Mobile Identity

GSMA Members Only

Mobile Identity Global Review 2013

Mobile networks and digital identity – the convergence of strategy and opportunity

Table of Contents

List of Figures

Foreword

The need to establish and assert identity has become increasingly important as civilisations have grown and individuals have interacted more widely. Documentary forms of identity have existed since before biblical times; the Persian King Artaxerxes issued letters to allow his subjects safe passage into lands beyond the Euphrates River. An Act of Parliament, in 1414, under the reign of King Henry V, led to the creation of "safe conduct" documents, which later became known as passports (from the French, literally meaning to pass through the gates of a walled city).

The notion of safe conduct could barely be more relevant within the context of identity in the 21st Century. Today, we use identities – in digital form – to conduct a wide range of activities in the online world, from sending emails to buying goods and services, through to managing bank accounts and accessing government services. In doing so, we expose ourselves to a growing range of risks; identity theft and associated fraud are very much crimes of the modern age.

As the number of services we access online has grown and the level of risk we expose ourselves to has increased, the need for new identity solutions has become ever more critical. Though those who suggest that "the password is dead" may be overstating the case, there is nonetheless a need for more sophisticated, secure and convenient means of creating, managing and applying digital identities.

The mobile medium represents one of the most powerful and flexible platforms for the transformation of digital identity. Ubiquitous, intelligent, and protected by the SIM card which is constantly authenticating, mobile already comprises all of the ingredients required to take the notion of identity into its next generation, from strong registration processes through to a secure element in the SIM in which keys, certificates and cyphers can be stored.

This report provides a detailed overview of the emerging opportunity for mobile operators in the realm of identity, with examples of services that are already live, and suggestions for how mobile operators can position themselves at the front line of the digital identity arena. It is our vision that by 2015, mobile should sit at the heart of identity.

I very much hope you enjoy this report, and would encourage you to contact our Mobile Identity Programme team in order to discuss the identity opportunity, and its accordant challenges, in more detail.

Anne Bouverot
Director General
GSMA

Executive Summary

Within a very short period of time, digital identity has risen to become a key strategic issue for mobile operators. As consumers, corporations and governments undertake an increasing range of activities online, the need to authenticate the identity of individuals *and* organisations has grown.

Whereas in the real world, identity can be verified through the use of physical tokens, such as ID cards, passports and other documents – supplemented by face-to-face interaction – in the digital world, the process of establishing that an individual is who he or she claims to be is materially more complex.

In the world of ecommerce, in which approaching $1 trillion of business is transacted[i], the vast majority of buyers and sellers have never met, and never will. Yet the identity assertion processes used in the online world are often remarkably weak: in most cases, the individual creates their own identity credentials – a username and password – and the service provider can do little to verify the identity of the individual to which they pertain. This can leave individuals and service providers open to identity theft and fraud.

Regrettably, individuals tend not to recognise the risks that they face online. The usernames and passwords that they choose when creating a digital identity are often startlingly weak: the most commonly used password in the English-speaking world is the word "password"[ii].

The mass media have already begun to speculate about this situation: the notion that "the password is dead" has become a regular feature of articles and editorial comment[iii]. Whereas this may be an overstatement, it is nonetheless clear that the technological means by which identity is created, managed and asserted in the digital world appears increasingly inadequate.

The mobile medium can potentially offer a very sophisticated means of addressing these challenges. Since their inception, GSM mobile networks have operated strong registration processes, through which they check the physical identity tokens of individuals and create a secure mobile identity (MSISDN and IMSI) stored in the SIM card. Operators are accustomed to authenticating every event that takes place on their networks. They have developed extremely sophisticated fraud detection and mitigation protocols. Further, mobile networks offer high-speed Internet access, and mobile devices have become akin to powerful, portable computers.

Mobile operators have at their disposal a wide and growing range of solutions that can help to bring new levels of convenience, security and privacy to online activities. From identity federation, which leverages mobile operators' strong registration processes to provide an identity for individuals that can be used to log in to a wide range of third party websites, through to second factor authentication, which could ultimately make the password redundant in many online and real-world settings, mobile operators have the opportunity to position themselves at the frontline of digital identity creation, management and authentication.

Doing so is no easy matter. Trust sits at the heart of the identity arena – and trust has to be earned. The capital expenditure involved in developing and deploying mobile identity management solutions may be marginal, but the opex involved in demonstrating to individuals that mobile identity solutions are robust and secure, and demonstrating to service providers that mobile identity adds value, will be substantial. Nonetheless, investing in mobile identity is likely to be critical. Without a role in the identity arena, operators may lack a key strategic element of the "smart pipe" model.

Indeed, if operators are unable to provide robust, integrated and standardised mobile identity solutions, they may find themselves essentially excluded from the ecommerce market (or playing a minor role).

One of the most important issues for operators is the need for commonality. In most cases, the customers of mobile identity solutions are online service providers. If those service providers are provided with a common platform that is available from the majority of operators, they will be more inclined to make use of it. If operators develop divergent solutions, based on incompatible technologies, the identity opportunity may never fully materialise. Much of the competition in this market comes from large, Internet companies who offer service providers a simple means of engaging – typically a single set of APIs (application programming interfaces)[iv] that can be used globally. Mobile operators, as a collective, will have to aspire to the same level of "ease of use" if they are to make their mark on the identity market.

Identity is already part of mobile operators' core business. And there is a strong argument to suggest that that mobile identity solutions can add considerable value and differentiation to voice, messaging and other core services, as well as online access, transactions and the myriad use cases emerging on the Internet.

Mobile operators must recognise that the identity opportunity will only be effectively exploited if mobile identity solutions are different from and better than their online equivalents. Simply transposing existing solutions onto the mobile device and SIM card is unlikely to be enough.

Mobile operators must take an innovative, creative approach to identity, recognising that existing solutions fall short of end-users expectations and the authentication needs of many service providers.

With this in mind, operators should consider mobile identity within the broadest possible context. Primarily, this means thinking about the notion of identity in its entirety, and examining the strategic and commercial possibilities from that level, before even considering mobile's role therein. The phrase "mobile identity" itself tends to promote a limited view of the opportunity and its attendant challenges: a more holistic strategic outlook will likely yield more effective and value-generating solutions.

Identity needs mobile: mobile is increasingly ubiquitous, portable, personal and secure. The mobile medium is based on a SIM card, the capabilities of which serve to position mobile operators at the apex of identity management, authentication and service provision. Not only is the mobile device nearly always with the individual who owns it, but also, the SIM card in that device provides an authentication process that is amongst the most secure available. It is a logical step to use that authentication ability across a broader range of use cases.

Service providers need mobile solutions: Mobile identity management services are of little or no value unless service providers – third party website operators initially – actively want to deploy them within the context of their sites, services and content. What mobile operators can offer service providers is considerable. At the most fundamental level, mobile identity management services can not only provide a secure alternative to the issue of multiple user names and passwords, but also, the mechanics of some mobile identity solutions – such as mobile digital signature and second factor authentication – are likely to have a materially positive impact on levels of security.

Additionally, mobile solutions should be able to deliver enhanced functionality to third parties, particularly as operators adopt federated architectures that allow service providers to make use of key network services and data (including messaging, location data and, of course, identity).

There are, of course, many challenges. Above and beyond the issues of establishing platform commonality and service interoperability, mobile operators will need to provide an extremely compelling business case in support of mobile identity solutions if they are to persuade literally millions of service providers to adopt. Further to this, they will have to ensure full compliance with legislation pertaining to privacy, data protection and security, as well as newer laws and regulations pertaining specifically to digital and mobile identity, signatures and certificates. In addition, they will have to ensure a common user experience not only across the broad range of mobile devices and operating systems, but also, ultimately, across all other connected devices, from PCs through to television sets and set-top boxes.

Because of the inherent complexity of identity as a topic, it is perhaps helpful for operators to think of mobile identity as being rather like presence: an individual's mobile identity not only comprises credentials and permissions, but also preferences and profile settings; therefore, mobile identity not only underpins authentication, access and secure payment (amongst other things), but also instructs service providers on how best to address the individual.

Arguably the most critical notion of all is control. Identity is uniquely personal, and individuals (consumers, enterprise users) are becoming increasingly sensitive to how their identity is manifest and used online. Some Internet companies have faced considerable ire from customers whose identities – or data deriving therefrom – have been shared without the explicit permission of the owner. Whatever identity solutions mobile operators develop and deploy, they should be founded on the notion that the individual – the customer – must be afforded complete control, and that by default, the absolute minimum information is shared.

This document is designed to achieve two objectives: to set out the challenge, and to offer some initial thoughts on how solutions should be developed. It forms part of a broader series of documents published by the GSMA Mobile Identity Programme team, which include white papers on technical and regulatory issues, case studies detailing the experiences of operators that have already launched mobile identity services, and blueprints relating to commercial and business modelling issues. Contact details for the GSMA Mobile Identity Programme team are provided at the end of this report; mobile operators who are interested in developing mobile identity solutions are invited to contact us and join our working group. For more information, please go to www.gsma.com/mobileidentity.

What is Identity?

Identity has, in a very short period of time, become one of the most talked-about themes in the telecommunications industry. A growing number of corporations see the management of identity, in all of its forms, as a key strategic issue and an increasingly fundamental component of their operations in today's digital age. Mobile operators are central amongst them[v].

In spite of the growing importance of identity as a strategic theme, what we mean by identity – the characteristics and distinguishing features that describe an individual, and differentiate that individual from others – *hasn't* changed. Identity has and will always be about demonstrating that an individual is who he or she claims to be. That process of validation or authentication, in turn, allows the individual to access places, services, content, groups and activities.

What *has* changed, however, is the "distance" between the individual and the validator. In the past, validation was a simple face-to-face activity. The individual would present a token or credential (such as a passport) to a representative of the validating entity (an immigration official for example) and that representative would decide whether or not to grant access. The representative would be trained to distinguish between genuine and counterfeit identity tokens, and how to assess whether the individual presenting the token was the same individual represented by that token, and would make a decision based on that training.

The Rise of Technology, and the Multiplication of Identity

But the inexorable rise of technology has fundamentally changed the dynamics of such processes. In fact, that change began many decades ago. The capacity to make a simple, fixed-line phone call to an entity – rather than appearing in person – meant that the identity verification process had to be re-designed in order to work in the absence of physical tokens and the human being to which they pertained. A new type of registration process had to be created – one that bound copies of tokens (passports, utility bills and so on) with data; information that only the individual could know, and which was otherwise kept secret from the outside world.

> "Identity is a central component of KDDI's existing operations, through our au ID proposition, and our future strategy."
>
> Takashi Tanaka
> President
> KDDI Corporation

With the rise of the Internet and other digital technologies (including mobile networks and devices), the multiplication of identity has accelerated. Our real-world, physical identity has been supplemented; we now have multiple user names and passwords; we have bank and credit cards imbued with our identity; we carry smart cards to access buildings and health records. And with each additional manifestation, our identity – real world and digital – has become more complex.

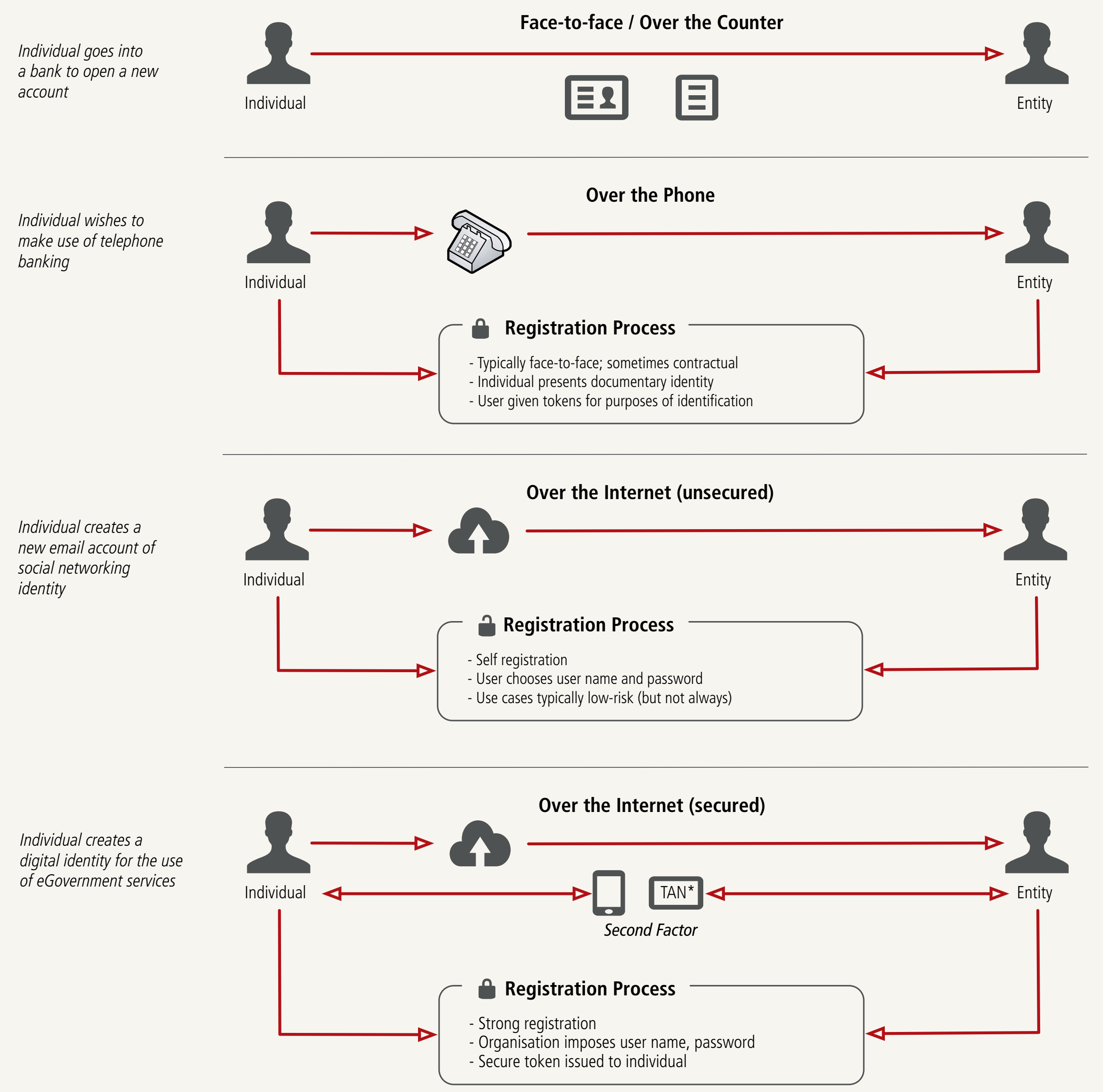
Core Identity and the Individual

At a fundamental level, an individual's identity is still derivative of basic biometric and physiological data; sex, date of birth / age, height, eye colour, fingerprints and, at a more fundamental level, genome.

However, at present, affordable consumer technology does not allow such biometric data to be accurately scanned and verified. Arguably, it won't be long before digital devices – particularly mobile phones – will be capable of accurately scanning irises or reading some other biometric attribute that will confirm, with a very high degree of certainty, the identity of the individual using that device. But between now and then, proxies will have to be used.

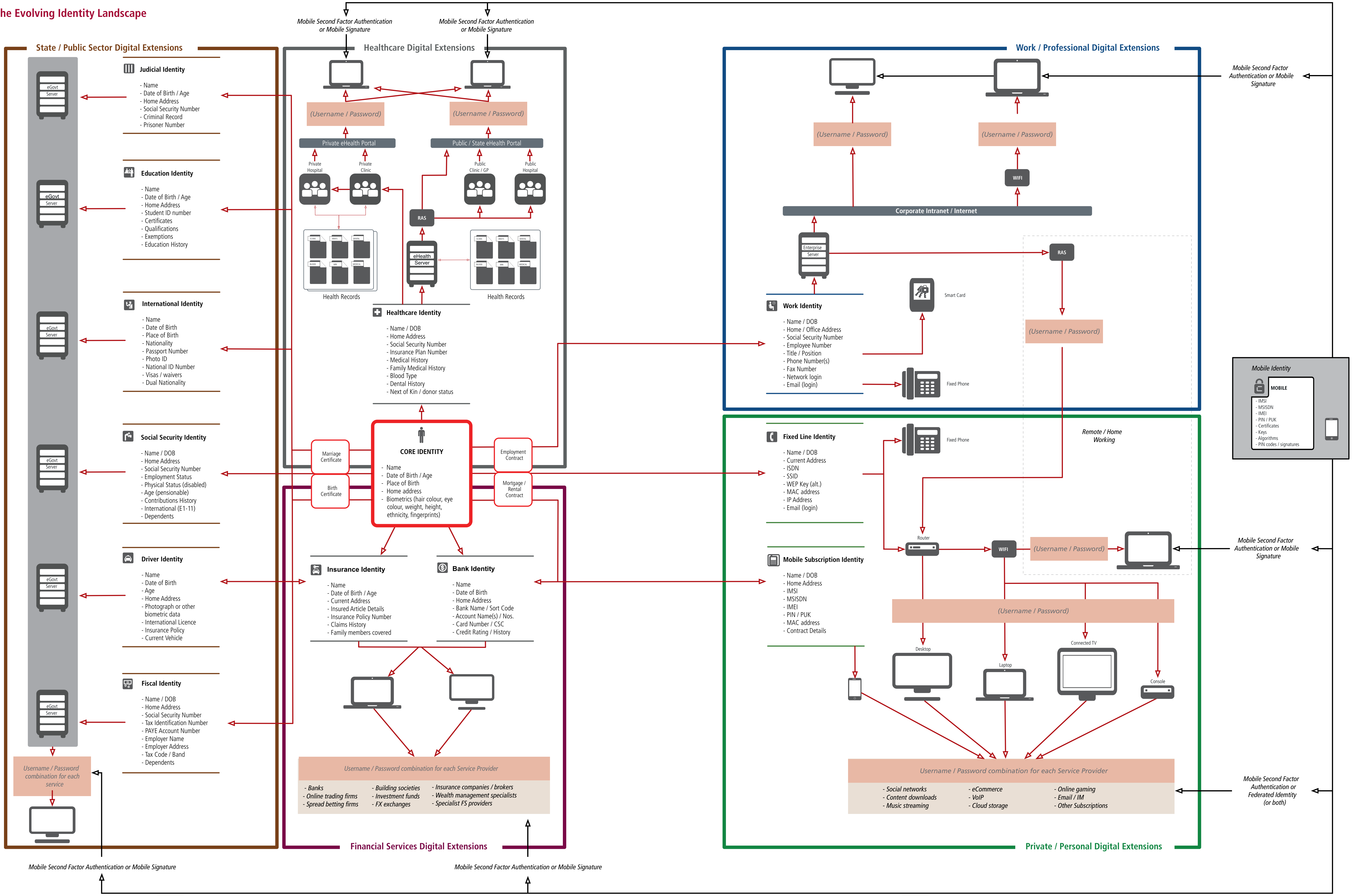
Those proxies range from smart cards to username and password combinations, mobile phone applications to PIN codes. In most cases, we have a different or derivative version of our identity for each separate application; our banking identity is not, for example, the same as our email identity, and so on.

