Mobile Identity

A Point of View Paper from the GSMA

Executive Summary

Within the course of less than two decades, the creation, management and use of digital identity has become a critical issue. As a growing percentage of the world's population makes greater use of online and digital services, the notion of identity has become exponentially more complex and multidimensional.

At the same time, identity theft and associated fraud have become an ever-greater burden on society and businesses. Criminals are becoming more sophisticated in their methods, whereas many users, regrettably, still take unnecessary risks. Today, a typical consumer has around 26 different online user names, but only five different passwords[1]. Worldwide, it is estimated that some 148,000 computers are compromised by hackers and malicious code every day[2]. The annual cost to businesses has been estimated at over US$350 billion[3], and that figure continues to rise.

The epicentre of identity theft and fraud is online. Service providers such as online retailers, social networks and e-commerce sites have most commonly been targeted, although even large corporations and government institutions have become victims.

This situation represents a very substantial opportunity for Mobile Network Operators, for whom the provision of secure, authenticated services backed by diligent fraud prevention measures is an established part of daily business. By extension, Mobile Network Operators are extremely well positioned to take a leading role in the arena of digital identity management.

Not only does Mobile Identity represent a revenue opportunity in and of itself, but also, it represents a critical strategic opportunity to cement the position of Mobile Network Operators as the guardians of identity, and all that stems from it. In particular, Mobile Identity services can allow Mobile Operators to improve upon their current status through four key areas:

1) Leverage operator assets most notably, the SIM card
2) Manage churn
3) Generate new revenues
4) Extend reach and improve brand image

If operators can work together to define interoperable Mobile Identity standards and deploy identity management solutions and services – rapidly and globally – then not only can operators robustly defend their position in the telecoms, information and media industries, but, also, they can expand their reach and role into new and extremely valuable markets.

This short point of view paper considers the emergence of Mobile Identity services, in all their guises, and examines both the opportunity and accordant challenges that Mobile Network Operators are likely to face as they proceed.

1. Experian, 17 July 2012
2. European Commission, 4 April 2012
3. Symantec, 7 September 2011

Introduction

Mobile Identity services provide customers with the ability to verify and authenticate themselves to 3rd party service providers, remotely and securely, via their Mobile Network Operator (MNO). This opens up a range of opportunities for both Mobile Network Operators and consumer-focused 3rd party service providers to build a rich suite of services and solutions for their customers. As mobile phones increasingly become the primary medium through which a wide array of digital services are accessed by consumers and businesses, Mobile Identity services will ensure that users' personal identity information is kept safe and authentication processes are kept simple and effective.

There exists a substantial opportunity for MNOs to enhance their services to customers by leveraging their unique position in the telecommunications and information services arena. In a dynamic marketplace where the ecosystem for electronic identity is quickly evolving, operators are uniquely placed to become trusted identity "brokers." By offering their customers more direct control over the management of their identities, while giving other service providers the opportunity to enrich their offerings to consumers, operators can become central players in the management of safe transactions and secure identity verification.

Mobile Identity services unlock a new range of opportunities, including:

- Accessing personal data securely
- Secure mobile banking and financial services, including digital payments and remittances
- Authenticated signature of documents and contracts
- Digital voting
- Enhanced access to eGovernment services (such as healthcare, social security)
- Secure NFC – authenticated access to buildings and facilities
- Identity storage
- Birth/life events registration and certificates issuance

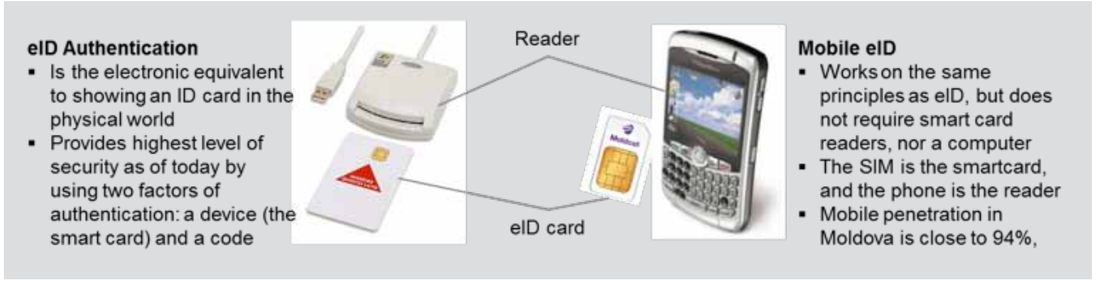
There are, of course, many other applications for Mobile Identity solutions. At the heart of the opportunity is the potential to use Mobile Identity as a means of establishing – or re-establishing – a sustainable, value-generating role for MNOs across a wide range of value chains and sectors.

