Mobile Identity - Unlocking the Potential of the Digital Economy

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities.

The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com** or Mobile World Live, the online portal for the mobile communications industry, at **www.mobileworldlive.com**

The Secure Identity Alliance is dedicated to supporting sustainable worldwide economic growth and prosperity through the development of trusted digital identities and the widespread adoption of secure eServices.

The Alliance offers leadership and advisory services to governments and other public bodies; supporting the implementation of digital ID projects to accelerate the wide range of economic, public health, electoral and sustainability opportunities offered by the shift to digital service provision.

Its Board Members are 3M, Gemalto, Morpho (Safran) and Oberthur Technologies. For more information, visit: **www.secureidentityalliance.org**

Content

1.	**Foreword**	**1**
2.	**The role and value of trusted identity**	**2**
2.1.	What is identity?	2
2.2.	Trust and the individual	4
2.3.	The economic value of identity	4
3.	**Why mobile identity?**	**6**
3.1.	The unique value of mobile identity	8
3.2.	Multiple options to authenticate	9
3.3.	Higher level access	9
3.4.	Privacy, security and convenience	10
4.	**Who manages identity?**	**12**
4.1.	Role of government in creating the framework	13
4.2.	The role of the mobile operator	14
5.	**Mobile scenarios**	**16**
5.1.	mPublic services	16
5.2.	mCross border services	17
5.3.	mHealth	17
5.4.	mEducation	18
5.5.	Smart cities	19
5.6.	mVoting	19
6.	**Critical considerations**	**20**
7.	**Conclusion**	**22**
8.	**Bibliography**	**23**

1. Foreword

Digital identity is one of today's key strategic issues for governments, regulators and commercial organizations across the world.

In the developed world many citizens are now living and conducting their lives online. They are paying taxes, managing bank accounts, buying goods and services and engaging with friends on social networks.

But as the number of digital identities grows, so do the risks of identity theft and associated fraud. The challenge for all those involved in defining policy and delivering services is to ensure citizens are adequately protected online.

In the developing world many digital initiatives focus on establishing social security infrastructures to address poverty, protect vulnerable groups, and deliver effective and inclusive health and social care services. Even here, success depends on the need to prove identity.

Whether governments are seeking to protect citizens online, boost economic growth, reduce the spiraling costs of public services or extend social care initiatives, the platform must be a trusted digital environment.

This requires the development of innovative identity management solutions that extend beyond user name and password to offer greater privacy and protection, greater choice and convenient access to services wherever and whenever citizens need them.

Mobile identity represents a powerful platform through which to achieve these aims.

This paper offers a perspective from the GSMA and the Secure Identity Alliance (SIA) on the opportunities presented by mobile identity in support of governments as they unlock the potential of the digital economy; by driving trust and confidence in the adoption and use of innovative content and services.

2. The role and value of trusted identity

Throughout history the need to establish and verify identity has been critical to the social, political and economic development of nations.

At the most fundamental level, the planning and delivery of economic and social support programs relies on the government's knowledge of its citizens: who they are, where they live, their social and economic circumstances and so on. That knowledge often begins at birth, with registration, and this 'root' identity then follows citizens throughout their lives.

However, in many parts of the developing world this first step can be a challenge. Migrant populations, the illiterate or those who live in remote rural locations struggle to accurately register a child's birth – and as a result are excluded from taking advantage of basic services that provide a vital 'foundation for support'. Utilizing the mobile device to register births therefore offers a compelling opportunity for these countries to establish identity and then provide access to basic government services.

More broadly, mobile identity offers a means of extending access to a vast array of additional services, such as banking, payment, commerce and retail, healthcare but also transport, utilities and other advanced identity based digital services.

In this way secure digital identities can become the gateways to greater social welfare, fairer government and of course, economic growth.

2.1. What is identity?

Identity describes a set of unique characteristics or attributes that distinguish one individual from another. Typically those attributes are derived from name, date of birth, physical appearance and a variety of social factors including home address, occupation and so on. In many countries citizens are issued with identity numbers when they are born which continue to be used throughout their lives.

Verifying identity in the physical world has been a relatively straightforward task. Individuals present themselves, along with a set of government and/or service provider generated credentials – such as a passport or driving license – to the organization requiring proof of identity. With identity proven, access is granted or the transaction completed.

This concept of 'presentation' of identity hasn't changed as we move into the digital age however, the number of identities and where they are presented – whether physically or virtually – has changed.

With the value of the 'business to consumer' sector of the online economy worth in excess of $1 trillion[1], the vast majority of transactions are now carried out between parties where neither is physically present. In Finland, for example, over 99% of banking transactions are carried out online[2]. How then can consumers and service providers be confident in the validity of these types of online transactions?

1 Global ecommerce sales will top $1.25 trillion by 2013, Internet Retailer, 14 June 2012, http://www.internetretailer.com/2012/06/14/global-e-commerce-sales-will-top-125-trillion-2013

2 Source: Valimo Mobile IDCase Finland, 2012, http://2012.smartcardforum.cz/prezentation/ke_stazeni/06_Nemec.pdf Source: Valimo Mobile IDCase Finland, 2012, http://2012.smartcardforum.cz/prezentation/ke_stazeni/06_Nemec.pdf

The answer is to create a series of computerized tokens or 'proxies' that are imbued with the citizen's digital identities and 'presented' to the service provider to allow authentication. These range from simple username and password combinations, presentation via electronic data on smart cards, to using a mobile phone in combination with a Personal Identification Number (PIN) code and the SIM.