Figure 1: Evolution of the Registration Process


Face-to-face / Over the Counter
Individual goes into a bank to open a new account
Individual
Entity
Over the Phone
Individual wishes to make use of telephone banking
Individual
Entity
Registration Process
- Typically face-to-face; sometimes contractual
- Individual presents documentary identity
- User given tokens for purposes of identification
Over the Internet (unsecured)
Individual creates a new email account of social networking identity
Individual
Entity
Registration Process
- Self registration
- User chooses user name and password
- Use cases typically low-risk (but not always)
Over the Internet (secured)
Individual creates a digital identity for the use of eGovernment services
Individual
TAN*
Second Factor
Entity
Registration Process
- Strong registration
- Organisation imposes user name, password
- Secure token issued to individual

*TAN stands for Transaction Authentication Number

Figure 2: The Evolving Identity Landscape



State / Public Sector Digital Extensions

eGovt Server

Judicial Identity
- Name
- Date of Birth / Age
- Home Address
- Social Security Number
- Criminal Record
- Prisoner Number

Education Identity
- Name
- Date of Birth / Age
- Home Address
- Student ID number
- Certificates
- Qualifications
- Exemptions
- Education History

International Identity
- Name
- Date of Birth
- Place of Birth
- Nationality
- Passport Number
- Photo ID
- National ID Number
- Visas / waivers
- Dual Nationality

Social Security Identity
- Name / DOB
- Home Address
- Social Security Number
- Employment Status
- Physical Status (disabled)
- Age (pensionable)
- Contributions History
- International (E1-11)
- Dependents

Driver Identity
- Name
- Date of Birth
- Age
- Home Address
- Photograph or other biometric data
- International Licence
- Insurance Policy
- Current Vehicle

Fiscal Identity
- Name / DOB
- Home Address
- Social Security Number
- Tax Identification Number
- PAYE Account Number
- Employer Name
- Employer Address
- Tax Code / Band
- Dependents

Username / Password combination for each service

Mobile Second Factor Authentication or Mobile Signature

Healthcare Digital Extensions

Mobile Second Factor Authentication or Mobile Signature

Mobile Second Factor Authentication or Mobile Signature

(Username / Password)

(Username / Password)

Private eHealth Portal

Public / State eHealth Portal

Private Hospital

Private Clinic

Public Clinic / GP

Public Hospital

RAS

SCANS XRAYS DENTAL BLOOD MRI MEDICAL

Health Records

eHealth Server

SCANS XRAYS DENTAL BLOOD MRI MEDICAL

Health Records

Healthcare Identity
- Name / DOB
- Home Address
- Social Security Number
- Insurance Plan Number
- Medical History
- Family Medical History
- Blood Type
- Dental History
- Next of Kin / donor status

Marriage Certificate

Birth Certificate

CORE IDENTITY
- Name
- Date of Birth / Age
- Place of Birth
- Home address
- Biometrics (hair colour, eye colour, weight, height, ethnicity, fingerprints)

Employment Contract

Mortgage / Rental Contract

Insurance Identity
- Name
- Date of Birth / Age
- Current Address
- Insured Article Details
- Insurance Policy Number
- Claims History
- Family members covered

Bank Identity
- Name
- Date of Birth
- Home Address
- Bank Name / Sort Code
- Account Name(s) / Nos.
- Card Number / CSC
- Credit Rating / History

Username / Password combination for each Service Provider

- Banks
- Online trading firms
- Spread betting firms

- Building societies
- Investment funds
- FX exchanges

- Insurance companies / brokers
- Wealth management specialists
- Specialist FS providers

Financial Services Digital Extensions

Mobile Second Factor Authentication or Mobile Signature

Work / Professional Digital Extensions

Mobile Second Factor Authentication or Mobile Signature

(Username / Password)

(Username / Password)

WIFI

Corporate Intranet / Internet

Enterprise Server

RAS

Smart Card

(Username / Password)

Work Identity
- Name / DOB
- Home / Office Address
- Social Security Number
- Employee Number
- Title / Position
- Phone Number(s)
- Fax Number
- Network login
- Email (login)

Fixed Phone

Mobile Identity

MOBILE
- IMSI
- MSISDN
- IMEI
- PIN / PUK
- Certificates
- Keys
- Algorithms
- PIN codes / signatures

Remote / Home Working

Fixed Line Identity
- Name / DOB
- Current Address
- ISDN
- SSID
- WEP Key (alt.)
- MAC address
- IP Address
- Email (login)

Fixed Phone

Router

WIFI

(Username / Password)

Mobile Second Factor Authentication or Mobile Signature

Mobile Subscription Identity
- Name / DOB
- Home Address
- IMSI
- MSISDN
- IMEI
- PIN / PUK
- MAC address
- Contract Details

(Username / Password)

Desktop

Laptop

Connected TV

Console

Username / Password combination for each Service Provider

- Social networks
- Content downloads
- Music streaming

- eCommerce
- VoIP
- Cloud storage

- Online gaming
- Email / IM
- Other Subscriptions

Mobile Second Factor Authentication or Federated Idemtity (or both)

Private / Personal Digital Extensions

Mobile Second Factor Authentication or Mobile Signature

Mobile Second Factor Authentication or Mobile Signature

What is Digital Identity?

At a simple level, therefore, digital identity is a proxy for or supplement to the real (core) identity of an individual (See Figure 2). A digital identity can be defined as the "digital representation of a set of claims made by one party about itself or another data subject"[vi]. In other words, a digital identity is a set of attributes or credentials that allows a third party to assess and verify the authenticity of the identity in question, and the claims being made by it (such as whether or not that identity is allowed to enter a certain website).

Digital identities can range in form; from the cursory – containing, for example, only a single attribute or credential (such as the age of the individual to which it pertains) to the complex – containing comprehensive details of an individual's domicile, bank accounts and so on.

A key difference between physical (real-world) identities and digital identities is volume. Whereas an individual would typically have only three or four key, physical identity documents (an ID card, a driving licence, a social security card and a passport, for example), individuals tend to have a large and growing number of digital identity manifestations (multiple email accounts, multiple social networking logins, online banking logins, online content storage logins and so on). As a function of time, the number of digital identity manifestations that individuals create and use is growing.

Human Nature and Digital Identity

Regrettably, we are often very ill disciplined when it comes to making these derivative identities secure. We choose user names that are our proper name; we choose passwords that are short and easy to remember; we use the same PIN number for multiple devices, services and providers. And by implication, we make it easier for our identities – or parts thereof – to be stolen.

A typical online consumer has 26 different logins – but just five different passwords.[vii]

The human condition sits at the heart of this problem. We are generally not good at remembering 'randomised' user names, passwords and PINs. So we default to what we know. And what we know is easy for criminals to predict or guess.

The word "password" is the most commonly used password in the English-speaking, digital world[viii]*. "123456" is the second most commonly used*[ix,x]*.*

As illustrated in Figure 3, there is a fundamental lack of imagination and sensitivity to security in individuals' common password choices.

Figure 3: Most Commonly Used Passwords

Rank	Password
1	password
2	123456
3	12345678
4	abc123
5	qwerty
6	monkey
7	letmein
8	dragon
9	111111
10	baseball
11	iloveyou
12	trustno1
13	1234567
14	sunshine
15	master
16	123123
17	welcome
18	shadow
19	ashley
20	football

Source: Born to be Breached: the worst passwords are still the most common, Ars Technica, 3 November 2012

Convenience versus Security

It may seem like an obvious point, but the reason individuals need an ever-growing number of logins and PINs is because the selection of entities that we need to verify our identity to has grown massively since the advent of the Internet. Whereas 50 years ago, we purchased goods from a small handful of local (bricks and mortar) shops, and purchased services from organisations and individuals in our locale, today we purchase increasingly indiscriminately from suppliers around the globe, over the Internet. The business-to-consumer segment of the online economy is expected to be worth in excess of $1 trillion in 2013 (and was already worth in excess of half a trillion dollars in 2011)[xi]. Yet for the vast majority of ecommerce transactions, the purchaser (the individual) and the seller never meet.

Identity is therefore an issue not only for the individual, but also for the entities to which that individual (and millions of others) connects and transacts. Companies want to know about individuals, partly to ensure that the risk of fraud is minimised, and partly because they want to sell more goods or services. Conversely, individuals want to be assured that a seller is legitimate and reliable, and not a criminal.

Registration and the Geometry of Risk

There are many different settings in which digital identity is used, and by implication, there are many different means by which individuals can register themselves, and thereby, create a digital identity. Use cases range from the relatively low-risk – such as social networking – through to the deeply personal and important – such as online banking or accessing health records via a government-owned portal. Clearly, the latter examples require a far more rigorous registration process than the former. The registration process – the means by which a digital identity is created – is central to ensuring that an identity is as robust and secure as its use-case or context requires.

Weak Registration

For applications such as consumer email, social networking and online gaming, the established convention is for individuals to self-register. The individual creates a username and password, without reference to any formal identity documents or credentials, and the service provider grants access, normally without performing any substantive checks on the authenticity of the individual's identity (because the service provider effectively has nothing to check, and other than requiring the user to indicate compliance with terms and conditions by clicking a tick box, has to assume that the individual has acted in good faith and has provided honest, accurate information – relating to a real, legal person).

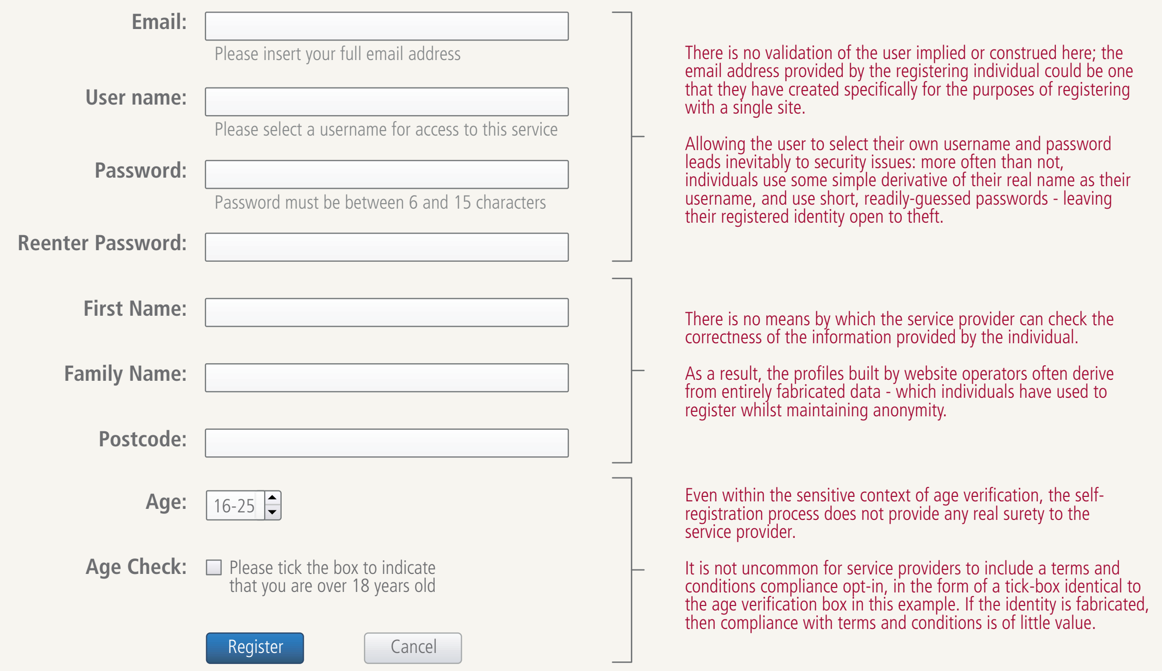
Even simple use cases can present risk to the individual. People share sensitive, personal information via email and social networking – details of bank accounts, the location of valuables and other information is occasionally shared by mail. Indeed, individuals' willingness to share information via social networking sites is of considerable concern. The password recovery processes employed by many email, e-commerce and similar sites typically involve the individual answering a series of questions (name of first pet, name of high school, and others).

These questions, and their corresponding answers, are self-selected by the user. Yet the answers to such questions are readily available from social networking sites, either directly from the individual or via their peers. As a result, a criminal may never need to know an individual's password – they just need to research the answers to typical password reset questions on the individual's social network posts.

Self-registration similarly poses risks for the validating entity; the corporation. Many Internet companies have found themselves exposed to malware, worms and viruses, which are spread through their networks via accounts (identities) set up by criminals. Facebook estimates that 1.5 percent of its monthly active users are "undesirable accounts," which are false accounts are created for spamming or other more malicious purposes[xii].

There is nothing inherently wrong with self-registration; indeed, it is critically important to companies whose business model depends on the assimilation of very large customer bases (with, by implication, the lowest possible barriers to entry). However, it has inherent weaknesses; it can readily be abused by criminals (and even malevolent employees), and can easily be misused by individuals who do not take sufficient care of managing their digital identities.

Figure 4: Online, Self-Registration Example



Email: Please insert your full email address

User name: Please select a username for access to this service

Password: Password must be between 6 and 15 characters

Reenter Password:

First Name:

Family Name:

Postcode:

Age: 16-25

Age Check: □ Please tick the box to indicate that you are over 18 years old

There is no validation of the user implied or construed here; the email address provided by the registering individual could be one that they have created specifically for the purposes of registering with a single site.

Allowing the user to select their own username and password leads inevitably to security issues: more often than not, individuals use some simple derivative of their real name as their username, and use short, readily-guessed passwords - leaving their registered identity open to theft.

There is no means by which the service provider can check the correctness of the information provided by the individual.

As a result, the profiles built by website operators often derive from entirely fabricated data - which individuals have used to register whilst maintaining anonymity.

Even within the sensitive context of age verification, the self-registration process does not provide any real surety to the service provider.

It is not uncommon for service providers to include a terms and conditions compliance opt-in, in the form of a tick-box identical to the age verification box in this example. If the identity is fabricated, then compliance with terms and conditions is of little value.

Strong Registration

At the opposite end of the registration continuum, financial services companies, governments and large corporations – because of the higher-risk nature of their online interactions – have tended to create strong registration processes that give them a higher level of assurance that a digital/online user is who he or she claims to be.

To create a digital identity that pertains to a bank account, for example, it is not uncommon for the individual to have to visit a bank branch in person, and present physical identity documents, and sign a paper contract (the precise methodologies vary by bank and by geographic region).

Commonly, the bank will issue the username and password, and these will typically have a high degree of entropy (they will contain randomised alpha-numeric strings that are much more difficult for a criminal to guess or otherwise crack). Figure 5 explains password entropy, and its implications for online security, in more detail.

Further, the registration process will include the creation of additional "factors" of authentication: that is to say that the bank may issue an additional identifier or token – a customer number, a security token (often a key fob which generates synchronised numeric keys) or a piece of software on the individual's computer or mobile phone.

Doing so adds a "layer" to the process of identity verification. The individual inputs a username and password, and is then prompted to provide the additional factor.

The additional factor may be "transacted" via a different medium. For example, the username and password may be submitted on a personal computer, whereas the additional factor may be input via a mobile phone. Under such circumstances, a criminal would need not only the username and password of the individual, but also their mobile telephone and any PIN number or code associated with it.