What is Mobile Identity?

In the physical world, we use government or service provider-generated certificates, cards or other documents to prove our identity. Historically, verification of identity has been based on the physical presence of the individual at the point of authentication, and interaction with the person requiring the proof of ID. For example, a typical identity card or passport contains a picture of the holder, which can be compared against the person presenting that document.

In the digital world, verification of a person's identity cannot rely on the physical presence of the individual, but instead 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.

As the digital economy has become increasingly pervasive and diverse, individuals and enterprises have recognised a growing need for more sophisticated means of providing identity, and managing its integrity in a digital context. As this paper will seek to illustrate, Mobile Identity has the potential to deliver secure, adaptive and user-friendly identity management solutions across not only the digital economy, but also many "bricks and mortar" settings.



(Source: "Optimizing Mobile Signature in Moldova presentation by GSMA, June 2012)

> "Mobile Network Operators are the only ones that can solve the identity challenges that we see on the ground." (UNICEF)

Not only has mobile become the most ubiquitous telecommunications medium on the planet, but also, it has become uniquely personal. In little more than a decade, the uses of mobile have expanded exponentially, migrating away from calls and text messages towards accessing online banking, purchasing, content goods and services and even accessing government services. Mobile's ubiquity means that such uses are likely to continue growing in number and diversity. Within that context, mobile represents the ideal platform for the creation, storage and management of digital identity:

- Via mobile, there is **one single device** for authentication: VPN logins, remote logins, corporate web applications and all other log-in processes can be integrated seamlessly into one set of credentials for use in multiple websites, allowing the consumer the ease of accessing services via their mobile phones with the knowledge their personal information is secure. Mobile Identity enables people to sign documents via mobile digital signature, perform business transactions, access medical records, vote and engage in a wide array of personalised online services wherever they are, over their mobile network. In this way, the mobile device adds an extra layer of security that browser-based platforms cannot provide.
- Via mobile, **there is ease and flexibility of management**: a user can select and control applications, websites and services through their device, managing everything from loyalty card preferences, banking and bill payment processes through to social networking, through a single interface. Unlike other platforms (and, indeed, physical ID cards), even if a phone is lost, access to the user's applications remains protected: each transaction requires the user to participate in the "proof of ID" event by inputting a unique PIN number.
- Via mobile, there is **no need for any additional hardware or software**. Most SIM cards come embedded with a secure element, in which log-in processes and verification codes can be held and encrypted by the user, and stored / managed by the operator. SIM cards are also connected devices, able to receive push notifications and authentication requests without requiring any action from the user. The costs of adopting Mobile Identity services are low for both consumers and businesses, while the benefits are numerous.

The mobile medium provides a ready-made, global platform for secure identity management. And that platform is uniquely appealing to end-users because it is tangible – it has a physical manifestation, which remains with the user at all times (the SIM card and device). Mobile Identity solutions are provided by Mobile Network Operators, which are typically large, domestic businesses (not virtual, online businesses) with very substantial customer support capabilities and sophisticated anti-fraud operations. Unlike large internet players, who face lower regulation regarding consumer data protection, Mobile Network Operators are governed by robust regulatory infrastructure that places them in a strong position to provide trusted identity services.

Mobile Identity is already changing lives

Many Mobile Network Operators around the world are testing, piloting and building scalable mobile-based digital identity solutions in response to pressing social and commercial needs in the healthcare, education and financial services sectors:

- **In Turkey**, for example, one operator has launched a mobile signature application that allows employers to release pay slips, banks to approve online credit applications, courts to accept formal legal cases, customs officials to process customs declarations and many other daily processes that historically required a "wet signature" on paper.
- **In Sri Lanka**, mandatory SIM registration for all customers has allowed citizens to digitally authenticate their identity - on the spot - to authorities through a simple 2-step SMS or USSD process, allowing them to leave important documents safely at home.
- **In Brazil**, credit risk score profiles are being created for unbanked customers by analysing SMS logs and prepaid top-up activity, allowing individuals to access loans and other credit facilities that would not otherwise have been available to them.
- In **Senegal and Uganda**, mobile operators are partnering with NGOs and local government authorities to implement birth registration for newborn babies in rural areas.