The proliferation of online services has led to the issue of 'volume' and multiplication of identities. Not all these identities are the same, and not all reflect a 'true' identity. For example, citizens may choose to protect their personal information by using pseudonyms to access services that do not require real world identities.

Typically identities used to access online banking and government gateway services are derived from strong registration processes that straddle the physical and virtual worlds. Citizens present their physical credentials such as birth certificates or passports, and are provided with the authentication tokens to enable online access.

Many other online services rely on self-registration – where citizens create their own user names and passwords to access webmail, social networks, news sites and eCommerce accounts.

However, estimates suggesting the typical online user (in developed economies) uses 26 different online user names but only five different passwords[3], presents an array of issues. First is the challenge of remembering 'randomized' names, passwords and PINs to access multiple services. Second is the security question of using such a small number of passwords – many of which can be easy for criminals to guess.

For example, the most commonly used password in the English-speaking world is password[4]. Similarly, the answers to password reminder questions – first pet, favorite food etc. – can often be easily found on citizen's social networking sites.

Moreover, the information provided to set up self-registered online accounts can be deliberately false. Citizens may use pseudonyms or provide incorrect birth date or mobile numbers to avoid giving away too much personal information.

Clearly there are challenges with online identity ranging from convenience through to trust. These are often well recognized, if not always acted on, by citizens.

While these present challenges for commercial organizations, they create potentially larger adoption and management problems for governments – for whom combining user convenience, trust and strong authentication are all crucial to the development of trusted online digital services.

3 Source: Warning about online fraud as information theft rises, BBC News, 17 July 2012, http://www.bbc.co.uk/news/technology-18866347

4 Source: Born to be breached: the worst passwords are still the most common, Ars Technica, 3 November 2012, http://arstechnica.com/information-technology/2012/11/born-to-be-breached-the-worst-passwords-are-still-the-most-common/

2.2. Trust and the individual

The issue of trust is fundamental throughout the digital ecosystem. Privacy is a major concern[5] of citizens when interacting with online service providers – from eCommerce and social media giants through to state-run digital portals.

To create an atmosphere of trust and assure the highest rates of adoption of public and private digital services, governments must address both real and perceived concerns to the benefit of their communities.

Doing so requires the creation, and public demonstration, of trust frameworks that address issues of privacy, transparency, control and accountability. Many such frameworks already exist – some are enshrined in data protection legislation, others in codes of conduct or contractual terms and conditions.

Governments, banks, mobile operators and online communities all maintain trusted relationships with their service users – to varying degrees of success. The challenge is to formalize and extend these to create trusted identity frameworks across an interdependent ecosystem.

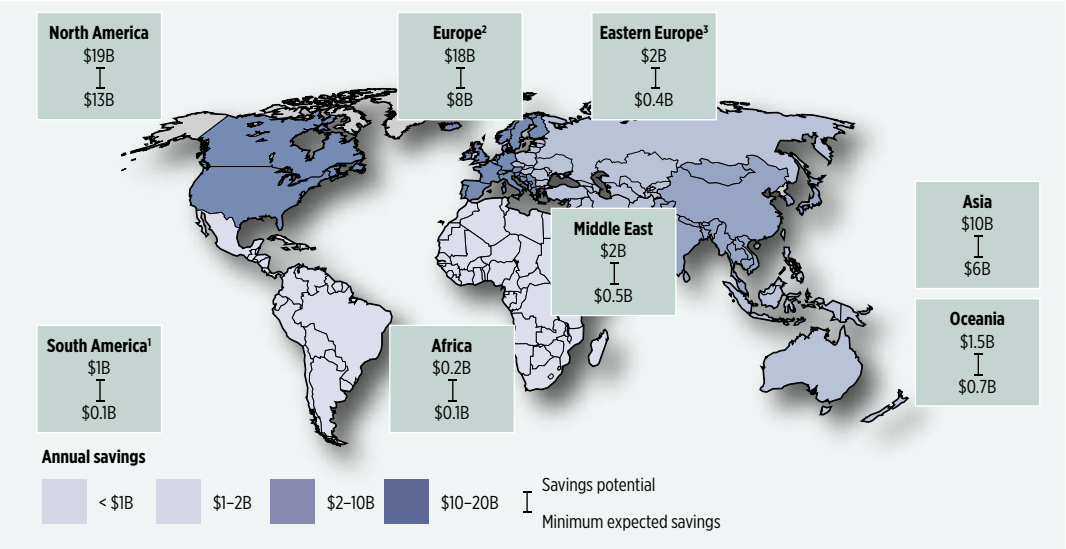
2.3. The economic value of identity

Governments and commercial organizations alike value trusted digital identities because without them the digital economy cannot function effectively.

In 2014, the findings of a joint research paper by the Secure Identity Alliance (SIA) and Boston Consulting Group (BCG) indicated that 'going digital' could offer governments across the globe up to $50 billion in annual savings by 2020[6].

Citizen self-service, automation, tax collection and digital signature were just some of the ways where a move into the digital economy could save money. However the true value of the digital economy extends beyond cost containment and reduction.