> "Orange is dedicated to working with other mobile operators to deliver an industry-wide, interoperable and standardised solution giving customers and service providers a common, secure mobile identity framework, as demonstrated by the recent launch of Mobile Signature in Moldova."
>
> Jean-Paul Cottet,
> Senior Executive Vice-President –
> Marketing, Innovation and New Activities,
> Orange Group

Figure 5: Password Entropy & Digital Security

Low Entropy Password

p a s s w o r d

L = 8
N = 26
H = 37 bits of entropy

Each letter has a 1/26 probability of being selected; there are 26 letters in the English alphabet (lower case only).

The degree of entropy, and hence the difficulty involved in guessing a password depends on its length, and the number of options available for each character.

The formula for calculating the degree of entropy (H) is as follows:

$H = L \log^{2} N$

where L is the length of the password and N is the size of the alphabet from which the word password derives.

Higher Entropy Password

P 4 s 5 w 0 r d

L = 8
N = 95
H= 52 bits of entropy

The entropy of this variant of the password is higher because the user has substituted numbers for some of the letters in the word "password".

As a consequence of this, and the use of both upper and lower case letters, the exponent is higher: in the example above it was 26; in this example it is 95 (because the number of options per character is the full printable ASCII set).

High Entropy Password

M y c 4 t h a $ n 0 n 0 s €

L = 14
N = 95
H= 91 bits of entropy

In this example, the user has chosen a longer password (based on an easily remembered phrase, which is also difficult to guess). Drawing on 95 characters from the ASCII set, and including 14 characters, this password has a high level of entropy. As illustrated in the table below, the longer the password and its constituent character set, the longer it would take a computer to guess it.

Time to Break a Password (assuming 10,000 guesses per second)

Password Length (L)	Lowercase Only (N = 26)	Uppercase, Lowercase & Numbers (N = 62)	ASCII Printable (N = 95)
5	19 minutes	1 day	8 days
6	8 hours	65 days	2 years
7	9 days	11 years	200 years
8	241 days	692 years	19,000 years
9	17 years	42,000 years	1.8 million years

Registration can be a costly exercise; which is why strong registration procedures, which tend to infer the highest cost, are typically only used in settings with either high attendant security risk or in which high value transactions are conducted, or both.

Figure 6: Strong Registration Example – Mobile Identity Subscription

1	User goes into operator store
2	User presents formal identity tokens (ID card, passport, utility bill, bank statement)
3	User agrees new mobile contract, which includes provision of mobile indentity service
4	User is given new SIM card (operator activates new card)
5	User chooses PIN code that protects public/private keys in SIM card
6	Mobile identity source activated

Conversely, the reason why many online companies have opted for self-registration is because they do not, generally speaking, have a physical (retail, office) footprint through which they can conduct strong registration; that is to say that they don't have access to facilities and people through which individuals (customers) can undertake registration.

Self-registration is problematic because of individuals' carelessness in the choice and use of usernames and passwords. As a function of time, it has also become problematic because individuals have begun to face login or password "fatigue": as the number of sites and services that they visit online grows, they struggle to remember all of their usernames and passwords[xiii]. This has negative implications for the individual's user experience, and also for service providers themselves (if consumers are unable or unwilling to login often).

Addressing these issues is of growing importance. As in the real world, the digital economy relies on trust – the ability to gain assurance that a counter-party is legitimate. Since trust is not implicit, mechanisms have to be put in place to compensate. This situation, in many respects, sits at the heart of the identity opportunity for mobile operators.

In the majority of cases, mobile operators already undertake a strong registration process; this has always been the case for contract customers, and is increasingly the case for prepaid customers (especially in those markets where some form of subsidy is available on prepaid devices).

Moreover, the mobile medium employs a SIM card, which is a sophisticated device that is capable of holding important information in a secure, encrypted environment and is already used for real-time authentication; and a mobile device that is personal (pertains, generally to a single individual), connected (for voice and data) and intelligent (sensitive to its location; capable of being disabled and locked). Given this, mobile represents a potentially ideal medium for the provision of identity management services.

European Union: new identity legislation pending

In June 2012, the European Commission proposed new rules on a Pan-European Regulatory Framework on the cross-border recognition and interoperability of electronic Identification, Authentication and Signature (eIAS). The primary objective of the proposed regulation is to boost trust and convenience for cross-border electronic transactions by ensuring:

- Citizens and businesses can use their national electronic identities to access public services in other EU countries where electronic identities are available;
- e-Signatures and related online trust services (including electronic seals, time stamps and web authentication) have the same legal value as in traditional paper based processes.

The draft regulation is designed to address a number of legal and technical barriers currently hindering the development of a single digital market in the EU, which relate to a lack of interoperability, legal certainty and market fragmentation (particularly, divergent national implementations on electronic identity and eSignature). The new framework will allow end-users to "sign" with a mobile phone in a technology-neutral setting, but will also require more stringent regulations for service providers, such as higher levels of accountability for security issues, clear and more stringent rules for the national supervision of eSignature and related trust services, and reinforced data protection and an obligation for data minimisation.

Adoption of the draft regulation is by co-decision of the European Parliament and the (Member States) Council, and is currently expected by June 2013.

Something I have; something I know; something I am

Something I have	In recent times, "something I have" has most commonly related to a card or document, such as a credit or debit card, a membership card or an ID card. However, it has become increasingly obvious that the SIM card, resident in a mobile phone, is potentially a more secure basis for performing the "something I have" function – not least because it is already encrypted, and connected to a network that is constantly monitoring for potentially fraudulent use. The SIM card and phone are constant companions to users – unlike, for example, a passport – and have already established themselves as critical elements of most individuals' private world.
Something I know	In its early manifestations, "something I know" was a password or similar secret alphanumeric string that only the individual and the validating entity knew. As a function of the evolution of technology, additional data have been added: customer numbers, PIN codes, passwords and others. Individuals are already accustomed to using such data on mobile devices. More importantly, because of the connected nature of the mobile phone / SIM, it is technically straightforward to add further layers of challenge and response to supplement "something I know".
Something I am	Historically, "something I am" was a matter of face-to-face contact; humans are generally very good at recognising faces and other physical characteristics. Even in circumstances where two individuals have never previously met, we are typically capable of making an informed value judgement about the authenticity and appropriateness of third parties. It is already possible to verify the authenticity of the individual through behavioural profiling, input characteristics (how the individual types an input) and similar.

To verify that an individual is who he or she claims to be in a high-assurance setting, the verifying entity needs to challenge the individual on the basis of at least two items – something the individual has (a physical token or document); something the individual knows (a password or PIN); and ultimately, something the individual "is" (biometric attributes). In the absence of low-cost technical solutions that allow for accurate and low-cost biometric scanning, the former two elements have tended to take the fore.

In summary, not only are the mobile network, SIM card and mobile device capable of accommodating these three variables, but they are also capable of adding more subtle and sophisticated "factors" of validation / authentication. The mobile medium, therefore, strongly lends itself to becoming a key tool in the establishment, management and application of digital identity.

KYC – Know Your Customer

In order to become a mobile subscriber, the individual typically needs to participate in a "strong" registration process during which they normally (though not universally) have to present documentary proof of their identity; such proof typically includes presentation of a passport or similar ID card, a contemporary utility bill (as proof of current address) and a bank statement (amongst other things).

As such, mobile operators often have a relatively high level of assurance that any given individual is who he or she claims to be. This is not always the case, for example, in the online world, particularly within the realm of social networking[xiv]. This assurance is profoundly important. Mobile operators' businesses are based, at a fundamental level, on having a high level of assurance that each individual is legitimate. Without such assurance, operators would be exposed to a disproportionate risk of fraud and associated bad debts.

Viewed from the perspective of the identity opportunity, a high level of assurance is a considerable asset. It infers, at least in principle, that mobile operators could assert the authenticity of an individual's identity to third parties; that is to say, an individual could use their mobile identity to login to third party websites, and those websites should be willing to accept that the person logging is legitimate because of the inherent strength of the mobile registration process.

The Importance of Trust

But achieving this requires the building of trust, on a very substantial scale. There is no particular reason why a service provider should trust a mobile operator to assert the authenticity of an individual identity (nor indeed is there a specific reason why the individual should trust the operator to act in this manner on their behalf). Trust has to be earned. This, of course, is nothing new. It has taken a considerable amount of time for individuals and third parties to trust the identity solutions we commonly make use of today.

Within a contemporary setting, the establishment of trust has tended to relate to the credibility of the institutions involved and the robustness of the solutions being used. We trust banks, online retailers and others because over time they have demonstrated – for the most part – that they are worthy of that trust; and in addition, they have deployed systems that help them to earn and maintain trust, by ensuring that the information they hold relating to individuals' identities is stored securely and used responsibly.

The notion of trust is especially acute within the context of identity. To any given individual, their identity is both personal and extremely important. A compromised identity leaves the individual unable to access many of the products and services that define daily life – from withdrawing cash from a bank to logging into a personal email account. Therefore, for any organisation to take a meaningful role in the management of individuals' identities, it must demonstrate that it can be trusted to perform such a sensitive function.

There are numerous examples of corporations failing to recognise the sensitivity of individuals' identity and associated data. Some social networks have taken a cavalier attitude towards the use of individuals' personal data;[xv] service providers have allowed weak security to result in the theft of literally millions of individuals' identity data; even governments have allowed sensitive identity attributes to fall into criminal hands or those of the media.

United Arab Emirates: Etisalat making ID cards mobile

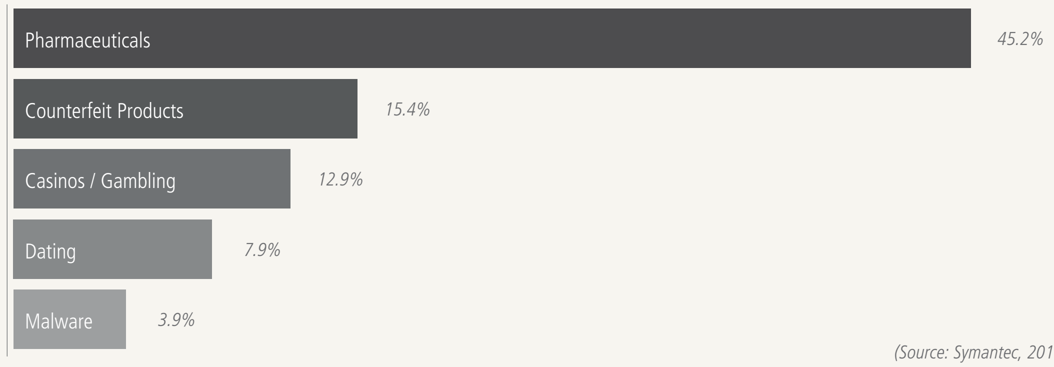
Following the successful execution of its "My Number, My Identity" program, Etisalat, the leading mobile operator in the United Arab Emirates, is working with the National Identity Authority to place the credentials of the Emirates National ID Card onto NFC-enabled phones and SIM cards. The National ID Card – held by all residents and every Emirati citizen - currently contains a secure chip that enables PKI signatures for activities which require strong customer authentication. Placing the National ID credentials on the SIM card of a mobile phone provides an additional level of security and convenience, and is seen as key to enabling a broad range of strategic business verticals.

Use cases for sophisticated, trusted and verifiable identity include consumer identity validation at border crossings, merchant recruitment for Etisalat's m-commerce service "Flous", medical practitioner validation for Etisalat's mHealth program "Mobile baby" and utility payments across emerging markets. All from the simple touch of their NFC phone.

Online Threats

Spam

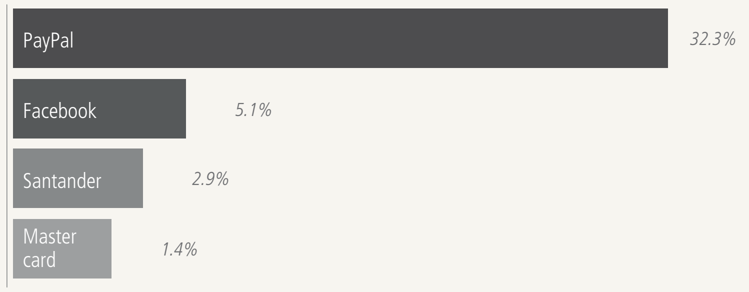
In 2012, it is estimated that spam messages represented over **85% of global email volume** That is equivalent to on average over **80 billion spam email messages per day**. The subject matter of those messages was dominated by fake pharmaceutical offers and counterfeit products.



(Source: Symantec, 2012)

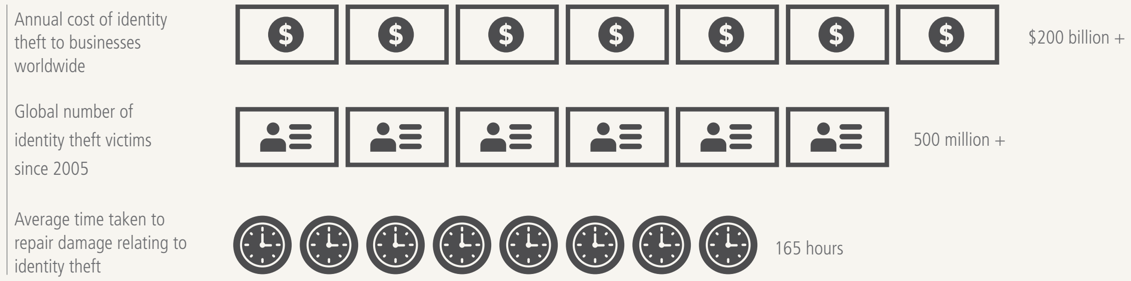
Phishing

Phishing and scams account for less than 3% of spam, but whereas spam is typically little more than a nuisance, phishing attacks can lead to material financial loss for consumers and businesses. Paypal and its users are the most commonly targeted.



(Source: Symantec, 2012)

Identity Theft



(Source: New Fraud Frontier, March 2012)

The Digital Identity Paradox

Most human beings are not (yet) able to understand or quantify digital identity risks. That is to say, we engage in the creation, use and management of digital identities without fully understanding the attendant risks associated with doing so.

We buy and sell online; we manage our money; we consume content; we communicate; we share; and yet, a typical individual has little understanding of how hackers, fraudsters and other elements of the criminal fraternity might intervene.

We would never leave our home without locking the door, yet we often save our online banking username and password on our computers – essentially equivalent to leaving a key in the front door. We would never put a sign on our home saying "we're away on holiday" yet we happily post such information on social networking sites for all to see. A somewhat mischievous website, which nonetheless helps raise awareness of this important issue, has recently been created, and is illustrated here.

Source: www.pleaserobme.com

The paradox, of course, is that individuals express concern about identity theft, yet do too little to protect themselves against it.

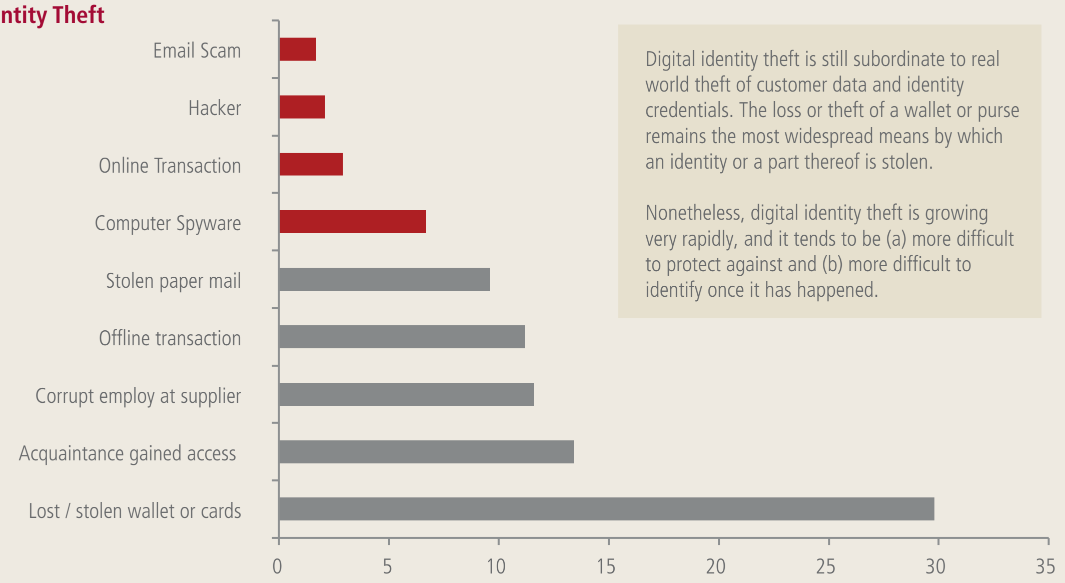
The Rise of Identity Theft

Addressing this situation is of growing importance. Identity theft has become a critical issue for individuals, corporations and governments, the cost of which – in financial, emotional and practical terms – is rising year on year. Estimates vary, but it is clear that the cost of identity theft to businesses and individuals already runs into many billions of dollars. And it is important to note that forms of identity theft are becoming more diverse and ingenious.

For example, a recent study in the United States has suggested that medical identity theft affects over 1.8 million individuals each year, with an annual cost to the healthcare industry of over $40 billion[xvii]. The cost to individuals can be similarly high; many individuals whose identities are stolen and used fraudulently are dropped by their insurance companies, and end up having to pay for the services that have been consumed by fraudsters.

Similarly, in many countries in the world, social security fraud has become increasingly widespread, with criminals claiming unemployment, housing and other benefits using the identities of legitimate (and deceased) citizens[xviii]. Not only does this type of identity theft imply financial cost for the state, but it can lead to substantial financial and emotional costs for victims.

