products and Services Landscape

Quarterly Report November 2015

Hannah Metcalfe

Executive Summary

Over the last year, we have showcased many new products and services from our M4D Products & Services Tracker. As the number of mobile products and services increases, the opportunity for identity solutions has also grown.

Digital identity unlocks new opportunities for people in emerging markets who do not have other formal means of identity, such as a passport or national ID card. In particular, it gives people living in rural areas or those with low literacy the chance to register themselves and become eligible for more mainstream government services, such as education and health care. However, it also creates new vulnerabilities: in markets where people may have little experience or awareness of data privacy issues, it is paramount that the privacy and security of their data is maintained.

In this final edition of 2015, the M4D Impact Products and Services Quarterly Report investigates the opportunities for digital identity and the different ways mobile can help countries provide their citizens with official identification more quickly.

The report will look at digital identity needs in three areas:

- Mobile products and services offering a form of digital identity
- Digital identity and Mobile Government Services
- Digital identity and Disaster Response

We still have a long way to go before digital identity fully addresses the global identity gap. However, different ways of offering digital identification to the unregistered are being explored, including mobile as a scalable and trusted solution. By looking at what is currently being offered in the areas listed above, we can identify the opportunities, barriers, and value of mobile in providing a formal identification system.

Many mobile network operators (MNOs) are interested in digital identity. Digital identity not only offers MNOs a commercial opportunity to gain access to new users, but can also improve people's livelihoods and contribute to citizens' welfare and development. Because of their large consumer base and distribution channels, MNOs are well placed to support governments and NGOs with digital identification (ID) in emerging markets.

However, while digital identity is a great opportunity, there are important privacy and security considerations. The last section of this report will look at some of the products and services that address identity protection and encryption for mobile.

Mobile Identity

It is estimated that over

1.8BN

people lack access to formal identification: women and rural populations are the groups most affected by lack of identification.

Because of its scale, the mobile industry has a unique opportunity to address this gap and work with partners to provide identity for the unregistered. This initiative builds on the global agenda around Identity for Development (ID4D) and birth registration, drawn from Article 7 and 8 of the UN Convention on the Rights of the Child. Additionally, the UN Sustainable Development Goal 16.9 aims to address the identity gap with the goal of "providing legal identity to all, including birth registration" by 2030.

Children who are unregistered (and therefore unable to prove their age) are much more vulnerable to underage marriage, child labour and underage army enrolment. Global players such as the World Bank consider offering digital identity to people living in emerging markets a 'game changer' or a 'poverty killer', as it has the potential to register people and give them a form of identification.

While our trackers contain over 2,000 products and services that serve the needs of people in a number of sectors—including health, education, employment, financial services and civil engagement—it is critical to prove 'you are who you say you are' in order to access these basic services.

In the physical world, we use certificates, cards or other documents generated by the government or service providers to prove our identity. Historically, verification of identity has been based on the individual being physically present at the point of authentication, with interaction with the person requiring the proof of ID. In the digital world, verification of a person's identity cannot rely on the physical presence of the individual, but rather requires some form of identity verification that assures both the service provider and the user that the information provided is accurate and safe from abuse.[1]

Trusting the link between a real identity and a digital identity first requires someone to validate the identity: in other words, to prove someone is who they say they are. The more valuable the digital identity, the more work is required to validate it and establish a safe and secure authentication.

1. Mobile Identity: A Point of View Paper from the GSMA July 2013

Mobile products and services offering a form of identity

In addition to specific identification services, some of the products and services that we track can potentially act as forms of recognised digital identification.

SPOTLIGHT: Vodafone Ghana Connected Farmers Club

Vodafone Farmers' Club provides farmers with farming tips, weather information, market prices, and nutrition tips. It also offers free calls between farmers in the club, free calls to the helpline and the most competitive call rates.

Vodafone Ghana is now looking to extend these club benefits to fishermen through a partnership with USAID and Société Générale (SSG). The goal is to support sustainable fishing to safeguard the fish stocks in Ghanaian waters, which have been heavily depleted. The project is in partnership with the Ministry of Fisheries and Aquaculture Development (MOFAD).