FIGURE 1: EGOVERNMENT YIELDS $30–50B ANNUAL SAVINGS BY 2020—ENABLED BY TRUSTED DIGITAL IDENTITY



Note: Savings measured vs. 2011, include interactions between government and citizens (excluding businesses) 1. South America, Central America, Caribbean
2. Western Europe, Central Europe, Northern/Southern Europe 3. Eastern Europe incl. Russia Source: SIA; BCG analysis; Economist Intelligence Unit; UN eGovernment survey 2008-2012

5 Source: Mobile Privacy: Consumer research insights and considerations for policymakers, GSMA, February 2014, http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf

6 Enabling the eGovernment 2020 Vision: the Role of Trusted Digital Identity, SIA & Boston Consulting Group, March 2014, http://www.secureidentityalliance.org/index.php/resources

As providers of essential online services to whole populations, governments can take the lead in promoting high value trust-based digital economic and social interactions; from extending eCommerce to empowering eDemocracy and personalized health services, through to the creation of an entirely new citizen-to-citizen economy in which private individuals can provide services to one another in a trusted environment where accountability and the rule of law exists.

An EU study by MICUS Consulting estimated the digital economy in Europe could contribute an increase in the annual economic growth rate of 1.09% across the 27 EU Member States . Other studies have analyzed the positive effect of digital identity on GDP, employment, tax, business efficiencies and other social factors such as the reduction of cybercrime and identity theft[8].

Governments across the world are certainly aware of the opportunities and a significant number have taken action. Canada, Finland, Estonia, Germany, India, Singapore, South Korea and UAE represent just a small number of the many governments who are taking advantage of new and existing physical identity infrastructures to create digital identities that underpin the establishment and adoption of successful digital public services.

"The only thing you can't do online is get married or buy a house! However, contracts for these activities can be generated online, ready for download and signature when you visit the public notary's office." **Annela Kiirats,** eGovernance Academy, Estonia

7 Source: The Impact of Broadband on Growth and Productivity, http://ec.europa.eu/information_society/ eeurope/i2010/docs/benchmarking/broadband_impact_2008.pdf

8 Sources: Cf. Álvarez Capón (2010): Catastro, politicas públicas y actividad económica, p. 16 or RSO, CapGemini, CS Transform (2009): Benchlearning: Study on impact measurement of eGovernment; BSG (2013) The value to our Digital identity http://www.lgi.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

3. Why mobile identity?

Mobile identity offers a range of intriguing, problem-solving opportunities for government. Indeed many are already moving in this direction.

In Estonia, for example, citizens have been using their mobile identity (Mobile-ID) to engage with over 400 public and private sector services since 2007[9]. These range from electronic banking, to applying for a driver's license, to entering or accessing academic grades at university or changing a pension plan. All services are completed using the electronic signature function of the mobile device - which holds legal equivalence to a physical signature.

In Sub-Saharan Africa, in Uganda[10], the mobile phone has become the enabler for the creation of physical identities by allowing births to be registered and communicated to the country's central registry office. Similar services operate in Senegal, Tanzania, Liberia and Kenya.

The United Arab Emirates meanwhile has announced plans to provide citizens with access to every public service via the mobile device. Mobile identity is the key enabler of this ambitious program, with the credentials of the Emirates National ID Card being tested with NFC-enabled phones and SIM cards[11].

These are just a small number of examples. Comparable services exist or are being planned across the world. However the key point is that mobile identity – provided via mobile networks and devices – delivers the catalyst to unlock tomorrow's digital economy.

It is important therefore to view mobile as part of a wider ecosystem when defining policy, and planning and implementing identity solutions, and the digital public services they support.

A mobile birth registration pilot[12] in Senegal, covering 30 villages and a population of around 50,000 people, saw 100% of births registered during the program - representing around 300 children over the course of two months.

9 Source: Estonia's Mobile-ID: Driving Today's e-Services Economy, GSMA, http://www.gsma.com/personaldata/wp-content/uploads/2013/07/GSMA-Mobile-Identity_Estonia_Case_Study_June-2013.pdf

10 Source: Mobile Birth Registration in Sub-Saharan Africa, A case study of Orange Senegal and Uganda Telecom solutions, GSMA, http://www.gsma.com/personaldata/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf

11 Source: Mobile Identity Global Review 2013, GSMA, http://www.gsma.com/personaldata/wp-content/uploads/2013/12/Mobile-Identity-Global-Review-2013.pdf

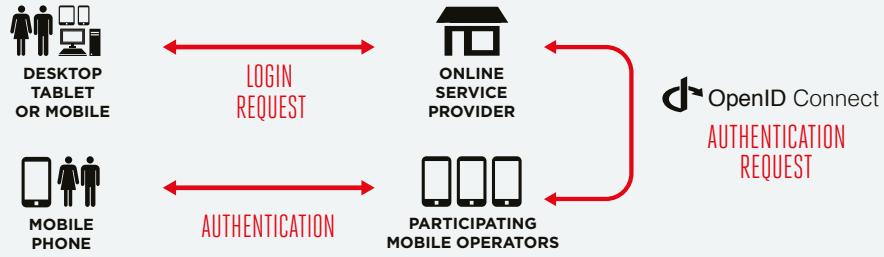
12 Source: Mobile Birth Registration in Sub-Saharan Africa, A case study of Orange Senegal and Uganda Telecom solutions, GSMA, http://www.gsma.com/personaldata/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf

Introducing Mobile Connect

At Mobile World Congress 2014, the GSMA unveiled the Mobile Connect initiative with the support of leading mobile operators. The GSMA Mobile Connect service will simplify consumers' lives, offering a single, trusted, mobile phone based authentication solution that respects their online privacy.

mobile connect

Mobile Connect services provide customers with the ability to authenticate and identify themselves remotely and securely via their mobile phone providing access to digital services. This opens up a range of opportunities for both mobile operators and consumer-focused service providers, like governments, to build a rich suite of offerings for their customers, while ensuring the user's private and confidential information is kept safe.