Figure 7: Bases of Identity Theft



Digital identity theft is still subordinate to real world theft of customer data and identity credentials. The loss or theft of a wallet or purse remains the most widespread means by which an identity or a part thereof is stolen.

Nonetheless, digital identity theft is growing very rapidly, and it tends to be (a) more difficult to protect against and (b) more difficult to identify once it has happened.

Source: Javelin Strategy & Research, 2012

The Identity Challenge

Digital identity has become an issue of great importance partly because of the rising tide of online criminal activity; partly because of the increasing breadth, depth and diversity of individuals' online lives; and partly because as a result of this diversity, convenience – in terms of the user experience – is steadily declining[xix] (and risk, accordingly, is rising).

Mobile as the "Remote Control"

The mobile medium has a key role to play in addressing the management of digital identity / identities. Mobile networks are ubiquitous, mobile phones are increasingly powerful and intelligent, and mobile SIM cards have a long and proven track record of robust security.

Mobile's primary advantage – and the attendant opportunity – derives from the fact that the SIM card and the mobile device are already considered personal; are taken everywhere the individual goes; used as part of life's daily routine and are viewed as being as important and valuable as a wallet or purse. That does not, however, infer that mobile phones are, or will be, used for everything. They may never be used in any meaningful mass-market way for watching full-length movies, for example. But they could readily become a critical medium for asserting identity as part of the process of renting a movie online.

We have already experienced a rapid rise in the online purchase and rental of movies, and the mobile medium could readily add value: as a payment authentication factor when a movie is being purchased from the online provider; as an age verification medium so as to ensure adult-rated movies are not viewed by minors; as a security function for an individual's online movie library, such that their paid-for content cannot be accessed or stolen by others.

Similarly, a mobile-based identity could be "federated" across multiple online movie sites, such that the user need not create a separate username and password for each one – they could use the same mobile identity to access these and other sites. User profile information from the user's mobile identity could be used to generate movie recommendations each time the individual connects.

Indeed, mobile operators' comparatively strong registration process could replace the online movie provider's weak self-registration process, and remove a barrier to entry for end-users. The depth and breadth of operators' registration processes may infer the ability for the movie provider to create richer, stickier and more revenue-generative services (by, for example, recognising that a subscriber is a foreign national who may want to buy or rent movies in more than one language).

Finland: A showcase for mobile identity interoperability

In Finland, all three mobile operators – TeliaSonera, DNA and Elisa – have launched mobile identity services that transcend a wide range of use cases. Uniquely, the three operators have formed a "circle of trust" – an agreement under which the operators accept digital identities created by each other, and allow those identities to effectively "roam" on their network and make use of agreements that each individual operator has with third party service providers.

As a result, a subscriber with a digital identity created with DNA, for example, can use that identity to access the services of third parties that are partners of TeliaSonera and Elisa, and vice versa. In essence, this means that the operators have agreed to adopt the same technical platform, trust the authenticity of identities provided by each other, and provide third party service providers with a single, plug-and-play solution for the adoption and integration of mobile identity services.

Making use of wireless public key infrastructure (W-PKI) enabled SIM cards, the operators have deployed strong authentication that offers a level of security that is equivalent to the existing digital identity scheme run by Finland's banks (called BankID).

Current Mobile Identity Solutions

Many mobile operators have already recognised the importance of taking a role in identity, and have deployed services and solutions in response. Those services map, in broad terms, against the nature and dynamics of the opportunity; they range from federated identity services, which allow mobile subscribers to create a single, mobile-based identity which can be used as a login for multiple websites and online services, through to mobile signature, which provides a direct replacement for a "wet" ink signature on a paper contract. The existence of these solutions at such an early stage serves to reinforce the seriousness of digital identity as a topic, and the importance of the strategic opportunity that digital identity represents.

(1) Federated Identity

Federated identity provides a mechanism for a single set of credentials (a single digital identity) to be used across multiple IT systems or websites, rather than the user having to register and remember credentials for each. It is often mistakenly referred to as Single Sign On (SSO), which is a similar concept, but with the key difference that in SSO the user only need enter their credentials once to access all the IT systems or sites.

In the online world, federated Identity is becoming very popular amongst users for accessing online services, and a number of prominent web players including Facebook, Google and Yahoo, now provide federated identity platforms for users to log in with their existing credentials to a range of different third party websites.

The benefit to the third party website is that they can effectively outsource the management of user identities to one or several of the identity providers, whilst still being able to manage the user's individual account.

Better still, for those website owners integrating the Facebook Login identity system specifically, they receive additional information about the user from Facebook, which they can then use to personalise the site to deliver a better user experience – on an individual by individual basis.

Figure 8: Example of Federated Identity Logins

Federated identity services are already available from a large and growing number of service providers, as illustrated here.

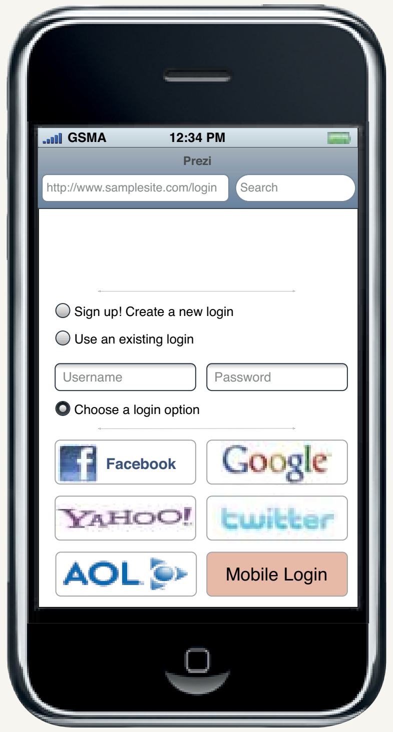
From the perspective of consumers, these services offer convenience: they can use a single identity to log into multiple websites and services, and therefore no longer have to remember multiple usernames and passwords.

From the perspective of service providers, the key benefit is access to very large customer bases.

Mobile operators are in the process of deploying federated identity solutions that essentially perform the same function as existing online services.

However, operators are also examining the integration of additional features, such as "add-to-bill" and second-factor authentication, such that both end customers and service providers enjoy greater functionality.

An additional benefit to service providers is operators' level of assurance that an individual customer is who he or she claims to be.



Estonia: a glimpse of the future for mobile identity[xx]

Estonia is arguably the world's most advanced country within the realm of digital and mobile identity. The country's Mobile-ID service allows an individual to use their mobile phone as a form of secure electronic identity. Like an ID Card, the Mobile-ID can be used for securely accessing eGovernment services and for digitally signing documents (a process which has already become an established norm in Estonia). The service uses a W-PKI SIM card, which individuals must request from their mobile phone operator (all of the country's mobile operators offer such SIMs). Private keys are stored on the SIM card along with an application for authentication and signing.

In brief overview, the service works as follows:

- The individual clicks the "Log in with mobile ID" option on a supported website;
- The phone displays a message indicating that a connection is being made;
- The user is prompted to enter a PIN code into the phone;
- The message on the phone disappears and the website is automatically reloaded with a logged in screen.

The list of applications of this mobile digital signature service is broad and growing. Individuals can vote (even when overseas), pay for goods and services online, pay for municipal services such as parking, access social security services and even register a new business.

Federated identity solutions offered to website owners are typically based around three different but related open technical standards, established by international bodies: OpenID, OpenID Connect and OAuth, all of which can equally be offered by mobile operators. Moreover, operators have the opportunity to further enhance their propositions with seamless sign-on (when accessing via a mobile device) and verified user profile attributes to make their offerings more competitive and comprehensive.

Whereas in a typical website login, the individual enters their credentials to enter the site, when accessing a service over mobile, the operator already knows who the user is and doesn't need the user to enter any credentials (as the phone has already been authenticated via the SIM). As a consequence, for the user logging in becomes a simple one-click process; they select their operator as their chosen identity provider (from a list which might include other mobile operators, Facebook, Yahoo and others) and the login process takes place automatically.

Where the mobile approach to federated identity will likely become especially potent is within the context of desktop or laptop access (i.e. non-mobile, non-SIM). From a regular PC (connected via fixed broadband), the individual can still use their mobile identity to log in, by selecting their operator, then inputting their mobile phone number. Where appropriately configured, the website will then automatically generate a message to the individual's mobile phone, asking them for permission for the PC-based login.

Permission would typically be granted through use of a one-time-password (OTP), which would be sent to the mobile phone, and which the user would have to input via the PC, or through the user inputting a pre-registered PIN on the phone, which would then return a validation message to the site.

This type of approach adds very considerable security to PC-based Internet access – under such circumstances there would be no need for individuals to save usernames and passwords on their PC, nor remember any (other than a single PIN code, under some configurations) and indeed, this use of mobile as a second factor makes it functionally more difficult for any third party to gain access to an individual's services, content and – most importantly – identity, online (though it is important to note that the solution does require the device and SIM to be connected to the network, and therefore within the coverage footprint of the operator).

(2) Mobile Two-Factor Authentication

The example above blends federated identity with second factor (2FA). But it is important to note that there are many types of 2FA, offering a range of security levels and varying functionalities and user experiences.

2FA solutions typically fall into the three categories set out earlier:

- **Something I know (such as a username, password or PIN)**
- **Something I have (such as the SIM card and mobile device)**
- **Something I am (such as a biometric parameter)**

As previously discussed, the security of an identity authentication system or process can be materially increased by using mechanisms or parameters from more than one of the above categories.

For the sake of clarity, however, it should be noted that systems that use two sets of credentials (for example a username and password combination, plus a piece of memorable information such as a secret word that only the individual and the verifying entity are aware of) are not 2nd factor since both sets of parameters come from the same category ("something I know"), and if written down together on a piece of paper could be easily compromised.

Sri Lanka: Dialog's ground breaking "Connect" solution

Dialog, a leading mobile operator in Sri Lanka, has developed a service by the name of Dialog Connect, a seamless sign-on solution allowing customers to login and access content from third-party websites using a combination of their mobile number and a secure customer PIN. Several thousand unique users are already using Dialog Connect on a daily basis, to access online content such as music, retail and gaming. Service providers in Sri Lanka see value in the Dialog Connect solution in providing verified customer profile information while reducing the "friction" that a user has to endure in creating a new username and password for each site. With analysis of click-through conversion rates, Dialog can turn its mobile identity solution into a powerful tool for customer analytics, and provide third party service providers with key information to enhance their offerings to consumers. At the same time, Dialog Connect subscribers can access services in the knowledge that their identity information is kept secure due to the strong regulatory and privacy environment in which mobile operators conduct their business.

Though Sri Lanka has a population of over 20 million, there are only 5 million personal bank accounts in the country, and just one people individuals have access to consumer credit. However, with mobile penetration at around 95% and strong government-backed commitmentby the regulator to increasing Internet usage throughout the country, the market for mobile commerce and many other mobile-enabled services is expected to grow substantially over the next two years. In this context, the ability to provide verified customer identity services will place mobile operators in a central position for enabling payments and access to services across many industry verticals.

A more secure solution therefore is to combine the credentials (username and password) with, for example, a hardware token that automatically generates a One Time Password that the user has to input when logging in to their account. Even if such a token, which is an instrument that banks commonly issue to their customers, were stolen, it would useless without knowledge of the credentials and vice versa.

Consumer research has however highlighted that hardware tokens are generally not liked by customers, as they represent yet another device that can be lost, stolen or damaged[xxi].

> "For Etisalat, mobile identity is at the heart of our strategy. In addition to the strong value proposition of Mobile Identity as a stand-alone service, we also see it as a foundation and enabler for our main strategic business verticals including commerce and our health based services.."
>
> Mr. Khalifa Alforah
> Chief Digital Services Officer,
> Etisalat Group

Mobile is a potentially strong vehicle for delivering additional factors of authentication, as set out to the right:

- **Something I have**:
  - Checking whether the device being used to access the account belongs to the user;
  - Using the phone as an alternative to hardware tokens for generating One Time Passwords (OTP);
  - Ability to receive OTPs sent to the device via SMS, or via IVR.
- **Something I am**:
  - Location of the user;
  - Behavioural profile of the user (time, place and usage patterns);
  - Simple biometrics (fingerprint scan, face recognition).

In addition to the above, the "something I know" element is readily input and transmitted by the mobile phone, which is typically always connected and always with the user. The mobile phone is already being used by a number of proprietary solutions as a 2nd factor of authentication, the most well-known being Google Authenticator, which generates a One Time Password on the device; there are many other, similar solutions that send OTPs to the device via SMS or use an IVR system.

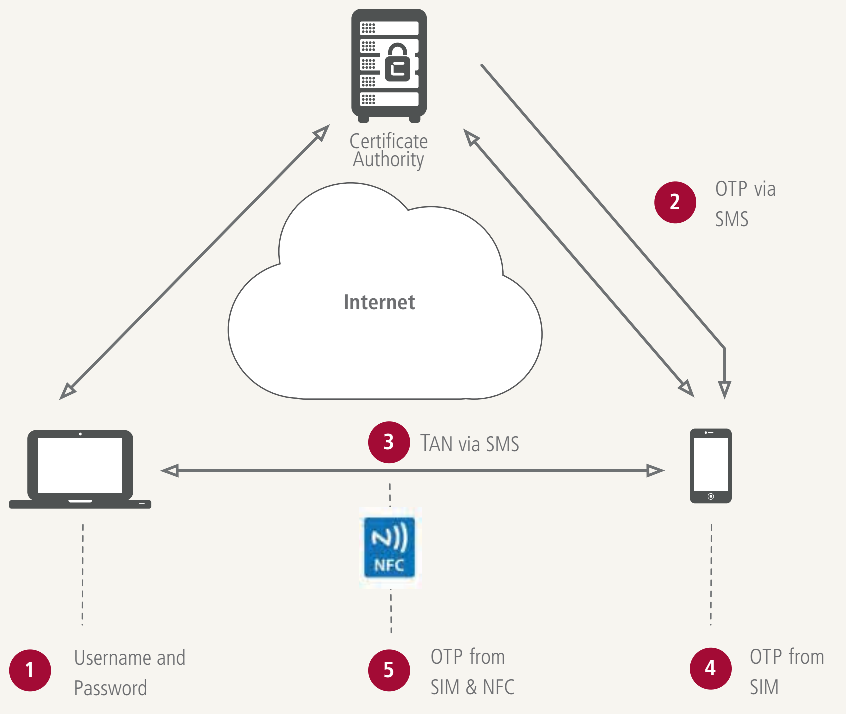
By enabling a real-time "challenge and response" these solutions present many advantages over simple, single factor username and password credentials.

However, while they are more secure than browser-based and single-factor approaches, many such solutions are still open to what are known as "man-in-the-middle" attacks. For instance, IVR-based calls can be automatically forwarded to the attacker's own IVR system, and SMS messages can be captured on the device by a Trojan app such as ZITMo (ZeuS In The Mobile)[xxii] and also forwarded on to the attacker. A more secure approach is therefore to generate a One-Time Password on the device itself, in a secure environment such as the SIM, by downloading and activating a Java applet over-the-air, which can generate time-based one-time-passwords on an as-needed basis.

The OTP can then either be transmitted directly to the relying party over the secure mobile channel, or entered manually by the user into the device (e.g., PC, tablet etc.).

Another option would be for the OTP to be transferred from mobile to PC via an NFC reader attached to the PC and would act as a good substitute for hardware-based TAN[xxiii] tokens used in online banking or VPN access tokens used for remotely accessing Enterprise IT systems. These options are illustrated on the following page.

Figure 9: Second Factor Authentication Methodologies



In a little more detail, the methodologies set out above are as follows:

1. Credentials (username + password) only (something I know)
2. Credentials (something I know) + OTP via SMS on mobile (something I have)
3. Credentials (something I know) + OTP via SMS & entered via PC (something I have)
4. Credentials (something I know) +OTP generated on SIM and transferred directly via mobile channel
5. Credentials (something I know) + OTP generated on SIM and transferred via PC using NFC reader

Other than in methodology one, which is simple username and password entry, all of these methodologies include a second factor which ensures that something other than the username/password combination is required in order for access to be granted, and hence the user must be in possession of the mobile device and SIM card for the solution to work.

(3) Mobile Digital Signature

Digital signatures assert identity by using Public Key Infrastructure (PKI)[xxiv] to digitally sign and secure a message sent between two parties. In some respects, therefore, digital signature has a slightly different purpose to other mobile identity management solutions:

- It encrypts a message so that only the sender and recipient can read it;
- It enables the recipient to check the authenticity of the message and to verify that it hasn't been tampered with in transit;
- It securely assigns an identity to the message so that the recipient knows who sent it (a process known as signing).

The SIM already provides a secure environment for running cryptographic operations (for authenticating the user on the network) so is an apt tool for supporting digital signatures. By establishing a Wireless Public Key Infrastructure (WPKI) and providing digital certificates to users via the SIM, a digital identity can be established and used across a wide range of services, especially where there is a high level of contingent risk or potential loss.