> "The concept of a secure identity has become a critically important issue for citizens, governments, enterprises and any organization that determines rights and privileges for individuals."
> (Smart Card Alliance)

Creating an effective identity management ecosystem

Through a unified, secure and efficient identity management ecosystem, businesses and service providers will be able to make informed investments and tailor their services more precisely to individual preferences, including more personalised banking and financial services, enhanced access to healthcare, education and eGovernment, and safer management of online social networking. Mobile Network Operators should ultimately become guardians of identity, providing secure and authenticated access, as part of a broader ecosystem of checks and protocols.

As the benefits of Mobile Identity management solutions emerge, more and more operators are looking at ways to integrate their existing subscriber data management platforms with additional identity management capabilities, such as single sign-on and session management – both across devices and between service providers within the wider ecosystem. In this way, operators can move from simply being "network providers" to being "service and content enablers" by leveraging their key assets, including subscriber, device and application intelligence, performance intelligence, location and context awareness, and access network awareness[4].

> "If mobile identity solutions are deployed quickly and globally, and with full interoperability, there is a very real opportunity for mobile network operators to establish a key role for themselves spanning real world and virtual world authentication and payment." (Greenwich Consulting)

In order to execute an effective identity management system that puts control into the hands of the consumer while also maximising the benefits to businesses, all organisations and entities involved in the wider ecosystem of identity services must work together. A streamlined ecosystem is one in which identity providers, management service providers, consumers and other third parties all agree on the rules regarding the sharing and management of consumer identity information.

4. Ovum industry study: "Telco Opportunity: Become Trusted Identity Brokers," Ovum, published April 2012.

The importance of interoperability

When it comes to streamlining authentication procedures and digital transactions between multiple service providers, interoperability will be key to delivering efficient and accessible services to consumers and businesses. In the online world, for example, interoperability is limited and, as a result, consumers face the constant inconvenience of filling out forms for each new online service. In essence, a new unique ID has to be created for each service provider, leaving the consumer with the perennial problem of creating, managing and securely storing multiple user names and passwords. Operators that are able to consolidate - or "federate" - this type of data will be able to greatly diminish the impact of this problem (though it will likely always exist to some extent). In an ideal world, a single ID, managed by the user and authenticated each time it is used, would allow for not only a secure "auto-fill" process to populate service providers' forms, but also, a single resultant digital ID that can be accessed and managed – with authentication – via mobile. A major challenge for Mobile Network Operators will be the extent to which they can persuade or incentivise service providers to use such a solution.

A number of initiatives have been established to help foster the creation of effective digital identity management regulation and to support the growing interest in Mobile Identity services around the world. Organisations such as the Kantara Initiative and Open Identity Exchange bring parties together to develop identity assurance frameworks that ensure the availability of both high-and low-assurance models in clearly defined and easily accessible terms. They also work to ensure that sufficient and well-functioning Trust Frameworks are in place to allow service providers to trust the credentials issued by entities such as financial institutions and local government authorities. In some countries, like Finland, Estonia and Moldova, for example, the government has been a significant player in establishing the grounds for interoperability, providing a key determinant in the success of these services in those countries.

With their strong track record and long-standing industry experience in defining global interoperability standards, Mobile Network Operators are amongst the most prepared organisations to define interoperable standards for strong authentication and identity management solutions. Particularly as proposals for digital signature and e-ID legislation emerge in Europe and elsewhere, Mobile Network Operators should be in a strong position to work in unison to create solutions that simultaneously respect the legislative context and reflect the needs of customers (both enterprise and consumer).

The opportunity for operators

The broader ecosystem for digital and electronic identity is quickly evolving around the world, with significant players looking to establish their positions in the market. Web-based authentication programmes such as Google Authenticator, Facebook Connect and IBM Federated Identity Manager are gaining traction among users who want a simple, streamlined log-in process.

Some would argue that the Over-The-Top (OTT) service providers have an advantage over the mobile industry because they don't have the infrastructure or processes that "burden" the MNO. However, the GSMA Mobile Identity programme believes strongly that operators' infrastructure and processes can be a crucial differentiator in providing MNOs with the unique ability to provide secure and trusted identity services to customers, in a way that web-based service providers cannot.

There exists a substantial opportunity for MNOs to enhance their services to subscribers by enabling them to manage their identity either on their SIM or through other applications provided by their MNO.