- **For consumers, Mobile Connect ensures that authentication is provided by the operator to the service provider with no personal data shared without their permission. This will enhance user privacy, reduce the risk of identity theft and simplify the login experience for a range of services by leveraging the established data handling processes of the operators and inherent security of the SIM for authentication and identification. With a streamlined, secure log-in, consumers will have easier access to retail, government and banking services, among others, without the need to remember additional passwords.**
- **For service providers, Mobile Connect will offer the advantages of an improved consumer experience, including reduced drop-off rates when signing on to new services; lower cost of managing credentials; and validation of important consumer attributes such as age.**

The technology behind Mobile Connect is based on the widely adopted open source technology of OpenID Connect, which provides a single interface for service providers to connect with mobile operators.

With operators well placed to offer identity services due to their assets such as the SIM card, strong customer registration process, authentication, fraud detection and mitigation processes - Mobile Connect offers a compelling proposition for government and private organizations seeking to deliver secure, digital identity-based services.

Visit **gsma.com/personaldata** for more information

3.1. The unique value of mobile identity

Mobile offers a compelling proposition for governments seeking to provide secure access to digital services. It provides an ideal platform for creation, storage and management of digital identity thanks in part to the sheer number of devices worldwide. With 6.99 billion connected mobile handsets[13], the mobile is the most ubiquitous telecommunications medium on the planet. With accessibility key to the success of digital services, it makes sense to leverage this technology.

This challenge is greater than simply addressing accessibility, security is a central consideration. The SIM card, encrypted and part of every mobile device, is arguably the most secure technology on which to store identity credentials. Additionally, mobile identity can provide high security assurance in combination with other existing online and digital infrastructures and technologies.

In over 30 years of live operation the SIM card has been, and continues to be, continuously monitored and updated with advanced security and the latest encryption algorithms. The SIM is also viewed as personal to the user, can be taken everywhere with them, and is transferable between devices.

13 Total number of mobile connections, excluding M2M, at the end of Q3 2014 was 6.99 billion. Source GSMA

3.2. Multiple options to authenticate

Mobile identity solutions are also flexible in terms of how they can deliver a wide range of applications and use cases. In particular, mobile identity can differentiate from existing authentication and digital identity services by providing solutions that improve user convenience while maintaining security, and by providing the user with control through both the SIM and the device.

From a user perspective, a federated identity model brings together the citizen's multiple digital identities from distinct identity management systems. For service providers having a single point of contact with mobile operators (acting as identity providers) allows them to offer a convenient, mobile based authentication solution to their customers. This option is considerably easier – and inherently more secure – than the standard username and password option.

Within this model, a single set of credentials (a single digital identity) can be used across multiple IT systems or websites, rather than the user having to register and remember credentials for each. The user provides their mobile phone number upon registration for the service; this number is then used to route a challenge to their mobile phone either to Click OK to authenticate or to enter a PIN as an additional security measure. If the prompt is correctly completed, the authentication is confirmed with the website and access is granted.

This process can be even shorter for users accessing digital services when browsing on their mobile device over the mobile network, the authentication process can occur seamlessly and instantly.

3.3. Higher level access

Where a higher level of security is required – for access to government, banking or health services for example – the mobile again offers significant opportunity through its ability to support higher factor authentication.

Recent innovations in device technology allow two factor authentication to become three or four-factor – by adding 'something I am', for example, the user's location or biometric data.

For very strong authentication use cases, for example when a legally binding proof of authentication or authorization transaction is required, the introduction of mobile signature based on PKI (Public Key Infrastructure) technology adds robust identity proofing and the generation of digital signatures for identity validation.

3.4. Privacy, security and convenience

With universal adoption of digital public services uppermost in the minds of policy makers, the need to combine security, privacy and usability into any form of digital identity is paramount.

Privacy is a central tenet of any digital or mobile identity service. Citizens are concerned about where and how much of their data is being captured when using online services. A global poll by the GSMA found over 80% of mobile users expressed concern over sharing personal data, and believed it was important to give permission before data was used[14].