> "Mobile identity represents a substantial opportunity for mobile network operators to provide a unique customer identification service, through which customers can access different services (social networking, banking, e-health, public administration, employee identity and many others) through a variety of different devices, leveraging a core asset of the GSM system: the authentication and security provided by the SIM card and the network. Taking advantage of the secure environment and multi-application platform provided by the SIM, operators can store certificates and keys in the SIM which allow for secure customer authentication and the opportunity to digitally sign content and files.The GSMA is working to create a common framework to enable recognition and acceptance of mobile identity services across multiple countries, in order to achieve economies of scale and the delivery of a truly international mobile identity footprint. Telecom Italia is investigating possible service scenarios in accordance with the European Digital agenda, to drive the adoption of mobile identity as an asset to increase the diffusion of digital services, leveraging the pervasive adoption of mobile phones."
>
> Franco Bernabè
> Chairman & Chief Executive Officer
> Telecom Italia

Figure 10: Mobile Digital Signature Provisioning Process

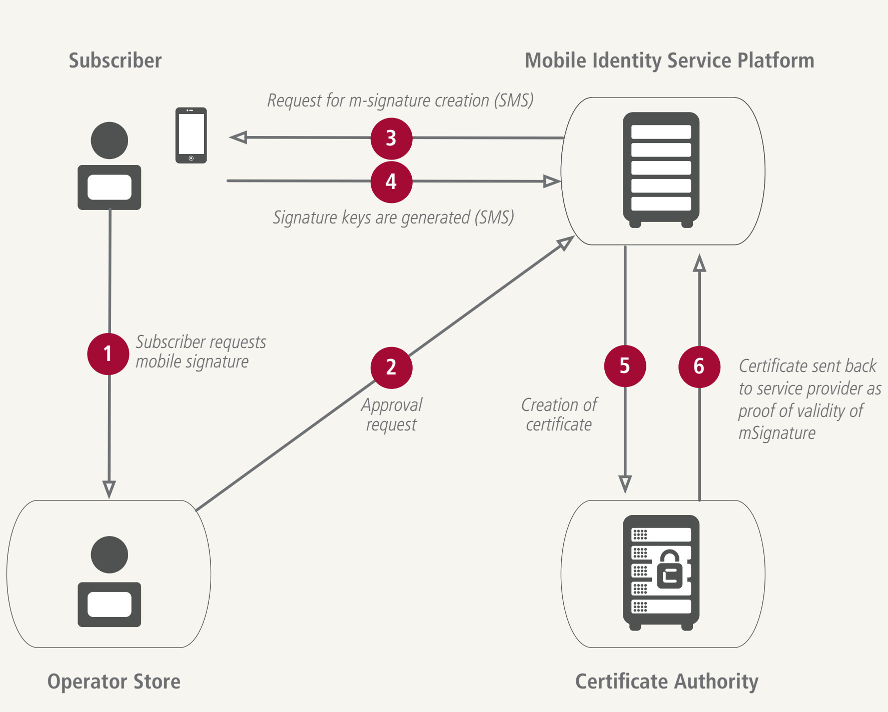

Subscriber
Mobile Identity Service Platform
Request for m-signature creation (SMS)
3
4
Signature keys are generated (SMS)
1
Subscriber requests mobile signature
2
Approval request
5
Creation of certificate
6
Certificate sent back to service provider as proof of validity of mSignature
Operator Store
Certificate Authority

Figure 10 to the right illustrates the process for provisioning a user with a mobile digital signature.

The first step, following the user's initial request, is for the operator to verify the supplied user credentials[xxv]. Once validated, the Mobile Identity Service Platform (which could be operated by the operator or a vendor on their behalf) issues a request to the user's WPKI-enabled SIM to generate a set of keys: a private key that remains in the secure element of the SIM and a public key which is passed on to the Certificate Authority (CA) to sign with their own private root key, hence generating a digital certificate for the user.

The certificate itself could be issued by a private entity for use in a business context (e.g. email, VPN), a personal context (e.g. gaming), or if issued by a national authority could be used for banking, e-government services, healthcare and other applications that are dependent on verified identity. Usually, certificate authorities are organized in hierarchies; for example, a national government might operate a root certificate authority that accredits secondary certificate authorities, which in turn accredit individual users.

To sign a document or transaction, a hash[xxvi] of the data is first sent to the Mobile Identity Service Platform (MISP). The MISP then contacts the user via SMS and asks them to sign the hash by entering their secret PIN on their mobile device. The combination of the PIN and the user's private key triggers a cryptographic process within the SIM to sign the hash and return it to the MISP, where the certificate used to sign the hash can then be checked by the Certificate Authority. If correct, the signed and validated data can then be passed on to the recipient and the transaction is complete.

What this means, in practice, is that it is possible to deploy a solution in which the authenticity of sender and recipient are verified to a very high degree. The encrypted messages exchanged between them are thus deemed secure enough to be relied upon for commercial and / or personal matters that might otherwise be considered too sensitive to be transacted via digital means.

In short, a number of governments around the world have found mobile digital signature methodologies to be secure enough for them to be afforded the same rights, in law, as a hand-written signature on a piece of paper.

That is to say that in a number of countries, including Turkey, Moldova, Estonia, Finland and elsewhere, it is possible to sign contracts via mobile, arrange a loan, buy a property or even vote.

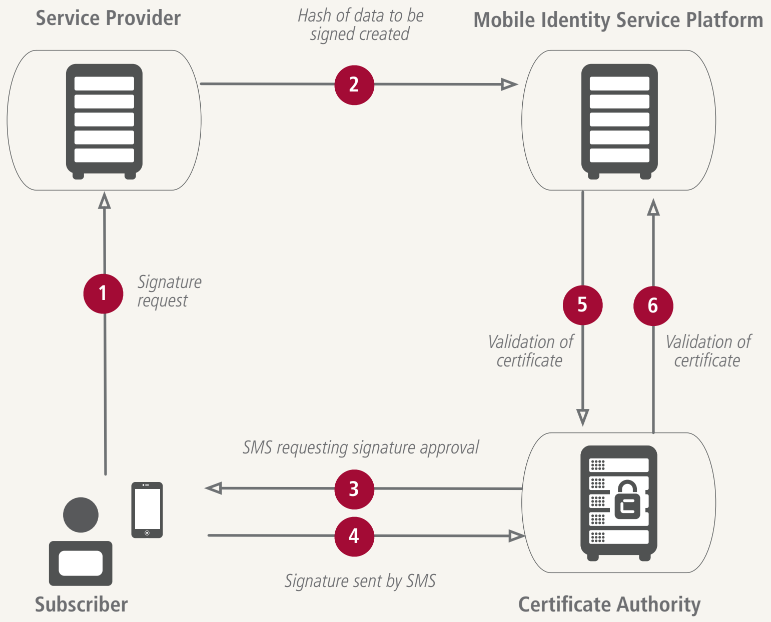
(4) Identity Attribute Brokerage

As previously mentioned, there can be considerable benefit to users and service providers if basic information about the user (pertaining to that individual's identity) can be shared, selectively. A simple example would be in providing the individual's name and delivery address automatically when buying goods online, or in personalising information presented to the individual based on their location. Mobile operators are especially well placed to act on the user's behalf in brokering this type of information to third parties:

- Operators have already built up a trusted relationship with users and have verified important demographic attributes such as name, age and address during their registration process;
- Operators' core business is based on the provision and sale of communications services, not the trading of customer data, and therefore they can take a more measured and sensitive approach to the sharing of individuals' information with third parties (than is often the case amongst online businesses);
- Since mobile operators are only just beginning to collect more detailed and wide-ranging identity attributes, they can provide individuals with the opportunity to very precisely set out, and subsequently manage, the information that pertains to their identities and the rules under which that information is shared.

In the longer term, by providing a federated identity service that spans multiple websites, mobile operators should be able to collect and collate a richer profile based on the user's behaviour – what they access, when and where – than would normally be the case in the "fixed internet" world.

Figure 11: Mobile Signature Process Flow


Service Provider
Hash of data to be signed created
Mobile Identity Service Platform
2
1
Signature request
5
Validation of certificate
6
Validation of certificate
SMS requesting signature approval
3
4
Signature sent by SMS
Subscriber
Certificate Authority

Turkey: the birthplace of mobile digital signature[xxvii]

Turkcell is the leading communications and technology company in Turkey, and the first operator in the world to launch a mobile digital signature solution. The idea behind Turkcell's Mobil Imza (mobile signature) is to offer a remote, secure way to complete transactions in a manner that is equivalent to providing an "original" signature on a hard paper copy. This makes it possible to sign documents and authenticate individuals via a mobile phone, in a way that is legally approved, secure, easy and convenient. Launched in 2007, Turkcell's Mobil Imza service specifically targeted the banking sector: in Turkey, it is common practice for customers to have to sign a comparatively large number of contracts, terms and conditions and other documents in relation to financial transactions. The Mobil Imza service was therefore designed to make such processes simpler and easier, and remove the need for individuals to visit bank branches in order to physically sign documents.

Since launch, the service has attracted a substantial base of users, and usage levels have increased more than five-fold. Turkcell is now in the process of deploying the service more broadly: to the initial roster of banking service providers, the company has now added insurance brokers, the Government, ecommerce companies and even large corporations, who use the underlying MSign technology to secure communications and electronic document signatures within the context of their own operations.

Live Mobile Identity Services

The services explained above are, for the most part, already live and available from a variety of operators worldwide. Whereas the mobile industry is at an early stage of development within the context of digital identity management, a number of forward-looking operators have recognised not only the importance of individual identity management services, but more broadly, the importance of holding a front line position in the identity ecosystem.

In Finland, for example, all of the country's mobile operators offer mobile digital signature services, which in turn have been adopted and deployed by service providers including the Finnish Government, a growing number of banks, online stores / ecommerce providers, the postal service, airlines and others.

Use cases range from the relatively simple, such as using mobile identity for age verification in liquor stores, through to the comparatively complex and sensitive, such as requesting medical test results from the national health service. The digital signature service has achieved widespread usage in part because the mobile operators worked closely with the government to ensure that the mobile signature service was in accord with the government's requirements.

Service providers agreed to adopt the service also because of the strength of the registration process, and the level of assurance relating to subscriber data that resulted. In the case of Finland, the strength of the registration process combined with the capabilities of the underlying technology (WPKI) has proven extremely successful.

Operators in Estonia have deployed the same underlying technology as the basis of their mobile digital signature. Because of the inherent security and reliability of PKI technology, operators' mobile signature services can even be used for voting and accessing citizenship registers (amongst other things).

Indeed, the version of citizens' identities on the mobile device / SIM now has the same legal status as Estonia's ID card[xxviii]. As is the case in Finland, the number and diversity of use cases is substantial and growing.

In the developing world, the notion of identity tends to be comparatively under-developed, and this has implications for individuals' use of contemporary services, particularly those pertaining to the state. In many emerging economies, it is not uncommon for births to go unregistered. Inevitably, without a birth certificate, a child is unable to enjoy the benefits of public health, education and other services. It is estimated that around 40% of births go unregistered worldwide[xxix]. All individuals affected by this issue effectively have no formal or official identity, and therefore to all intents and purposes, do not exist in the eyes of the state.

Mobile operators have taken a leading role, alongside aid agencies, donors and individual governments, in addressing such issues. In a number of countries in Sub-Saharan Africa, for example, mobile technology has been used to replace legacy, paper-based birth registration processes. In these cases, the mobile medium acts as a simple (but highly effective) bearer for the transmission of birth registration data. The process ultimately results in the creation of a paper birth certificate (which is of course still the norm world wide). But by allowing for the timely and accurate transmission of registration data, the chances of any given child receiving a correct certificate shortly after birth are greatly increased[xxx].

Sub-Saharan Africa: pioneering birth registration via mobile

Within the context of many developing nations, mobile has become an enabler for the creation of physical, documentary identities. Critical identity documents such as birth certificates are often not issued, either because a child is born in an extremely remote location where state infrastructure is not available, or because of shortcomings in legacy processes, through which certificates are lost, stolen, or simply never issued. Uganda Telecom has been amongst the most dynamic operators in Sub-Saharan Africa in addressing this issue.

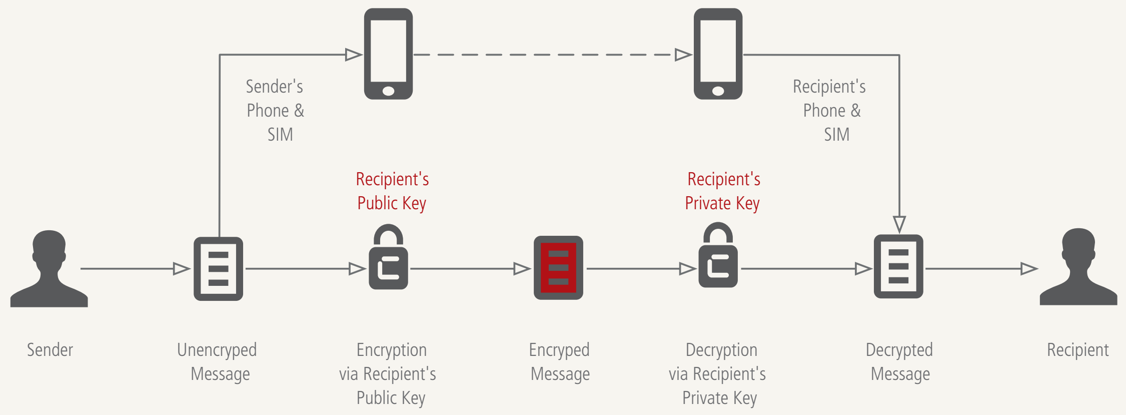
Focused specifically on the issue of birth certificate creation, Uganda Telecom developed a mobile-based process that circumvented the need for legacy, paper-based processes for recording births, and communicating information to the country's central registry office, the Uganda Registration Services Bureau. Village chiefs, who traditionally have been responsible for registration, were issued with mobile devices running Uganda Telecom's Mobile VRS solution (mobile vital records system). Hospital midwives were issued with a PC-based version of the same. The systems allowed responsible parties to populate registration forms electronically, and send them digitally to the registration bureau. By return, the bureau is able issue a short-form, temporary certificate; a paper certificate is issued later to the child's parents or guardian.

Similar services (using different technical solutions) have been deployed in Senegal, Tanzania, Liberia and Kenya. There has been a material improvement in the accuracy and timeliness of birth registration processes. This is likely to have a meaningful impact on the quality of life experienced by those registered, since it is very difficult to access health, education and other state services without having a valid birth certificate.

Public Key Infrastructure

Public Key Infrastructure (PKI) is a means of securing communications and transactions via digital telecommunications networks. First developed in the early 1970s, PKI is a cryptographic system that binds a digital public key to a specific individual, via a certificate authority, and assigns a secret private key to the individual. The public and private keys are discrete, but mathematically connected. As such, User A wishing to send a secure message to User B encrypts the message using User B's public key. Only User B can subsequently decrypt the message, using the private key. The message cannot be decrypted using the public key. Each time a message is created and encyped using the public key, a "hash" is created: the hash is a complex string of characters that is created by an algorithm, and is unique to the message. The PKI system not only encrypts and decrypts messages, but checks that the message has not been tampered with or altered, by ensuring that the hash created at the point of encryption is identical to the hash created upon decryption. If they are not identical, it is assumed that the message has been interfered with by a third party.

In Wireless PKI, all of the above also pertains, but instead of private keys and hash algorithms being held on the user's PC, they are typically stored in the secure element of the SIM card, where they enjoy a comparatively high level of security and protection.



Critically within the (W)PKI architecture, private keys are never exposed – they remain stored in a secure location, and are used only to decrypt.

Only public keys are normally used to encrypt – but they are specifically designed not to allow decryption.

Emerging markets have often taken a lead in mobile identity innovation. One of the world's first federated identity services was designed and developed by an operator in Argentina, working closely with two vendors. The federated identity service, which exposes the mobile operator's network assets to third parties via a single database (though not an API set), allows those third parties access to a service delivery platform that comprises everything from messaging, charging and billing, and basic user profiling, all the way through to content push and advertising. The solution even allows the operator's own services to work with those of online players: for example, the operator's photo-album service now integrates with online equivalents such as Flickr and Facebook. The solution also allows the mobile (federated) identity to be used over the fixed Internet, on PCs, tablets and other devices.

These are early days, but the importance and power of mobile identity management solutions are already clear. As a function of time, the role of mobile identity – and its position within the broader identity domain – will likely become clearer, and the number of accordant possibilities will grow.

Mobile Amongst Many Digital Identities

Though there are many different types of mobile identity management solutions, ranging from federated identity through to mobile digital signature, in essence the opportunity for mobile operators should be viewed more holistically; success will derive from establishing and maintaining a front line role in the digital identity management landscape. Mobile identity solutions do not and will not exist in isolation – they will always sit alongside other solutions and providers. Indeed, there are already many other identifiers that could be used as the authentication medium for an individual's online activities, from their Apple ID through to their Gmail address. Mobile identity will likely always have to coexist with these solutions; but the more rapidly mobile operators enter the identity arena, the more substantial and strategically important their long-term position can be.

As a consequence of mobile's unique capabilities (always connected, always with the user, highly secure) mobile operators can ultimately position themselves as "gateway" identity providers: that is to say the mobile phone will become the medium for the user to control and manage multiple identities, including government-issued identity credentials, bank-issued identity components and others.

In taking a frontline role in the management of digital identities, mobile operators are developing new solutions that enable new partnerships with suppliers operating right across the digital identity ecosystem.