In this way, Mobile Identity services have the potential to enable Mobile Operators to:

1. **Leverage assets** – Mobile Identity services and solutions represent an additional layer of value generation that derives from mobile networks and the SIM cards that allow consumers to employ them. In many cases, operators are already providing authentication services through single sign-on and other web-based portals – often for their own services. Such Mobile Identity services, where successfully implemented and extended to other third party service providers, are likely to allow Mobile Network Operators to continue their drive for more users and more frequent usage. Furthermore, unlike web-based and other Over-The-Top players, Mobile Network Operators can also rely on their strong customer care processes and customer billing relationship to strengthen their relationship to both the customer and to those businesses with which they partner.
2. **Manage churn** – Mobile Identity services indirectly offer a key means through which MNOs can help to reduce churn. As individual operators increasingly position themselves as custodians of secure identification and authentication, they will be able to harvest more comprehensive data about customers' preferences and usage, and, as a result, tailor services and tariffs to best meet the needs of subscribers. In this way, operators should be able to better manage churn, and, over time, reduce its corrosive impact on the bottom line.

3. **Generate new revenues** – Mobile Identity solutions have the capacity to both establish MNOs in value chains in which they presently do not participate, and re-establish MNOs in value chains from which they have been displaced. In particular, mobile authentication services will enable easier monetising of services related to direct revenue generation (such as e-commerce, m-commerce and other payment services where transaction fees can be applied), as well as those services with substantial privacy obligations (such as legal, health and e-government services). While not all Mobile Identity services may generate revenues directly, most will be connected with revenue-generating events in which operators may be able to participate, generating revenues either from the subscriber or, more likely, from the enterprise partners involved in transactions.
4. **Extend reach and improve image** – As Mobile Network Operators increasingly take on the mantle of custodians of identity on behalf of their subscribers, they should become an increasingly important part of the fabric of society – providing, in effect, social infrastructure. In turn, this should bring improvements in brand recognition and perception, as well as new commercial opportunities, new partnerships and new propositions.

There is a genuine need for improved digital identity management, both within the online world and more broadly. As a greater proportion of economic and social activities moves from real world to virtual world, the need for secure, easy-to-use and adaptive identity management services will become increasingly acute.

Mobile has already established itself as the most ubiquitous and widely available telecommunications medium in the world; the SIM card has proven extraordinarily robust as a means of authentication, service deployment and data storage and management; operators themselves have become trusted service providers. Customers increasingly recognise and respect these facts. Mobile Identity represents a logical next step in the evolution of Mobile Network Operators. Consumers are becoming increasingly aware of and sensitive to the use and management of personal data by third parties. However, research suggests that Mobile Network Operators are perceived to be amongst the most trustworthy of enterprises, and consumers would be prepared to share personal information with them, particularly in return for better services and levels of service.

The opportunity for service providers

Service providers in a broad range of sectors can benefit substantially from the added security and convenience that Mobile Identity services provide. Allowing clients to sign contracts or e-invoices remotely, for example, enables key business transactions to be processed immediately, providing greater satisfaction for customers and easier document management for businesses.

A growing number of banks and other financial service providers are recognising the opportunity that mobile-based authentication methods bring to their customers, enabling clients to manage their accounts remotely, apply for credit via digital signature and even withdraw cash from an ATM without their bank card.

Mobile Identity connects customers to businesses in ways never before possible: through secure single-sign-on, for example, customers can access a wider array of service providers with one simple log-in process, giving businesses the chance to engage new customers and facilitate the customer experience through offerings such as easy management of loyalty programmes.

Healthcare service providers around the world are opting for the ease and security that Mobile Identity services provide, such as remote storage and retrieval of medical records from a secure server and SMS or USSD-based checks for blood type or allergies in case of emergency.

Furthermore, with the additional authentication factors that Mobile Identity services offer, such as the authentication certificates generated by qualified certificate authorities, businesses and end users are protected against liability in the case of user fraud.

The opportunity for enterprise users

Mobile Identity services give companies the flexibility of allowing their employees access to confidential company files at any time, from anywhere. As a growing percentage of employees now bring their own laptops, smartphones and tablets to work, additional authentication and device management processes are now necessary to ensure that company information remains secure and the integrity of employee identity is carefully protected. Mobile Identity services are comparatively easy to integrate into existing security and IT infrastructure, as little or no additional hardware is needed. Appropriately deployed and managed, mobile can add a new layer of strong-authentication to protect both data and users.