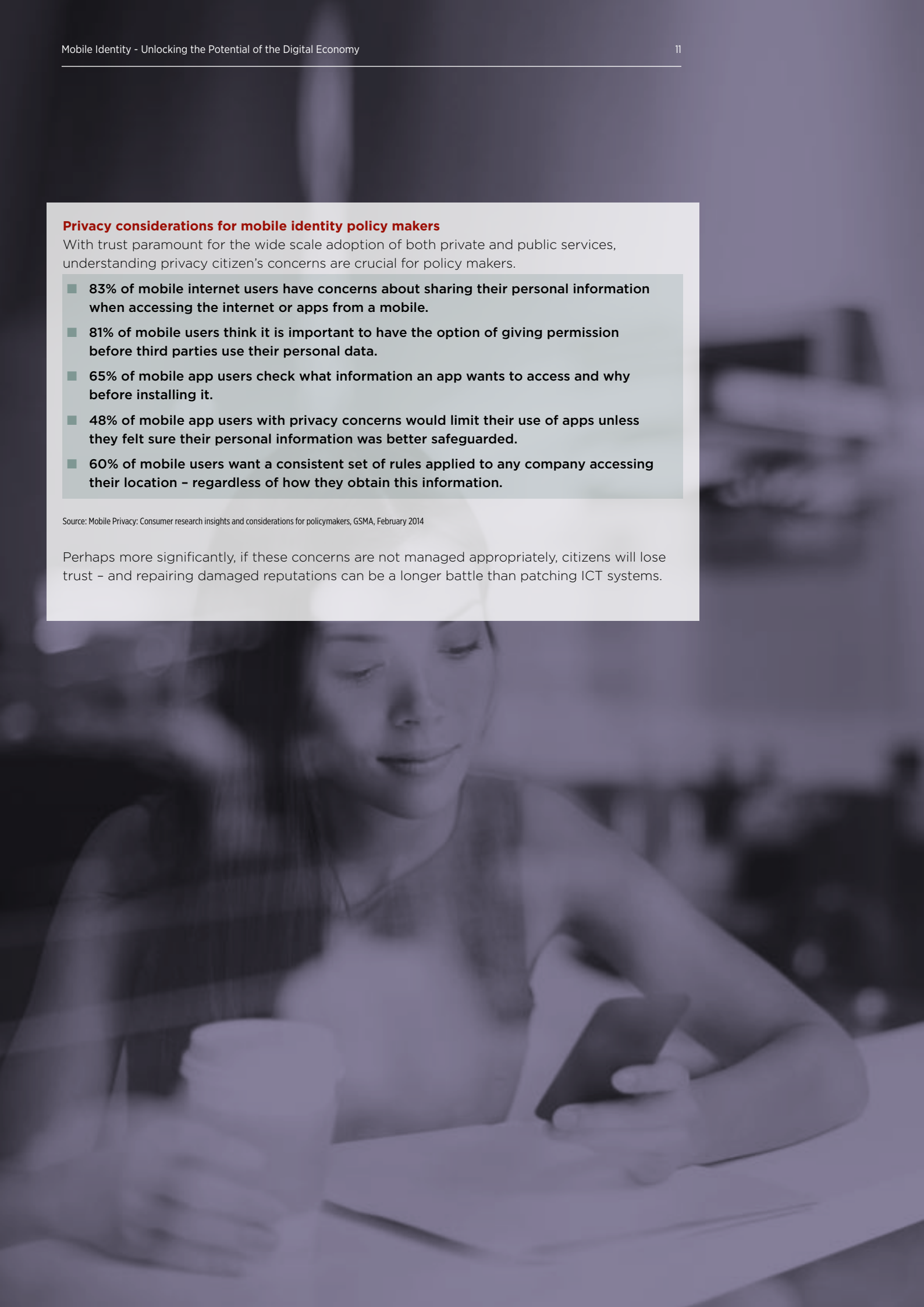
Citizens often associate their mobile numbers with their identity. Lawmakers, including the European Union, agree and have ruled that citizens have specific rights over their mobile numbers. Calling Line Identity Prevention already restricts the appearance of a mobile number during a call, and this ability to present or withhold the identity is now culturally embedded.

Extending protection into the digital world through mobile identity solutions is a natural extension of these voice call rights. Mobile operators, for example, are going to great lengths to protect privacy. The GSMA, which is proposing to use the OpenID Connect from the OpenID Foundation, has also defined a mobile profile that provides a Pseudo Anonymous Customer Reference (PCR) instead of the real identifier to the third party service providers. The concept is to share a token (i.e. the PCR) when the user is authenticated – rather than actually sharing any data.

It is therefore clear that understanding the barriers to online activity is crucial to inform the planning and delivery of digital public services.

However, any form of privacy and security protection must not detract from the citizen's digital experience. Too long or complex an authentication process and citizens will avoid the service. Authentication that is too weak results in government service providers risking the onerous consequences of criminal attack.

14 Source: Mobile Privacy: Consumer research insights and considerations for policymakers, GSMA, February 2014, http://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_insights_and_considerations_for_policymakers-Final.pdf



Privacy considerations for mobile identity policy makers

With trust paramount for the wide scale adoption of both private and public services, understanding privacy citizen's concerns are crucial for policy makers.

- **83% of mobile internet users have concerns about sharing their personal information when accessing the internet or apps from a mobile.**
- **81% of mobile users think it is important to have the option of giving permission before third parties use their personal data.**
- **65% of mobile app users check what information an app wants to access and why before installing it.**
- **48% of mobile app users with privacy concerns would limit their use of apps unless they felt sure their personal information was better safeguarded.**
- **60% of mobile users want a consistent set of rules applied to any company accessing their location – regardless of how they obtain this information.**

Source: Mobile Privacy: Consumer research insights and considerations for policymakers, GSMA, February 2014

Perhaps more significantly, if these concerns are not managed appropriately, citizens will lose trust – and repairing damaged reputations can be a longer battle than patching ICT systems.

4. Who manages identity?

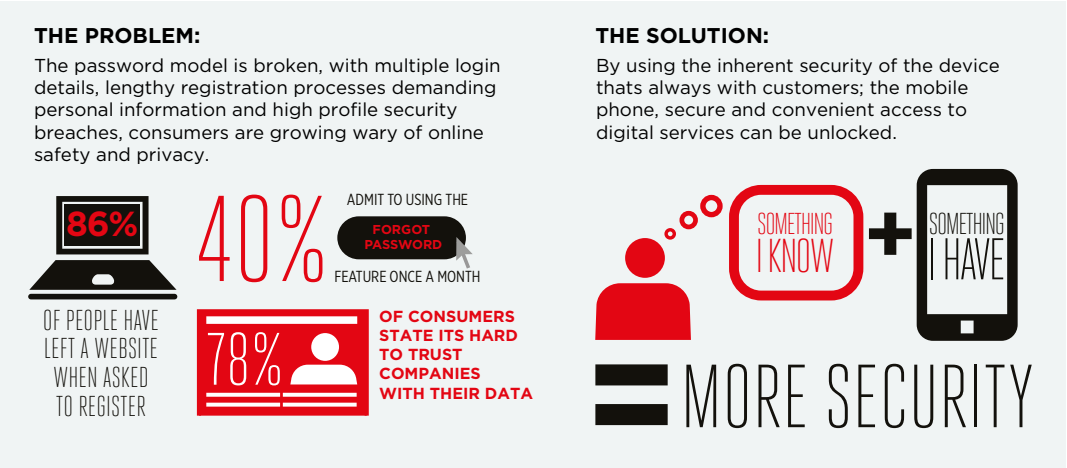
With the multiplication of digital identities, and the raft of online social sign-on services now being offered by the major internet players, questions of identity ownership, provision and management come to the fore.