Key Challenges for Mobile Identity

(1) Systems & Standards

Effectively all mobile identity solutions service parties other than the mobile operators themselves: that is to say that mobile identity management services ultimately become part of a third party service provider's proposition to end users (consumers or enterprise customers). What this means, in practice, is that the mobile industry will have to develop mobile identity solutions with a vast range of third parties in mind.

In short, the mobile industry must present a unified, interoperable suite of identity platforms that third parties can use. It is helpful to illustrate this point with an example. Imagine a website that sells concert tickets to consumers across the European Union. It is of considerable value for that website owner to be able to make use of federated mobile identity on his website – partly because he recognises that there are hundreds of millions of mobile subscribers within Europe; partly because he wants to be able to add functionality to his site (such as second factor authentication). But for this to be practical and cost-effective, the site owner needs to be able to write a single block of code – not a discrete block of code for each operator in each country (the latter would be too costly in terms of programming resources and processing overhead).

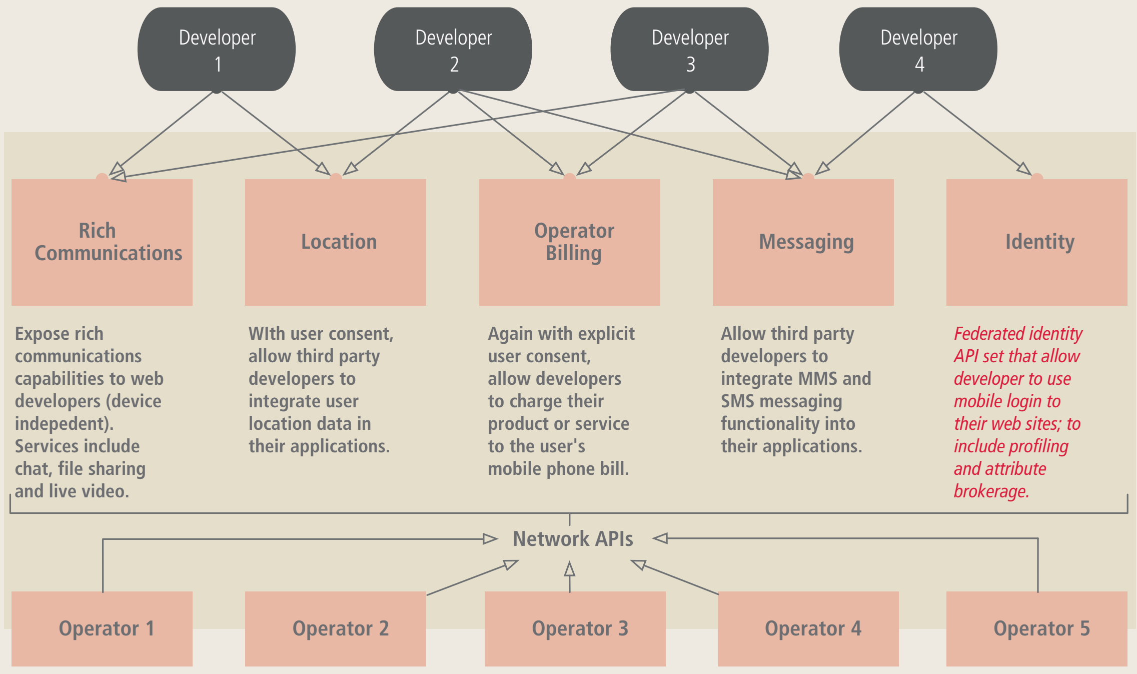
As a consequence, it is critically important that operators work together to establish a common, fully interoperable approach: such that to the greatest extent possible, a website owner or developer can access to mobile identity services in a manner that is "plug and play".

This is important because of the fragmented nature of the mobile industry. In each country, there are multiple operators, with different shareholders. By contrast, in the Internet world, it is possible to create a federated login via a single company, such as Facebook. Facebook operates in all countries across the European Union, and website owners need only use a single API to deploy its federated login offering (Facebook Connect).

There will be subtle amendments to the federated proposition on a country-by-country basis within the European Union, depending on local cultural preferences, legislation and regulations (and of course the service itself would have to be presented in the local language). But the underlying code – the machinery that makes the service functional – should be, to the greatest extent possible, uniform.

OneAPI

The GSMA OneAPI initiative defines a commonly supported set of lightweight and web-friendly APIs to allow mobile network operators to expose useful network information and capabilities to web application developers. The initiative aims to reduce the effort and time needed to create applications and content that is portable across mobile operators. A key objective of the OneAPI programme is to define and launch a seamless cross-operator reach for third party developers.



Rich Communications: Expose rich communications capabilities to web developers (device independent). Services include chat, file sharing and live video.

Location: WIth user consent, allow third party developers to integrate user location data in their applications.

Operator Billing: Again with explicit user consent, allow developers to charge their product or service to the user's mobile phone bill.

Messaging: Allow third party developers to integrate MMS and SMS messaging functionality into their applications.

Identity: *Federated identity API set that allow developer to use mobile login to their web sites; to include profiling and attribute brokerage.*

There are many advantages to the use of APIs across the mobile industry, not least that developers can integrate mobile network functionality into their offerings, on the basis of unified code, and developers' propositions can subsequently be federated across all of the operators that participate in the API initiative.

The same challenge applies to all mobile identity services. Even looked at on a single-country basis, interoperability is key. For example, if all operators in a single country deploy mobile signature solutions, and those solutions are not interoperable, their value is greatly diminished. The customers of a bank in that country on Mobile Operator A might be able to use their operator's mobile signature solution in support of a bank's services, whereas the customers of Operator B may not.

This would make the whole notion of using mobile signature less attractive to the bank, because it could not offer uniform functionality to all of its customers. And of course this situation becomes even more complex if the bank's operations cover multiple countries.

> "Mobile has to do for identity what it did for interpersonal communications. In essence, it has to take identity – physical, digital and mobile – into its next generation".
>
> Douglas Daberius
> Head of Solutions, IP Open Core MBB Voice
> & IP Transformation,
> Nokia Siemens Networks

Even in an environment where operators deploy the same (generic) mobile identity solutions, there is ample room for inter-operator competition. Every service or solution that is deployed for third parties can equally be used by operators in support of their own products and services, and indeed, can become the basis of a new innovation path. But there is an underlying, unavoidable need for operators and their vendors to align, such that the service provider community ultimately sees mobile identity management as a single, uniform suite of services provided via a common set of platforms – rather than fractured, fragmented and fundamentally incompatible.

(2) Portability

The same set of issues pertains to portability. An additional key reason for ensuring that mobile identity management solutions are uniform is so that a subscriber to Operator A can take a mobile identity created via that operator, and churn to Operator B. If this type of functionality is not "baked in" to all mobile identity solutions, their combined impact will be limited. Customers move from one mobile operator to another – this is a key enabler of competition in the mobile industry. However, individuals tend to change bank, for example, comparatively infrequently.

It would be wholly impractical if individuals hard to "start again" with their mobile identity every time they moved from one network operator to another. Not only would customers face inconvenience, but service providers would perceive considerably less advantage from the deployment and active use of mobile identity management solutions.

(3) Legislation and Regulations

The very notion of identity is linked intimately to issues of privacy: the privacy and integrity of any individual's privacy must be respected, as must their security (i.e. their identity should not be accessible to or usable by a third party). And whereas notions of privacy, confidentiality and other more complex issues (such as non-repudiation) are a fundamental part of mobile operators' business today, the broader use of mobile identity implies the need for even greater care and attention.

There have been serious consequences for companies that have taken a cavalier attitude towards privacy and security, and part of the opportunity for mobile operators is to distinguish themselves as responsible, capable guardians of individuals' digital identities. Legislation and regulations are of course country and region specific, and therefore compliance is an issue that must be addressed by individual operators. Even so, mobile operators should consider the creation and launch of digital and mobile identity services as an opportunity to offer consumers and enterprise users the highest levels of security and privacy. The sharing of identity information should be on the basis of consent – not default settings[xxxi].

(4) Device Dynamics / Operating Systems

The mobile device ecosystem is increasingly difficult to navigate: though the smart phone revolution has delivered a degree of homogeneity to the upper end of the device landscape, there remains an installed base of devices that is highly diverse, with massively differing levels of functionality. Though this is a natural underlying characteristic of the mobile industry, and one that operators are entirely used to dealing with, it is especially sensitive within the context of digital identity.[xxxii]

Going back to the example above, a bank wishing to deploy a secure mobile digital signature service will want to be assured that the service works fully irrespective of the device that the individual uses. By implication, solutions must be architected such that they can function on feature phones as well as smart phones; and they must be developed in such a fashion that, to the greatest extent possible, the user experience is common.

Integrity	The integrity of any credential, data, message or transaction is a critical concept within the realm of identity. For an identity system to be trustworthy – and trusted – it must be able to test and confirm the integrity of a message. In other words, identity systems must be able to demonstrate that the contents of the message or data have not been tampered with or altered in any way, between the point of origin and the point of receipt. To trust an identity solution, the user (and third party service providers, amongst others) must be assured that the solution is capable of encrypting and decrypting data in a manner that does not allow a third party to interfere with the data, and alerts both sender and receiver if any interference is detected.
Non-Repudiation	The notion of non-repudiation relates to the creation of uncontestable evidence that a message or data were sent from one user to another. Within the context of identity solutions, non-repudiation is a critical element – it ensures that no user can deny having sent or received or otherwise modified a piece of data, a document or transaction – after the fact. If it were possible for a user to delete their identity on a system, and all of the activities undertaken under the auspices of that identity, there would be little value in the solution itself, and no reason for third party service providers to trust it. It is therefore important that identity solutions are capable of providing non-repudiation, such that fabricated disputes over actions cannot occur.
Confidentiality	Within the context of digital identity, the notion of confidentiality is complex. One might imagine that the very act of creating an identity is in conflict with the notion of confidentiality. However, within the identity arena, confidentiality relates to what a user (an individual, with a specific identity) does. Therefore, confidentiality typically pertains to the use of crypto-graphic techniques to ensure that any data relating to an identity, and any actions taken by that identity, are encrypted in such a manner that they cannot be intercepted, modified or stolen by a third party.

Source: Digital Identity, Phillip J. Windley, O'Reilly.

Note: Based primarily on the US market.

Argentina: Movistar driving mobile identity integration

Movistar in Argentina has partnered with Nokia Siemens Networks in order to develop identity services using NSN's One-IDM (Identity Management) platform. Under the auspices of the Movistar's identity services, subscribers are able to link their Movistar identity to other third-party services online, and benefit from a unified view of their preferences. The service is highly customisable, and can accommodate different profiles - per service provider - under a single user identity. The service also provides a single-sign-on process, whereby one sign-on event allows immediate access across a broad range of third party services (defined by the customer). Supporting a number of prominent internet identity protocols, including OAuth and OpenID, the service has already proved popular amongst service providers. Movistar has also integrated use of the mobile device as a second (multiple) factor, such than a session being established on a PC can be authenticated in real time via the mobile network - implying a far higher level of security for the end-user. Importantly, the service federation approach has allowed Movistar's own value-added services, such as its photo album service, to interwork with web-based services such as Flickr or Facebook.

More broadly, ease-of-use is a critical success factor for all mobile identity management solutions. One of the key challenges that such solutions must address is the inherent complexity of multiple online logins and related user fatigue; they must also add security (through second factor for example) in a manner that does not require the user to navigate complex menus or input large strings of text or numbers.

The underlying complexity of identity solutions is considerable. For digital identity solutions to function optimally, by definition they must simultaneously embrace the complexity of digital certificates, hashes and encryption – and expose the end-user to none of it. The success of mobile identity management solutions depends materially on vendors and operators (and third party service providers) being able to uphold principles of privacy, security, confidentiality and non-repudiation within the context of services that are inherently non-complex and easy-to-use, across the broadest possible range of devices.

(5) Mobilising Service Providers

The mobile identity opportunity is almost entirely dependent on the participation of third party service providers. The more service providers that adopt mobile identity management solutions, the greater the opportunity for mobile operators (and the greater the functionality for end-users).

Convincing service providers to adopt mobile identity solutions is a very sizeable issue. It is in principle a Catch-22 issue. Subscribers will not adopt mobile identity solutions until service providers have integrated them into their offerings.

Service providers will be unlikely to integrate mobile identity until operators can demonstrate that a large proportion of their customer base is engaged. Again, this is a key reason why mobile operators will need to cooperate in the development of their identity solutions: partly so as to ensure that service providers are presented with "plug and play" functionality across their own operating footprint, and partly so as to ensure that the greatest possible percentage of mobile subscribers are reachable to any given service provider.

Numerous operators have already had to address this issue within the context of mobile identity, and have made very considerable progress. But there is a very clear difference in terms of uptake by service providers – and individuals – in countries where a single operator has deployed a "bespoke" mobile identity solution, and those countries where all operators have deployed a common solution (or at least one which offers unhindered interoperability).

Within this context, time is of the essence. The sooner mobile operators begin deploying mobile identity solutions, the sooner they can begin the unavoidably long and complex process of attracting service providers.

(6) Optimising Costs

Though by comparison to many of the activities that mobile operators undertake – such as building multi-billion dollar networks – mobile identity solutions are typically inexpensive in terms of capex, they can often imply high levels of opex. This is particularly the case with mobile digital signature, which relies extensively on the use of secure digital certificates. Certificates are necessarily expensive: certificate authorities generate certificates that "guarantee" the validity / authenticity of an individual or credential, and therefore, the certificate authority typically has to accept liability. They therefore charge fees for certificates that include an overhead to compensate the authority for accepting such liability.

The cost of certificates varies considerably, and scales with the implied risk associated with the use of the certificate (logically, therefore, a certificate relating to online banking is more expensive than a certificate used within a non-financial use case). But it is not uncommon for certificate authorities to charge tens of dollars for an individual certificate – which may have a period of validity of just one year).

As a result, early mobile digital signature solutions have tended to be expensive – making them less appropriate to the mass market. As the number of active mobile digital signature subscribers rises, the cost will naturally tend to fall, but operators may still have to find ways of further lowering costs (for example by sharing the cost of certificates with service providers, rather than passing it on in its entirety to customers).

Japan: KDDI driving federated identity innovation

KDDI of Japan has pioneered the development of federated identity. Under the brand name au, KDDI has developed a smart ID proposition under which a subscriber can create a single, federated identity, which affords access to a wide and rapidly growing range of service providers, content vendors and others.

The au ID is used as a gateway to a series of propositions. It provides a common, secure login to a wide variety of third party applications, a 50GB online storage locker for subscribers’ content, access to online and offline coupons and loyalty points schemes (run by third parties), and a suite of security features.

KDDI’s approach differs from other federated identity propositions because the au ID works only on KDDI’s network, and only for its subscribers. However, given the size of KDDI’s customer base (which was considerably greater than 35 million at the end of 2012), this is not a limitation.

The proposition to service providers includes access to KDDI’s substantial base of au ID subscribers, as well as the ability to use the au ID platform for settlement with subscribers and other features.

Another important non-financial cost related to mobile identity solutions is encryption. There are many different encryption tools that can be used in support of mobile identity solutions: and the choice of encryption typically relates to the inherent risk of the specific use case.

It is important to note that no encryption system is infallible – cryptography is the science of making the cost of uncovering the contents of a message greater than the value of the contents themselves. By implication, there is no single cryptographic solution that is appropriate for all circumstances or use cases.

The more robust and secure the encryption protocol used, the greater the processing overhead implied on the device; this in turn has a direct impact on the user experience, because higher levels of encryption imply longer processing times and therefore the perception of a poorer quality of service.

Cryptography is too broad and complex a subject to consider in greater detail here. Suffice to say that mobile operators and their vendors must take great care in the choice of cryptographic protocols so as to ensure that the processing cost (overhead) is tolerable within the context of the level of security demanded by the use case.

(7) Determining Policies

Arguably the most complex element of the digital identity arena is policy. Within this context, policy pertains to the recording, coding, storage and usage of individuals’ data.

The use of different identities, attributes and credentials in different circumstance is of material importance. Indeed, current use of different physical, identity documents illustrates the issue readily. A student entering a bar in the United States must show a driving licence in order to demonstrate that he or she is over the legal minimum age for the consumption of alcoholic beverages.

The main credential carried by that document is that the individual has passed a driving test – a point that has no relevance or interest to the bar. Perhaps more importantly, however, the driving licence also contains the name and home address of the individual; the bar does not need access to this information, and in many cases, it is likely that the individual does not want to share it.

Most importantly, the driving licence also includes the individual’s date of birth. Even this is not the information that the bar needs; the bar needs to know if the individual is over the age of 21 – not the date of birth. Whereas the doorkeeper at a bar is unlikely to scan, store and make use of the information on driving licences shown by people entering an establishment, the same cannot be assumed within a digital setting. In other words, the same cannot be allowed to happen in a digital setting: if the required credential is “user is over the age of 21” then only that credential should be supplied. A key difference, however, with the above analogy, is that whereas doorkeepers typically have no interest in the superfluous information on a driving licence, most internet-based service providers would very much like to gain access to such information.

The complexity of the myriad use cases that exist within the broader digital identity domain is considerable. And for every use case – including the most simplistic and seemingly mundane – a detailed analysis must be undertaken in order to establish which attributes and credentials pertaining to the individual are required (and which are not), how those attributes and credentials should be provided, for how long and for what purpose.