Using boat identification numbers, fishermen will be able to 'blow the whistle' on bad fishing practices by calling a hotline when they observe poor behaviour, such as fishing with lights. The hotline will be connected to enforcement agencies and the reporters will cite the number of the boats seen fishing illegally so that the offenders can be apprehended. People in the fishing ecosystem, including fish processers, will be invited to join the club as well.

The long-term goal is to sign up all fishermen for the programme and after they are registered, have their canoes numbered. In time, with government assistance, the hope is to enforce registration so that only fisherman who are members will be able to fish on the sea. This project is in its early stages, but it already has potential to align with the digital identity initiative for fisherman and farmers in Ghana.

SPOTLIGHT: Health insurance in Nigeria

MTN, Salt and Einstein MTS, and the National Health Insurance Scheme (NHIS) have partnered to launch Y'ello Health, a mobile-based universal health insurance service targeted at mobile subscribers and offered through health management organisations. This micro-insurance service offers people in Nigeria access to affordable health insurance coverage on a pre-paid basis via mobile. People pay for and access preferred medical treatments completely through their mobile.

The service is expected to help patients who need to visit hospitals at least twice a month (up to 7 times a year) get medical coverage of up to NGN80,000 ($402) annually.

MTN is Nigeria's largest MNO, and it is suggested that nearly 80 million people now use this service. Because of the information that users provide when registering for this service, Y'ello Health could serve as a form of digital identification for Nigerians who might not have previously had any.

While these services potentially offer certain segments of society a form of identity, there is a risk that they could make digital identity solutions more fragmented. In many markets, public and private stakeholders are competing to offer identification in many forms, such as health insurance cards, bank identity cards, or voter identity cards.

Digital Identity and m-Governance

Because of this fragmentation in digital identity solutions, there is pressure on national governments to align their efforts and focus on nationwide services.

In the second edition of the Products and Services Quarterly Report, we put a spotlight on our Mobile Government and Citizen Engagement Tracker. Within this tracker, we track mobile Government services—services that are run or owned by government that benefit citizens, businesses and Government units in a particular country.

As the number of mobile products and services continues to grow, it has become clear that they will only become sustainable in the long term if they can securely authenticate the identity of individuals and organisations.

For governments, digital identity provides a cross-sector platform on which to build a robust and reliable identification system. More products and services can be delivered via mobile, giving governments a greater opportunity to actively engage with citizens and share information on government-related matters: for example, paying taxes via mobile, reporting road damages, or registering to vote via a mobile phone.

To deliver services more efficiently, identification is key. Identification can also be the basis for a more secure society, as it gives governments greater knowledge about their citizens' demographics.

SPOTLIGHT: India Aadhaar and mobile

India has paid particular attention to digital identity. Digital India is a programme aimed at transforming India into a digitally empowered society, and its vision is centred on three key areas:

Digital infrastructure as a utility to every citizen

Governance and services on demand

Digital empowerment of citizens

SPOTLIGHT: India Aadhaar and mobile

In 2010, the Indian government developed a large digital identification scheme with the aim of registering 1.2 billion citizens via biometric data (fingerprints and iris scans) and providing them with a unique 12-digit identification number, known as Aadhaar.

Unique Identification Authority of India's (UIDAI) Aadhaar system already offers a mechanism to link mobile numbers to the Aadhaar identity. Aadhaar authentication also offers mobile One Time Pin (OTP), an automatically generated numeric or alphanumeric string of characters that authenticates Aadhaar users for a single transaction or session. Government applications can take advantage of Aadhaar's strong link to mobile in two ways:

- **Verifying the identity of a user using demographic authentication.** Government service applications can check the "Aadhaar to mobile number" link by using demographic authentication (data checks on a person's age and gender). This could ensure that the mobile number and Aadhaar correspond with a user's demographic profile.
- **Using the Aadhaar OTP service to authenticate an Aadhaar holder.** Government service delivery applications can use the Aadhaar OTP service to authenticate users without storing their mobile numbers or creating their own authentication mechanisms.