Ultimately, ownership of identity / identities is the preserve of the individual. Whether physical or virtual, the fact that ownership resides with the individual citizen is the critical starting point for any digital identity journey.

But ownership is just part of the story. Citizens using both public and private digital services require the ability to manage their identities.

Identity is an intensely personal issue and individuals see it as core to themselves and not something to be traded. Citizens are, of course, aware that some of their data is being used in a commercial context. For example, while many accept some degree of data sharing in exchange for a free social networking service, they are often confused as to what data is going where. 78% of consumers state that they find it difficult to trust companies with their data[15].

FIGURE 2: AS DIGITAL SERVICES CONTINUE TO INCREASE IN IMPORTANCE, MOBILE PHONE ENABLED SECURE AND CONVENIENT ACCESS BECOMES FUNDAMENTAL



Governments and other stakeholders – among them banks and mobile operators – have key roles to play in creating the trust frameworks and the mobile identity solutions that will breed confidence among users.

15 Source: http://www.gsma.com/personaldata/wp-content/uploads/2014/08/GSMA-infographic_web.pdf

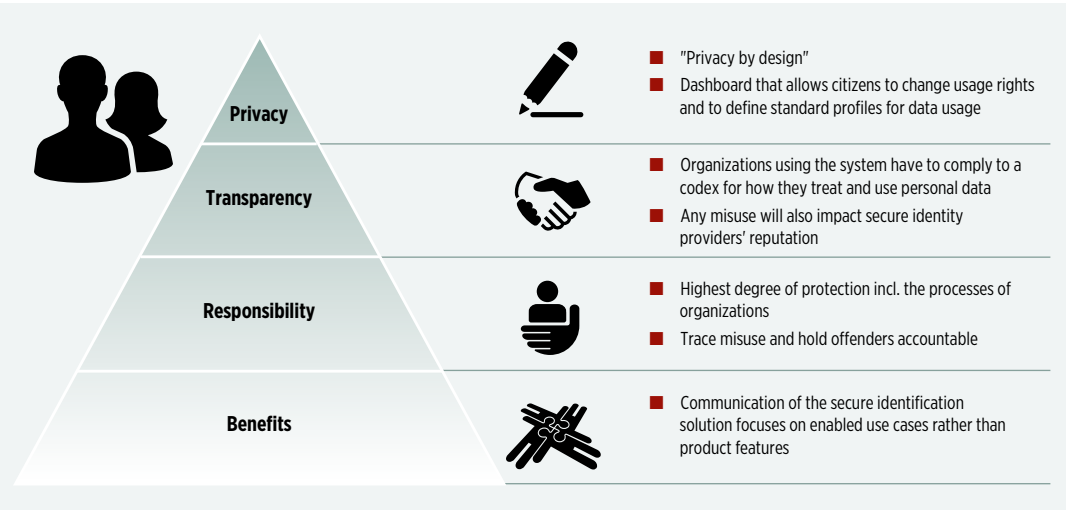
4.1. Role of government in creating the framework

While governments can act as service providers, they also carry a wider responsibility for fostering and helping to create the trusted environment or framework within which public and commercial service providers, and a new crop of identity providers, will operate.

SIA and BCG believe the following guiding principles must underpin digital identity[16]:

- **Protecting citizens/consumers; building in 'privacy by design' to give citizens/consumers privacy controls and options that including the ability to change access rights.**
- **Transparency; organizations must be fully accountable for a trusted flow of data, adhering to clearly defined codes on how they work with and use personal data.**
- **Responsibility; organizations are responsible for safeguarding data relating to digital identity.**
- **Communication; the benefits of any secure identification solution need to be communicated clearly to users in order to empower consumers and assure appropriate data usage.**

FIGURE 3: IMPLICATIONS FOR TRUSTED DIGITAL IDENTITY



How governments choose to establish these trust frameworks is largely dependent on the maturity of existing identity infrastructures and the cultural, legal and political environments that are particular to each nation state.

For example, some countries, including the Sultanate of Oman (the first smart card-based national ID solution deployed in the Middle East), the United Arab Emirates, and Estonia favor an identity framework based on national digital identities. Here the government acts as the primary provider of the identity.

16 Enabling the eGovernment 2020 Vision: the Role of Trusted Digital Identity, SIA & Boston Consulting Group, March 2014, http://www.secureidentityalliance.org/index.php/resources

In another scenario, identity is delivered via a hybrid federated identity model where both public and private certified providers deliver full registration and management. In Norway, for example, its single sign-on portal gives citizens access to over 270 service providers[17], including major banks and numerous other commercial organizations, and supports multiple levels of authentication that includes PIN code authentication tokens, certificates stored in USB pens and via the mobile, using the via the Mobile BankID service. Sweden, Finland and Singapore also take a similar approach.