Summary

Whereas the list of challenges facing mobile operators within the digital identity domain may appear daunting, many of them relate – at a fundamental level – to the opportunity. From the perspective of individuals, the mobile industry represents a “clean sheet of paper” in terms of digital identity management. There is therefore a considerable opportunity for operators to position mobile as a uniquely responsible medium; one which respects privacy, delivers the highest levels of security and confidentiality, and most particularly, one that affords complete control to end-users (as will be explained in greater detail in the final section of this report).

That said, digital identity is unavoidably complex and sensitive, and the process of engaging service providers represents a massive undertaking. But the strategic importance of digital identity outweighs the challenges set out here, and others that may arise in the future.

Vision of the Future

Before considering the future of mobile identity per se, it is worth first considering why mobile represents the optimal medium for the provision of identity management services.

It is therefore worth briefly restating the issues that mobile identity solutions are aimed at addressing. Identity is a broad concept – and importantly, is one that is far broader than the term “mobile identity” implies. It is critically important that operators recognise that the role of mobile pertains to a very substantial subset of what we call “identity” today.

Initially, and for the most part, the mobile medium will most commonly provide identity management services within the context of online use cases; but in the longer term, there is no reason why it should not add convenience, security and privacy within the context of real-world identity use cases – from entering a building to buying goods in a supermarket. Identity is a very broad ranging enabler, and mobile identity solutions can yield value within a far broader setting than just the mobile world.

> “Mobile identity is no longer just a futuristic concept. At Axiata, we see it as a reality today with the potential to revolutionise the customer relationship and experience. But time is of the essence and the Operator community will suffer if we miss the opportunity to act now”
>
> Jamaludin Ibrahim
> President and Group CEO
> Axiata Berhad

Why Digital Identity Needs Mobile

It is instructive to consider the situation from other perspectives. Why, for example, does digital identity need mobile? At the simplest level, digital identity needs mobile because mobile is the only medium that is based, at a fundamental level, on an extremely secure technology (the SIM card) which is already used for “live” authentication. This is central to the opportunity: not only is the mobile device nearly always with the individual who owns it, but also, the SIM card in that device provides an authentication process that is amongst the most secure available. It is clearly a logical step to use that authentication ability across a broader range of use cases.

Within the context of the online world, mobile’s authentication ability is potentially of considerable value. As mentioned earlier in this report, individuals are not only performing a broader range of functions online, but they are also performing functions with a greater degree of implicit risk (buying, selling, banking and so on). The ability to verify the authenticity of buyers, seller and indeed service providers is of material importance.

Another key reason why digital identity needs mobile is registration. Mobile operators already perform strong registration processes for a substantial (and growing) proportion of their customer bases. Like banks, mobile operators have to perform “know your customer” registration processes for commercial reasons (the mitigation of risk) and sometimes for legal and regulatory reasons (mandatory SIM registration, for example). By implication, mobile operators know key attributes / credentials pertaining to the identity of their customers.

It’s Not What You Know, It’s Who You Know

Clearly, mobile operators are not alone in having access to certain key data relating to customers’ identities. An online retailer, for example, may have a wealth of information related to its customers, including their name, address, bank or credit card details, and purchase history (amongst many other things). However, it is arguable that their current operating model exposes them to considerable risk, because they are not able to authenticate their customers in a secure manner – their authentication process is no more than the individual entering their username and password.

Unlike any other medium, mobile is able to authenticate the individual’s identity, via a variety of means (in the example above, the online retailer could use mobile to provide second factor authentication in association with any attempted purchase).

Within the context of this example, the mobile operator involved may never gain exposure to profiling information relating to their customer’s online purchase behaviour / history, but would nonetheless have a key role to play in ensuring that the purchase is executed securely and in a manner that respects the need for privacy and non-repudiation.

Mobile Operator Positioning

Aside from mobile technology itself, mobile operators have several other characteristics that potentially give them an advantage in the identity ecosystem.

The first is that, in all countries, all mobile operators are local; that is to say that they are a locally incorporated, limited liability entity. Moreover, their capacity to engage in the business of being a mobile operator derives from a state-issued licence. Operators are, therefore, responsible and accountable businesses, which are required by the terms of their licence and by the regulations under which they are obliged to operate, to serve customers. Though it is not necessarily always clearly manifest, this situation implies that mobile operators occupy a position of trust within their host country.

Deriving directly from the above, mobile operators have become (and will continue to be) large organisations. More specifically, operators tend to have large retail chains, often wholly owned, which represent an ideal platform for strong registration processes (for which, of course, they are already used). In addition, operators have very large customer support functions, often comprising tens of thousands of staff, which are designed to resolve issues and problems for customers.

These are non-trivial points. Two of the single greatest weaknesses faced by online companies are (i) their lack of physical registration presence and (ii) their underdeveloped customer support infrastructure. If your social network identity is stolen, or fails, whom do you call?

In addition, mobile operators already have very sophisticated fraud detection and prevention systems, which constantly monitor for suspicious activity and, more importantly, constantly oversee the authentication process pertaining to all network activity. In short, therefore, the (ownership) structure of the mobile industry, the nature and capabilities of individual mobile operators, and the technology that they employ, place the sector in a potentially very strong position to address the digital identity opportunity.

Why Service Providers Need Mobile Identity

Mobile identity management services are of little or no value unless service providers – third party website operators and app developers initially – actively want to deploy them within the context of their services. At present, too few third parties recognise the benefits of mobile identity management solutions, and arguably too little has been done to date in order to persuade them otherwise.

Mobile identity solutions are suitable for a wide range of use cases. Federated identity (as a standalone solution) allows third parties to offer a single-click login solution that is considerably easier – and inherently more secure – than the standard username and password methodology. Second factor authentication can add a very substantial increment in security, particularly within use cases that involve financial transactions. And mobile signature allows for customers to sign – in a legally binding manner – contracts, new terms and conditions, and so on.

In summary, the key benefits that mobile identity management solutions can offer to service providers include:

(1) Security:

In all cases, mobile identity management solutions can add materially to the level of security of any online use case, either by circumventing the need for inherently weak username and password combinations, or by adding additional factors of security;

(2) Convenience:

Even where the mobile identity management solution adds an additional factor to a process (thereby sometimes implying additional key strokes), the mobile medium implies (or should imply) additional convenience for the user, both in terms of the trade-off between additional key strokes and greater security, and more generally, because of the ease with which a secure login or transaction can be achieved by using mobile either in isolation, or in combination with another medium (such as a fixed internet connection and a PC);

(3) Functionality:

By definition, the use of mobile identity management solutions should allow service providers to develop and deploy new services: partly because of the ability to "bind" different media together around a single digital identity (such as fixed and mobile, or even connected digital television and mobile), and partly because of the capacity to use mobile to deliver standalone new functionality;

(4) Reduced Fraud:

Though a net reduction in fraud is not implicit in the deployment of mobile identity management solutions (clearly, it depends on the design and inherent robustness of the solution), it is arguable that the use of the mobile medium should result in a reduction in fraud (a) because of the level of assurance that mobile operators have in the identities of the subscribers and (b) because of the capacity to add multiple factors to any given process or transaction;

(5) Improved Customer Knowledge:

Again deriving from operators' level of assurance vis-à-vis their subscribers' identities, third party service providers should be in a position to make more informed decisions relating to the needs and preferences of individuals.

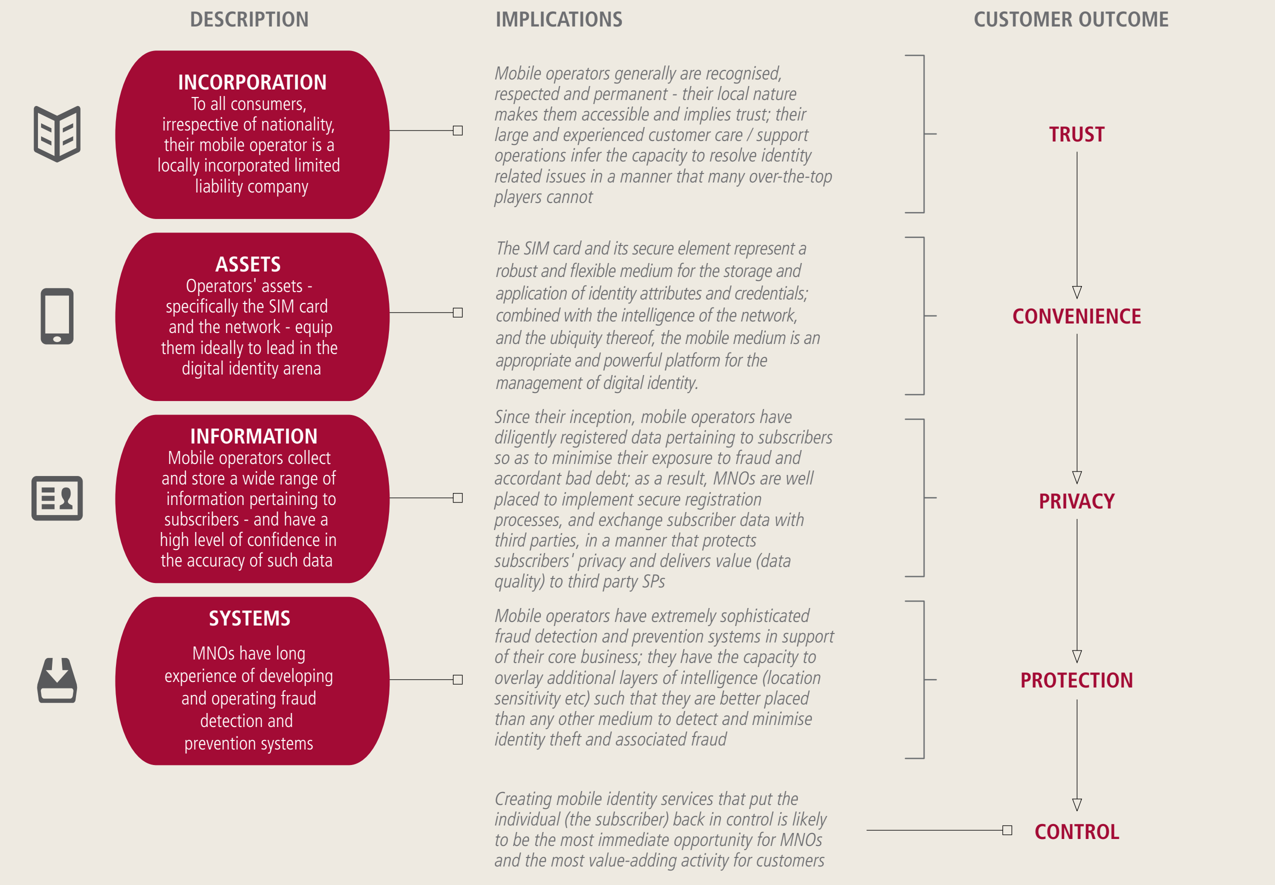
Moreover, in instances where the third party makes use of identity brokerage services from mobile operators, the level of assurance pertaining to individuals' attributes should allow for more informed customisation (particularly when compared, for example, to the attribute data that third parties might receive from social networking identity providers, whose registration process is weak, and whose customer attributes are largely unchecked).

Why Mobile Operators Must Act Quickly, and Collectively

All of the above advantages of mobile identity management solutions are essentially time-limited. That is to say that there are already mobile identity offerings available to service providers and consumers, which are being increasingly widely deployed and employed. The more widespread and popular these solutions become – irrespective of the mobile industry's view on their inherent security, functionality and usefulness – the more difficult it will become for mobile operators to compete. As an industry, we may question the usefulness of social network-derived identity management services, but our view is of little import if service providers continue to adopt them eagerly.

The mobile industry has yet to fully align itself to the digital identity opportunity. Whereas individual operators have made considerable progress, for the most part identity remains a strategic theme, rather than a line of business. This must change before the opportunity is taken by others (non-mobile players).

Figure 12: Mobile Operators and the Provision of Identity Management Services



INCORPORATION: To all consumers, irrespective of nationality, their mobile operator is a locally incorporated limited liability company

Mobile operators generally are recognised, respected and permanent - their local nature makes them accessible and implies trust; their large and experienced customer care / support operations infer the capacity to resolve identity related issues in a manner that many over-the-top players cannot

ASSETS: Operators' assets - specifically the SIM card and the network - equip them ideally to lead in the digital identity arena

The SIM card and its secure element represent a robust and flexible medium for the storage and application of identity attributes and credentials; combined with the intelligence of the network, and the ubiquity thereof, the mobile medium is an appropriate and powerful platform for the management of digital identity.

INFORMATION: Mobile operators collect and store a wide range of information pertaining to subscribers - and have a high level of confidence in the accuracy of such data

Since their inception, mobile operators have diligently registered data pertaining to subscribers so as to minimise their exposure to fraud and accordant bad debt; as a result, MNOs are well placed to implement secure registration processes, and exchange subscriber data with third parties, in a manner that protects subscribers' privacy and delivers value (data quality) to third party SPs

SYSTEMS: MNOs have long experience of developing and operating fraud detection and prevention systems

Mobile operators have extremely sophisticated fraud detection and prevention systems in support of their core business; they have the capacity to overlay additional layers of intelligence (location sensitivity etc) such that they are better placed than any other medium to detect and minimise identity theft and associated fraud

Creating mobile identity services that put the individual (the subscriber) back in control is likely to be the most immediate opportunity for MNOs and the most value-adding activity for customers

Speed is of the essence; but so is collaboration. A primary reason for the rise in other identity solutions – especially federated identity – is because of the ease with which third parties can access very large customer bases.

The use of a single API gives a third party access to the entirety of Facebook's base. At present, this is not yet the case in the mobile industry (though as illustrated earlier, our own APIs exist); further steps must be taken to ensure that a solution is deployed. Whereas the mobile industry, collectively, has the single largest customer base of any communications medium, that base is fragmented across hundreds of operators. Facebook's is not.

Standards and interoperability are therefore key. In addition to the creation of a common, industry-wide set of identity-related APIs, it is critically important that operators and vendors work towards agreeing and deploying standards / solutions that are "plug and play" from the perspective of third parties – spanning second factor authentication, mobile signature, attribute brokerage and other areas (as they are identified).

Replication is not the Solution

It is extremely important that the mobile industry take the fullest advantage of the opportunity presented by identity. Doing so involves driving towards mobile identity solutions that extend beyond the capabilities and functionality offered by existing operators in the digital identity space. Simply replicating what already exists will not serve to differentiate mobile operators and mobile identity management solutions; their functionality must be designed, very specifically, to give service providers and consumers functionality and levels of security that cannot be achieved by other means. By implication, therefore, it is important to consider identity (digital and mobile) – from day one – as something more subtle, sophisticated and advanced than the services on offer at present.

Identity as Presence

Within this context, it is important to note that the opportunity for mobile operators (and others) in the identity arena does not just arise from addressing issues pertaining to identity theft. Though creating solutions that improve levels of digital security, particularly pertaining to online activities, is hugely important, there are other issues that mobile identity can and should address.

In many respects, identity should pervade almost all of the services that individuals use in the digital world. Within this context, it is helpful to consider identity as being similar to presence.

As such, my identity infers and controls my availability, my level of access, the information I choose to share, the information I choose to keep confidential, the networks (of people) I belong to, the content I can consume and so on. It is a "halo" of attributes and credentials that describe and define my presence on my mobile network, online and ultimately, in physical places.

This line of thinking helps to clarify the strategic importance of identity. Traditionally, we think of mobile identity as a basic enabler that helps us log in and transact – mostly online. In the medium to long term, this is likely to be seen as a limited, two-dimensional view of a concept that should be more comprehensive.

Mobile identity should relate to every aspect of a mobile operator's business and every aspect of an individual subscriber's activity conducted over the corresponding network.

My mobile identity should not only allow me to control "my world" – as manifest through the websites I visit, the purchases I make and the content I consume, and it should also play a central role in my communication and interaction with people and things.

It is arguably both legitimate and meaningful for mobile identity management services to play a role in everything from voice calling (for example, as a means of ensuring the authenticity of the called party before establishing a secure, encrypted line), through to messaging (invoking an identity to "sign" a digital message before sending), and beyond in to web access, transactions and so on.

The identity component of communications services is likely just as important as the identity component of online use cases. As a means of asserting operators' critical role in the world of interpersonal communications, identity could readily become a means by which mobile operators create differentiation, improve (basic) service quality and diversity, and ultimately grow customer lifetime value.

This issue is of considerable importance: for mobile identity management solutions to serve mobile operators – as well as service providers and consumers – they must add value to the length and breadth of any given operator's activities.

Perhaps most importantly, if mobile operators are able to meaningfully employ mobile identity management solutions within the context of the core services (voice calling, messaging), their capacity to add financial value should be greatly augmented.

Today, some mobile operators are seeing voice calls that historically would have been carried on their networks migrate to VoIP service providers, social networks and others. There is early data to suggest that messaging traffic is migrating to over-the-top platforms, from which operators earn little revenue. By using identity to add value to core services – by generating new functionality, higher quality, improved security and so on – operators may be able to retain more value (by stemming the migration to non-mobile platforms) or even generate new value (by stimulating net additional usage).