SPOTLIGHT: Genkey, Tanzania

Digital identity has also been a focus in Tanzania's recent elections. Genkey, a Dutch identity solutions provider specialising in elections and healthcare, launched a national project in Tanzania to provide its biometric identity solutions for the 2015 October elections.

During the voter registration exercise, 24 million eligible Tanzanian voters were biometrically enrolled. This involved identifying a voter by their fingerprints, iris, voice, etc., and registering these voters in the Permanent Voter Register (PVR). GenKey's large-scale biometric-based deduplication solution was selected to ensure that each voter was enrolled only once. The GenKey SPiRE Voter ID Management Solution can set up and maintain the country's overall electoral process, upload and manage the voter registration data, and compile an accurate and credible voter register.

By using a system like this, government can enrol and identify millions of voters quickly and with a smaller risk of mistakes. This is beneficial to government and society because it minimises election fraud and makes the voter identification process more efficient.

For this project, GenKey was a subcontractor to Lithotech Exports of South Africa, the company that was awarded the contract by the National Electoral Commission (NEC) of Tanzania.

Digital identity in disaster response

Digital identity is also a key component for many mobile-based disaster response products and services. Identity plays a significant role in the aftermath of a disaster, particularly for displaced populations.

Migrants and refugees are often unable to provide identification, because they may have to leave their homes with very little notice and may not have even had official identification in their home country in the first place. With the 2015 European refugee crisis in the headlines and at the forefront of political discussion, the role of mobile and identity is once again being considered.

SPOTLIGHT: BITNATION: Blockchain Emergency ID

This project was created to provide Emergency Services and Humanitarian Aid to refugees during the European Refugee Crisis of 2015. Bitnation aims to provide the same services as traditional governments, such as insurance, security, marriage, death certificates, and land titles.

Bitnation is a collaborative platform for 'do-it-yourself government' that uses blockchain technology. Blockchain technology is seen as the main technological innovation of the digital peer-to-peer payment system bitcoin, since it stands as proof of all the transactions on the bitcoin network, which can then be used to authenticate someone's identity. A block is the 'current' part of a blockchain that records some or all of the recent transactions: once completed, it goes into the blockchain, which is a permanent database.

One of Bitnation's recent initiatives is the Blockchain Emergency ID, which gives refugees an emergency digital identification and a bitcoin visa card so they can receive funds from family even if they don't have a bank account. Blockchain Emergency ID is a basic emergency ID service based on blockchain technology. Blockchain Emergency ID is targeted at individuals who cannot obtain other documents of identification.

The purpose is to cryptographically prove your existence and family relations, which are recorded on the bitcoin blockchain. What makes blockchain technology important to digital identity is that the platform is hardened against tampering and revision, making the authentication of these individuals not only protected and secure, but also more legitimate.

The Blockchain identification works like a mini 'web of trust', where family members have to verify each other's family ties. Proving family relations can make it easier to reunite with your children, parents, or siblings, who may be in different locations.

The identification form generates a QR code (the image), which should be saved on a user's mobile. All the information on the form is readable through that QR code.

SPOTLIGHT: BITNATION: Refunite

The United Nations estimates that due to the Syria crisis, people are being displaced at the rate of one person every 15 seconds. Current family tracing programmes, which are often paper forms completed in pencil, offer little opportunity for information to be shared across agencies, borders or conflicts. This makes it much harder for refugees to be reconnected with relatives and friends. There is a demonstrable need for collaborative technology to be integrated into the family reconnection process, so Ericsson, Refugees United, and MNOs across the Middle East responded by partnering to expand these services with mobile.

REFUNITE is a non-profit technology organisation focused on reconnecting refugee families across a number of countries. Using an online and mobile platform, REFUNITE helps displaced people take the search for missing family into their own hands, free of charge. REFUNITE has longstanding partnerships with Ericsson and UNHCR, which has strengthened its ability to overcome the problem of family separation.

People living in refugee camps can use SMS, USSD, voice, and web to register for the service and then call a hotline (run from a Refugee Unites office) for support and advice on registrations.