In contrast, countries including the UK and the US currently have no national identity schemes, and are looking to a more open identity framework. Here governments play an enabling role – creating the environment in which to allow private and public organizations (banks, mobile operators etc.) to manage identity for citizens, businesses and consumers.

Ultimately, the choice of model rests with the individual government.

4.2. The role of the mobile operator

Among the many potential mobile identity providers, mobile operators are well positioned to provide digital identity services.

First and foremost is access to the SIM. While mobile identity credentials can certainly be stored on other secure elements within the device, the SIM benefits from a more stringent and globally accepted standardization environment and ubiquitous deployment across the world.

With regulation as a key element of the trusted framework, the local incorporation of every mobile operator, and the fact their business derives from a state-issued license makes them responsible and accountable to both customers and regulators.

The scale and reach of the mobile operator, its customer billing relationship and its fraud detection capabilities present an ideal platform for strong registration processes. And, of course, operators have established, sophisticated and qualified customer care processes, designed solely to resolve issues and problems for customers. This is particularly attractive for governments who often lack this level of support infrastructure.

It is also important to note that mobile users around the globe primarily look to their mobile operators for help when their privacy is invaded. In the UK, for example, nearly half of consumers polled see mobile operators as a likely provider of mobile identity services[18].

FIGURE 4: MOBILE NETWORK OPERATORS KEY ASSETS

Mobile network operators are uniquely positioned to provide trusted login and identity authentication on behalf of their subscribers.

17 Source: Gemalto, http://www.gemalto.com/press/Pages/news_1862.aspx

18 Source: GfK/GSMA Mobile Identity Study. May 2013, http://www.gsma.com/personaldata/wp-content/uploads/2013/12/Mobile_Identity_UK_Research_Infographic.pdf

5. Mobile scenarios

Mobile identity can provide the gateway to a vast range of government and public services. This section takes a broad look at current and future public service use cases where planning and deployment is predicated on trusted, secure mobile identities – allowing registration, secure authentication and access by citizens.

5.1. mPublic services

Identity plays a key role in enabling the creation and deployment of public services. From taxation to customs declarations and submissions, mobile identity is transforming how citizens and governments interact.

In Finland, the city of Helsinki[19] is using mobile technology to engage with citizens and to deliver innovative public services. For example, a new tax receipt app now allows citizens to calculate the total amount of direct or indirect taxes they pay monthly.

In Estonia, Mobile-ID[20] users can access a vast array of public services. Citizens can submit tax returns, apply for a driving license, register a motor vehicle with Road Administration and register a new company. Mobile-ID also provides access to personal information - from health insurance and disability assistance to school benefits and construction applications – from the State Agency for Information System.

Moreover, by extending public / partnerships, citizens can apply for personal loans, purchase insurance and pay their utility bills – all through the Mobile-ID system.

While these northern European countries are certainly much more advanced in mobile public services provision, the paper has already highlighted examples of simpler identity based services – including birth registration in sub Saharan Africa[21].

19 Source: http://www.gsma.com/connectedliving/wp-content/uploads/2012/12/cl_forum_virium_12_12.pdf

20 Source: e-Estonia.com and e-Estonia.com and Estonia's Mobile-ID: Driving Today's e-Services Economy http://www.gsma.com/personaldata/estonias-mobile-id-driving-todays-e-services-economy, GSMA

21 Source: Mobile Birth Registration in Sub-Saharan Africa, A case study of Orange Senegal and Uganda Telecom solutions, GSMA, http://www.gsma.com/personaldata/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf

5.2. mCross border services

Mobile identity solutions are making it possible for citizens and businesses to deal with public administrations in other countries too – taking advantage of online e-government services in the same way as resident individuals and companies.

By simplifying the administrative formalities involved in setting up a business in a new territory or establishing a new branch office, national governments are 'open for business', creating a framework that enables ease of participation in the wider global economy while streamlining the delivery of services to nationals and non-nationals alike.

Looking at Estonia again, its national Mobile-ID[22] service is already helping to boost export and trading activities with Lithuania and Azerbaijan. Enabling companies to set up in just minutes, the service also gives non-nationals residing in the country access to local citizen m-ID sign-in services so they can participate in key infrastructure services, such as DigiDoc and banking applications. This non-resident 'investor passport' approach enables satellite citizenship that's set to attract investment and creates the potential for 'digital embassies' in friendly foreign countries.

In Europe, the electronic identity, authentication and signature (eIDAS) Regulation[23] recently entered into force on the 17th September 2014, and is expected to enable seamless electronic transactions across borders and foster the use of mobile identity solutions across the Digital Single Market. The regulation will make it easier and safer for individuals, businesses and public administrations in different EU countries to identify and authenticate themselves, sign documents and check the authenticity of documents online.

5.3. mHealth

Mobile identity is transforming the delivery of healthcare and well-being for patients and practitioners alike, by enabling patients to manage their own health, access anytime-anywhere supportand benefit from more accurate diagnoses by healthcare professionals.

A key requirement in many healthcare situations is the ability to reliably identify both patients and carers. Mobile identity allows them to do just that; enabling patients, practitioners and providers to prove who they are online much more securely and conveniently than conventional sign on passwords.

Moreover, mobile devices allow patients to share and access their own data, monitor and manage their health via a variety of wellness and health applications anytime, anywhere, in ways that support quick and more accurate diagnoses by healthcare professionals.