The opportunity for governments

Governments have been some of the most enthusiastic adopters of Mobile Identity services. For those countries that already have or are in the process of deploying digital national ID cards, mobile-based ID verification platforms are often an integral component to an efficient and robust solution. The identity of the citizen can be queried via mobile and, in this way, governments can ensure that their services reach the right person directly, with great savings in time and in the cost of paper-based documentation procedures.

In many countries, mobile is fast becoming the primary medium for internet access, and this has important ramifications for those governments offering online information and service. Tax and customs declarations, pension services and transfers of social benefits, and even voting can all be conducted via mobile, bringing citizens even closer to the democratic process. This is of particular importance in developing nations, where fixed infrastructure is virtually non-existent outside of large cities, whereas mobile coverage is increasingly ubiquitous even in isolated areas. It is important to note that Mobile Identity services typically work on even the most simple of handsets – they do not require a smartphone with advanced features or specifications. As a result, Mobile Identity services can be deployed to the vast majority of the installed base of devices, although a new SIM card is sometimes required.

Opportunity for consumers

People want the freedom to connect, to log-in, to buy and sell, and to consume - from any location and at any time, without compromising the security of their personal information. They also want the flexibility to be able to access their important applications and services without having to remember an array of different passwords and PIN codes, which can be easily forgotten, or stolen by identity thieves.

Through protected "single-sign-on" services managed by their trusted Mobile Network Operator, consumers can do all of these things securely while gaining access to a wider variety of service providers via one safe login procedure.

Mobile Identity also affords consumers – as citizens – greater access to government services, enabling, for example, over-the-air access to social security payments, registration for health and education services, notification of births, deaths and marriages, and even voting for local and national elections. Secure authentication methods for mobile payments enable citizens in remote areas to receive salary or social security transfers, pay utilities and execute a whole host of other transactions without having to travel to their local municipal office or wait in line at their local service provider.

Mobile Identity management gives the user a "physical" manifestation of digital identity. The SIM card, the mobile phone and the ID application serve to make Mobile Identity more tangible and real than other digital identity management solutions. These attributes also typically lead to improved usability, efficiency and convenience. With each Mobile Network Operator having many hundreds or thousands of customer service representatives, Mobile Identity is not just a feature, but rather, it is a fully supported service – and one for which there is a genuine need amongst consumers, companies and governments.

Turkcell MobilImza

Turkey was the first country to launch a Mobile Signature solution – Turkcell's "MobilImza" service was launched in 2007. MobilImza offers a platform via which customers can undertake transactions which are equivalent, from a legal and practical perspective, to an "original" signature on a hard paper copy. In essence, the service makes it possible for customers to "sign" documents and authenticate their identity over mobile in a way that is legally compliant, binding, secure, easy and convenient.

MobilImza has been focused on addressing the needs of different segments, most particularly:

- Banking & financial institutions: secure access to account information and the ability to execute secure transactions
- Public sector, including governmental organizations and municipalities: to minimise loss of time, to reduce the number of physical documents, and to be able to serve citizens living in more remote areas
- Merchants, dealers, retailers, agents: secure identity management and authentication in support of electronic payments, transfers and queries
- Large companies: in support of internal workflows or document management

In 2009, the government started to use m-signature as part of the login process for one of its eGovernment service portals. Other public services were added in the following months. The number of available services has grown to over 60. These include, for example, secure access to medical records by doctors, secure VPN access for businesses, secure submission of tax declarations and many others.

Dialog #132#

In Sri Lanka, Dialog recently launched its #132# service, a highly successful solution that allows subscribers to append personal information to their mobile subscription, using a simple USSD code. As a result of a government-mandated initiative at the end of hostilities in 2009, a law was passed in Sri Lanka that required each citizen to be able to prove ownership of their SIM card. Dialog cleverly took advantage of this legislation to allow their customers to use the legal documentation information already collected from each customer during registration for the mobile subscription and stored in a secure server, as proof of their identity more broadly. In this way, customers had a way to link their mobile ID with their government-issued ID, all via their SIM card. As a result, citizens can now prove their identity to the authorities (such as the police, social services and others) using only their mobile.

Within the first six months of 2009, Dialog recorded 18.5 million uses of the service. Now, although the government mandate is over, Dialog still receives over half a million uses per year. Dialog is presently examining ways of incorporating additional data, such as critical health information, which could be retrieved in emergencies (blood type, allergies, medical history and so on).

GSMA Mobile Identity

GSMA Contact Details:

Alix Murphy
Programme Coordinator
Mobile Identity
GSMA
amurphy@gsm.org