This initiative has currently been deployed in nine countries: Kenya, Uganda, South Sudan, Somalia, Jordan, Turkey, Iraq, Democratic Republic of Congo (DRC), and the Philippines.

Access to REFUNITE services:

Search Through SMS

Turkey: send 1 via SMS to short code 9254 to start your search (free for subscribers of AVEA)

Iraq: send 1 via SMS to short code 380 to start your search (free for subscribers of Asiacell)

Jordan: send 1 via SMS to 91476 to start your search (free for subscribers of Zain)

Call Us

Kenya: 0800 724 882 (free for Safaricom subscribers)

DRC: Dial 62014 (free for Vodacom DRC subscribers)

Turkey: Dial 90555 7579254 (free for AVEA subscribers)

Global: Dial +1 313 241 7770 (regular charges apply for caller)

Search Through USSD

Kenya: Dial *883# to start your search

DRC: Dial *6213# to start your search

Search Through refunite.org

Search from your computer or a mobile phone

Ensuring data privacy with digital identity

While digital identity is a great opportunity, it raises important considerations about the privacy and security of users' identity and data. A successful digital identity initiative is likely to become pervasive over time, as it creates a record of data exposing a person's digital behaviour, which in turn is connected to a unique and traceable identity.

The challenge for governments, MNOs, entrepreneurs and NGOs is to ensure that digital identities meet appropriate standards and levels of assurance so that they prove a person's real identity and provide protection against fraud, hacking, and other cybercrime. In countries where certain groups of society are discriminated against, there is also a risk that digital identity may be used to prevent these groups from accessing mobile services controlled by the government. There have been certain cases of this in India.

Certain measures should be implemented with digital identity programmes, including (but not limited to):

Data protection

Suitable legislation

Allowing users to consent over how their data is used

Enforcing laws and regulations in appropriate ways

In addition, MNOs and technology partners should consider the potential risk to people's safety in countries where there may be surveillance and restrictions on freedom of speech.

While there have been a numerous efforts to protect users' data in developed markets, there is still a gap in the market for M4D encryption and data protection services designed for digitally underserved regions. Though still in their infancy, there are more and more services emerging to create such technology and make it more accessible to people in developing markets.

SPOTLIGHT: Security in-a-box

Security in-a-box is a collaborative project between the Tactical Technology Collective and Frontline Defenders, which provides a set of tools and guidelines for mobile security (within a broader digital security framework).

Specifically tailored for users' digital privacy needs, Security in-a-box has catered to human rights groups, LGBTI communities, and political revolutionaries in the Middle East, Africa, and India.

Funding was sourced through Hivos, Internews, Sida, The European Instrument for Democracy and Human Rights (EIDHR), Oak Foundation, Sigrid Rausing Fund, American Jewish World Service (AJWS), Open Society Foundations, and the Ford Foundation. The project's value is demonstrated by its success in garnering support from a broad range of organisations.

This service is a standout in the current M4D encryption service landscape, as it provides "tools and tactics" primarily to users in emerging markets, acknowledging the higher presence of basic phone models in most of these regions. It also provides a comprehensive comparative list of Android/ iOS-enabled services, with an individual user guide drafted for each tool.

Specific content includes:

Information on secure SIM use/mobile identification registration

Android Encryption info for LGBTI community in SSA & MENA, including:
- TextSecure (encrypted text)
- Redphone (encrypted voice calls)
- Obscuracam (blurs/deletes faces)

The criteria used to select suitable mobile products and services is listed below. A number of these features are in line with our recommendations for developing products and services:

- Trusted (audited independently or anecdotal)
- Matured (stable, active user-base community, responsive developer community)
- Open source vs. free software vs. robustness calculus
- User-friendly
- Multi-language and localisation support
- Multi-platform
- Available documentation (source, installation, usage, update)

It is an important ethical obligation to offer people digital identity services that guarantee their privacy and security. But first, it is essential to convince people—especially those who are still unregistered—that a digital identification is something they should want, need, and trust.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)207 356 0600
Fax: +44 (0)20 7356 0601
Email: m4didentity@gsma.com