Italy: TIM marrying mobile identity with NFC

Telecom Italia has been at the forefront of employing the SIM card as a secure means of authentication beyond core mobile operator network services. As early as 2003, Telecom Italia had recognised the importance digital identity and authentication, and had begun deploying solutions for the creation and management of digital certificates and cyphers across both fixed and mobile networks.

More recently, Telecom Italia Mobile has begun using NFC technology in parallel with WPKI enabled SIM cards, to underpin the development of secure payment for goods and services, ticketing, access control, couponing and other services.

At the heart of Telecom Italia Mobile's digital identity propositions is the company's SecureSIM proposition. The company uses the SIM card as a multi-application secure domain, in which space on the secure element of the SIM is allocated to third parties – with each being able to create, manage and store secure digital certificates. Their approach is based on the view that the SIM card is a powerful, capable smart card that can be used as a supplement to or replacement for existing smart cards offered by third parties.

This SIM based solution is already being employed in segments as diverse as banking, enterprise access and security, cloud access, online access (federated), and government services.

There are many ways in which this could happen. By way of an example imagine if, each time a subscriber changed an element of their identity (their phone number for example), that change were transmitted automatically to all other subscribers and service providers that the individual had authorised as being permitted to receive updates of such changes. This type of service would represent considerable convenience to the individual, but would likely also result in: (a) at best, an increase in call volumes, or (b) at worst, the retention of calls that might otherwise have not been connected (because third parties did not have the individual's correct phone number).

The Importance of Control

Identity is, by definition, uniquely personal – and something that every individual should manage meticulously. The fact that individuals have not tended to take the custodianship of their (digital) identities seriously enough may relate less to human nature and more to the absence of comprehensive tools and solutions.

Within this context, the mobile medium could become extremely important and powerful. In the online world, and more broadly in the digital, connected world, the mobile phone is not always the point of purchase, the point of consumption or indeed the point of access. But it could – and arguably should – be a key point of control.

Mobile has the capacity to envelop "something I have" and "something I know" – key ingredients in the verification of identity – and can overlay additional factors pertaining to location, behavioural profiling and so on.

It therefore could become a centrally important verification and assertion medium for many other value chains. The value to the individual – the end user – is the control over the nature and dynamics of their identity that this approach could afford them. The user creates a single, "federated" identity that can be used to log in to or otherwise make use of a wide variety of services, content and use cases (it is important to note that with time, the notion of identity federation should ultimately transcend every aspect of mobile identity, from simple federated login through to mobile digital signature).

Within this context, the user has a single digital (mobile) identity, as opposed to potentially dozens of different usernames, passwords, credentials and attributes. It should therefore be considerably easier for the individual to manage the constituent parts of that identity. This process of management has two key components: the creation and updating of data that pertains to the identity (such as address, marital status and so on); and the use of controls that specify how their identity should be used (what information should be shared, with whom, for how long, and what to do in the case of a conflict between the user's settings and the default requirements of a third party service provider, amongst other things). Research commissioned by the GSMA[xxxiii] has already suggested that end-users (consumers) have a desire for this type of control. Key findings of the research, which comprised over 4,000 respondents in the UK, Spain and Singapore, suggest that:

- 50% of respondents were concerned about sharing personal information whilst using the mobile internet and / or smartphone apps;
- 81% of respondents felt that safeguarding their personal information was very important;
- 76% of respondents stated that they were very selective about who they shared personal information with, because of privacy concerns;
- 92% of respondents expressed concern about applications collecting their personal information without their consent.

Not surprisingly therefore, 89% of respondents suggested that they believe it is important to know when their personal information is being shared by an application, and to be able to turn this feature off or on. 81% suggested that they would like to be asked for permission before an application makes use of their location[xxxiv].

This research tends to confirm the inference provided by news reports relating to privacy issues, and suggests that privacy and choice are of growing importance to individuals. The provision of control – and choice – relating to identity, is something that mobile operators should consider immediately; as a fundamental component of all mobile identity management solutions.

Such controls are rarely manifest in existing (non-mobile) identity solutions, or indeed more broadly on the Internet. There has often been a cavalier attitude towards identity, with service providers assuming the right to share, rather than assuming the right to privacy. There is a strong argument to suggest that mobile operators should err towards the latter (and indeed regulation is increasingly driving all parties in this direction).

Some may argue that service providers may be less comfortable with such an approach. However, there are several key counter-arguments that are likely to prevail:

(1)Governments are becoming increasingly focused on ensuring the integrity of individuals' / citizens' identities, and as a function of time, a growing number of governments are likely to mandate "privacy by default" and "privacy by design";

(2)Consumers will likely increasingly "vote with their feet" by moving their activities away from service providers who do not actively and deliberately protect the personal information of users;

(3)Service providers may ultimately recognise more value in personal data that an individual has volunteered to share – for some type of return – than data that has been harvested without consent.

If a given user has a single mobile identity, and is given tools via which that identity and the credentials / attributes it comprises can be managed, it can be argued that the information contained within that identity is likely to be more accurate, contemporaneous and complete.

Any given attribute therein is likely to be inherently more informative and valuable to third parties – so long as the user remains in control, and can choose to share such attributes, or not.

As inferred above, conflicts may occur: for example, an ecommerce website may employ a policy that states that it will only offer discounts to individuals who share certain attributes, and a user may by default have disallowed the sharing of such attributes. In these circumstances, the user can be prompted that attributes are required, and can make an active, informed choice as to whether to continue. There are often material benefits that accrue to individuals when they share attributes and personal information: typically in the form of discounts and so on. In and of itself, sharing of information is not inherently bad or wrong – it only becomes so if the user loses control over what is shared. Ultimately, sharing is about trade – where the individual feels that there is a reasonable return for sharing data / attributes, they will likely do so (and indeed will likely be more willing to do so if the process is an optional one, over which they have control).

Mobile identity management services should be posited on the basis of user control by default and by design. Where users wish to share liberally, they may do so – but they must instruct the system to do so.

In reality multiple federated identity services will ultimately coexist side-by-side. Therefore individuals may choose to have a small number of parallel, federated identities – of which mobile is one. They may, for example, have a fictitious social network-derived identity, which allows them to navigate third party websites with a higher degree of anonymity; by contrast, they may use their mobile identity for more sensitive matters, such as accessing eGovernment services or online banking.

Functionality, Innovation and Growth

A number of concepts have been included in this report – the mobile medium as an identity "remote control"; mobile identity management solutions as a type of "presence"; and the mobile medium as a guardian of identity wherein the individual has complete control over the contents and use of their identity. These have been presented to stimulate thought and discussion amongst mobile operators and identity solution vendors.

Irrespective of whether these concepts are agreed with or ultimately made use of, it is important that all mobile operators and associated vendors view mobile identity management solutions as a key ingredient to innovation. Identity should not be viewed as pedestrian or an "add on": it is a central component of the business of mobile communications, and all that it pertains to, both today and in the future.

Every individual on earth has an identity – and a growing minority have a digital identity. The majority already own and regularly use a mobile phone; and with time, all of these notions should converge, such that digital – and ultimately real world identity – are manifest within the mobile ecosystem.

With the growing deployment of near-field communications (NFC) solutions, the mobile medium is likely to have the opportunity to play a role in real-world identity. Checking in at airports, entering office premises, purchasing goods and service in stores, and even driving cars and other vehicles may ultimately become use cases for mobile identity management solutions.

The potential length and breadth of the use cases for mobile identity management solutions represents another reason why operators and vendors should take a broad, holistic and innovative view of what identity is (in its widest sense), how it is used, and how it will be manifest in the future.

The Size of the Opportunity

It is arguably still too early to quantify the mobile identity management opportunity; even the broader digital identity market is at a comparatively early phase of development, and is accordingly difficult to forecast. GSMA research in 2012 suggested that the value of the market for mobile identity management solutions could reach US$15 billion by 2015[xxxv].

This forecast, however, may represent only part of the opportunity. Other research, for example, has suggested that the market for mobile payments may reach US$1.3 trillion per annum by 2017[xxxvi] (driven in part by NFC and associated identity management). Even the nascent market for mobile cloud access is expected to be worth in excess of US$6 billion by 2016[xxxvii].

These and many other markets will likely rely in no small measure on the existence of mobile identity management solutions. In other words, the capacity for the mobile medium to extend its reach into new markets and segments will likely depend, to some degree, on the extent to which mobile operators agree and deploy capable mobile identity management solutions that add value for service providers and end users alike.

Forecasting revenues for mobile identity management services is difficult, not least because it is likely that the majority of income pertaining to mobile identity will be indirect (i.e. mobile identity management solutions will allow for revenues from, say, mobile cloud access to accrue to operators).

The Opportunity Cost

Operators must look beyond the immediate generation of revenue, and think about the opportunity cost of not embracing identity as a part of their core business.

If mobile operators do not position themselves as a key part of the identity superstructure, other corporations certainly will. This could mean that a social networks, banks, software companies or others take a frontline role in the validation, authentication and use of identity – even over mobile networks, SIMs and devices.

Clearly, this process has started: a user can login using their Facebook, Yahoo or other federated identity, via their mobile phone; similarly, users can download the Google Authenticator application and use it to secure their Drop Box and other online services. In these and other circumstances, the role of the mobile operator extends no further than providing data carriage.

Importantly, mobile operators should not engage in the identity opportunity under the cloud of "threat". Rather, operators should recognise that the creation and commercialisation of mobile identity management services is a key, strategic opportunity that should be entered into on the basis of identity's capacity to attract and engage service providers and consumers, underpin innovation and diversification, and generate value.

Next Steps for Mobile Operators

As this report has intimated, there is a substantial need for mobile operators and vendors to make a concerted effort to enter and develop the identity arena quickly. The more existing, over-the-top players have the opportunity to establish their solutions, the more difficult it will be for mobile operators to insert their solutions into the market.

Given this, all mobile operators who have not already done so, should begin assessing the identity opportunity in their countries of operation as soon as possible, and should examine their strategic and tactical options.

There is no fixed roadmap; the starting point in some countries may be federated identity; in others, mobile digital signature may be more relevant. In all cases, however, one of the keys to success will be the adoption of standards and the creation of interoperability – recognising that service providers around the world will want uniformity, and the ability to access the whole mobile industry on the basis of common platforms and solutions.

Operators must recognise that there are, therefore, two distinct sides to the identity opportunity. The first, which faces third party service providers, is best served by operators cooperating with one another, and vendors, to create commonality and ease of use for all mobile identity management solutions.

To the greatest possible extent mobile operators should offer a "one stop shop" for mobile identity solutions, for service providers. The second, which pertains to mobile operators' own use of mobile identity management solutions, is best served by operators using their own mobile identity solutions to power innovation across their own products and services; for the purposes of customisation, new functionality, higher quality of service and reduced fraud (amongst many other things). The former is about collaboration; the latter is about competition: and the two are entirely complementary. Operators compete today on the basis of standardised technologies, operating systems and so on. The same dynamics apply to identity, though ultimately across a broader suite of propositions.

Within this context, there are several steps that all operators should take:

(1) Work with other operators:

For service providers to be willing to adopt mobile identity management solutions they will likely want to be able to address all (or at least the vast majority of) mobile subscribers in any given geographic area. It is therefore important that operators work together at a national level to build a uniform, simple platform that third parties can easily use. The same argument applies at a regional and global level: mobile operators are entering the identity arena comparatively late, and face competition from large, global online firms, which are already well established. As a result, the only way mobile companies will be able to compete effectively is through cooperation, and the creation of mobile identity solutions that are not only universal (as viewed from the perspective of service providers), but also more functional, innovative, user-friendly and price-competitive (as viewed from the perspective of consumers).

(2) Listen to consumers and service providers, and earn and maintain their trust:

The specific dynamics of the mobile identity opportunity are likely to differ by country, and it is extremely important that mobile operators undertake research that investigates the needs of service providers (beyond size of customer base) and consumers – such that specific mobile identity management solutions reflect local preferences and attitudes, and take advantage of local opportunities and challenges.

(3) Work with governments and regulators:

There is growing evidence to suggest that the involvement of governments can be beneficial to the establishment of mobile identity management solutions. A key use case is access to eGovernment services; and of course governments are one of the most important (if not the most important) issuers of identity tokens and credentials). Working closely with governments, and regulators, is an important means of ensuring that all stakeholders understand how mobile identity can enhance privacy, security and interoperability. In many countries, identity is an extremely sensitive matter, and it is important that operators illustrate the clear benefits that mobile solutions can offer to the economy.

(4) Learn from other operators and vendors:

There is a large and growing body of experience from operators who have already entered the identity arena, and the vendors who have supported them. Given that the initial part of the mobile identity opportunity is an "ecosystem play", it is likely that operators with existing mobile identity management solutions will be willing to share their experiences and help those entering the market to avoid previous mistakes, and pick "low hanging fruit". A great deal of the ground work has already been done, and mobile operators who have launched identity services should be willing to share – and those who are planning to launch should be ready to listen. There is certainly no time for the wheel to be reinvented.

(5) Work with the GSMA:

The GSMA Mobile Identity programme is already working with the majority of mobile operators that have launched identity services, and works closely with all of the main vendors of identity solutions. It is in the process of assimilating a very substantial body of knowledge and experience, and is ready to work closely with any mobile operator wishing to launch a mobile identity management solution (subject only to that operator being a member of the GSMA). As mentioned earlier, the GSMA is also working closely with operators to establish a uniform set of APIs to underpin key federated identity propositions and additional, related functionality; and is working with vendors to drive standardisation and interoperability.

Endnotes

i Global ecommerce sales will top $1.25 trillion by 2013, Internet Retailer, 14 June 2012

ii Born to be breached: the worst passwords are still the most common, Ars Technica, 3 November 2012

iii The Password is Dead; Time for Better Online Security, Forbes, 15 April 2011

iv An Application Programming Interface (API) is a protocol that is typically used as an interface between discrete software components, in order to allow them to communicate with each other. In the case of the mobile industry, APIs are used as a means of exposing an operator's network assets to third party developers, so that the latter can, for example, integrate mobile functionality such as location sensitivity or messaging into their offering.

v The value of "Smart Pipes" to network operators, Telco 2.0 Research, February 2012

vi Source: Identity Gang Lexicon

vii Warning about online fraud as information theft rises, BBC News, 17 July 2012

viii Born to be breached: the worst passwords are still the most common, Ars Technica, 3 November 2012

ix *Ibid.*

x It is important to note that even hackers are increasingly sophisticated, and they have developed means of breaking passwords that can minimise the amount of time to "guess" each password. As a supplement to "brute" attacks in which software tries to the password randomly (at around 10,000 guesses per second), dictionary-based attacks make use of the fact that the majority of passwords are words used in everyday speech. This can very substantially reduce the amount of computer processing power and time required to break a password.

xi Global ecommerce sales will top $1.25 trillion by 2013, Internet Retailer, 14 June 2012

xii Bot problem? Facebook estimates 8.7% of users are duplicate, miscategorized or spam accounts, Inside Facebook, 1 August 2012

xiii Password fatigue sets in online, Fox News, 27 August 2012

xiv 83 million Facebook accounts are fakes and dupes, CNN, 3 August 2012

xv Online advertisers cautioned against privacy blunders, Reuters, 28 March 2012

xvi Source: interview with Etisalat

xvii Major medical record breaches continue to rise, Modern Healthcare, 29 September 2012

xviii Social security fraud on the rise, News Journal, 9 September 2012

xix Password fatigue sets in online, Fox News, 27 August 2012

xx For more information, see: http://e-estonia.com/components/mobile-id

xxi Australian Banks ramp up the use of more secure SMS authentication methods, SecurEnvoy, 13 November 2012

xxii Note: Zitmo has been prevalent in the past on Symbian, BlackBerry and Windows Mobile but has more recently been found on Android devices as well.

xxiii TAN stands for transaction authentication number. A hardware-based TAN generator is a small key-fob style device that issues authentication numbers that are synchronised with keys held by service providers. Originally (and as is still the case in some countries), TANs were paper based: customers were given a printed sheet with around 50 TANs, that were date-specific.

xxiv For more information on PKI, go to – http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html

xxv The operator performing the role of a Registration Authority (RA).

xxvi A hash is simply a number generated mathematically from the string of text within the message.

xxvii For more information, please see http://www.gsma.com/mobileidentity/wp-content/uploads/2012/08/MI_TurkcellReport.pdf

xviii http://e-estonia.com/components/mobile-id

xxix Unicef fact sheet on birth registration. See – http://www.unicef.org/newsline/2003/03fsbirthregistration.htm

xxx See – https://plan-international.org/birthregistration/files/count-every-child-2009

xxxi For more information on regulations and their implications for digital and mobile identity products and services, please see – http://www.gsma.com/mobileidentity/resources.

xxxii For example, Apple's iOS (operating system) does not support use of the SIM as a Secure Element (SE), and the SIM secure element is a non-mandatory second choice on Google's Android operating system. In some cases, therefore, basing authentication for mobile identity on the SIM will require changes to operating systems to be agreed.

xxxiii User perspectives on mobile privacy, GSMA / Futuresight, September 2011

xxxiv *Ibid.*

xxxv Mobile Identity Market Sizing, GSMA / Greenwich Research, April 2012

xxxvi Juniper Research, 18 August 2012

xxxvii Mobile Cloud Computing Outlook, Visiongain, January 2012

GSMA Mobile Identity

For further information, please visit www.gsma.com/mobileidentity
or contact the GSMA Mobile Identity team at
mobileidentity@gsma.com