For example, in the UK, the South London and Maudsley NHS Trust[24] uses mobile technologies to enable care workers to treat more patients in their own homes. By giving patients mobile devices and secure remote access to information and removing the barrier of travel to a clinic, the Trust has been able to reduce the number of clinic sites it operates from over 100 to less than 70, while simultaneously increasing the number of appointments delivered.

22 Source http://www.secureidentityalliance.org/index.php/resources, Visit Report – eServices in Estonia

23 Source: eIDAS Regulation (EU) No 910/2014 of 23 July 2014 – OJ L257, 28 August 2014 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

24 Source: http://www.o2.co.uk/enterprise/sectors/public-sector/health

5.4. mEducation

From sustainable mobile learning services to collaborative multi-sector education partnerships between governments, foundations, technology providers and schools, mobile identity is enabling wide-ranging education initiatives.

mEducation provides students, teachers, employees and all learners with the ability to learn anywhere, anytime and on the move with educational content made available over mobile networks to devices such as tablets, smart phones and feature phones.

Not only does this represent a powerful shift in the way education is delivered and received, it also offers opportunities to enhance teaching and assessment, and to streamline educational administration and management via mobile technologies. And as with all digital public services, confirming identity and enabling secure access is critical.

In Tunisia, for example, where 30% of young people below the age of 30 are unemployed, a new program is stimulating skills and employment opportunities for the next generation. The Najja7ni mobile learning service[25] now gives children and young people in remote areas, as well as disadvantaged youngsters in urban areas, the chance to learn Mathematics, Sciences, Arabic, French and English.

Today 2.5 million learners are using the service – which is designed to be accessible even when a handset has no credit. Najja7ni also delivers the region's first career-related mobile employment service that connects young people without internet access to employability resources, vocational guidance, financial inclusion and job opportunities via a basic handset. Around 1 million young people use the service to tap into labour market and training opportunities, access career guidance and post CVs.

25 Source: http://www.gsma.com/connectedliving/wp-content/uploads/2014/02/2013-2014-Q4-Tunisiana-Najja7ni-services.pdf

5.5. Smart cities

City administrations are looking to harness mobile connectivity to address the many challenges of urbanization, including traffic congestion, waste disposal and rising energy usage. These Smart City initiatives are helping to improve quality of life for citizens, make public services more efficient and fuel economic growth.

From loyalty programs, to public transport ticketing, mobile technologies are making it easier to travel. Dubai, for example, has become the first city in the Middle East where people can use their mobile phones to access public transport[26].

The service makes it possible for passengers to open a ticket barrier simply by tapping their handset against a reader. Using NFC (Near Field Communications) to connect the handset and validate the passenger's 'virtual account', commuters can check in and out of buses, metro stations and water taxis, prompting the appropriate fare to be deducted from their credit account.

In Germany, the focus is on reducing carbon emissions and energy consumption. The municipal government of Friedrichshafen[27] has developed an initiative to reduce energy consumption by bringing together communication technologies with a smart energy grid to deliver electricity consumption data to households so they can regulate their usage and lower impact on the environment.

5.6. mVoting

Trusted digital identities make it easy for citizens to verify and confirm who they say they are – giving them the security, convenience and flexibility they need to vote in local, regional and national elections.

With a national identity program in place, governments are able to authenticate voter identity and eligibility to vote i.e. 'Is this person over 18', and manage voter registration, as well as ensure remote populations are not disenfranchised. It also provides a route to eliminating potential voter fraud and enabling a more representative electoral result.

While both mVoting and eVoting offer compelling opportunities these are not yet widespread solutions. However, in 2011, Estonia became the first country in the world to allow mVoting in the national parliamentary elections where 3% of all votes cast were submitted via mobile[28]. As digital initiatives across the world become more mature, it is likely the provision of mVoting services is likely to increase.

26 Source: http://www.gsma.com/connectedliving/wp-content/uploads/2014/02/cl_sc_dubai_medres_01_14.pdf

27 Source: http://www.gsma.com/connectedliving/wp-content/uploads/2012/11/cl_tcity_web_10_12.pdf

28 Source: Estonian Information Systems Authority, August 2011, https://www.ria.ee/facts-about-e-estonia/

6. Critical considerations

There are, of course, some significant challenges to be addressed if governments are to be able to fully unlock the potential of the digital economy through the successful implementation of mobile identity solutions.

Mobile identity is at the core of a digital society and the entire emerging identity management ecosystem has a significant role to play in building trust in the digital economy. However, ensuring the benefits are realized will require consistent approaches. This consistency will be necessary in order to ensure the safe and secure use of data and identity management services, and to drive consumer confidence and trust.

Governments too are playing a key role in unlocking the potential benefits by providing digital public services and accordant applications to the mass market, paving the way for further service digitization to the benefits of citizens, businesses and consumers.

However, mobile identity should also be seen as a way for users to get access to a wide variety of digital rights and for more general online transactions and activities.

Legal and regulatory clarity and certainty within the mobile identity ecosystem are crucial to avoid hindering industry's willingness to invest. Policy makers should ensure that pro-investment policies are sustained, and harmonization and compatibility between regulations and self- regulatory models encouraged. This will not only provide more legal clarity, but will also ensure interoperability and cooperation between key stakeholders in the mobile identity ecosystem.

The protection of privacy and security is another key issue, and industry, government and regulators need to work closely together to clarify their roles and responsibilities. Equally, mobile operators and other service providers who aspire to become providers of trust and convenience for citizens and consumers should drive the application of good principles of privacy and security such as privacy by design, identity portability, accountability and education for consumers and citizens.

Users need to understand the role of mobile identity and how it works in reality. They also need to increase their awareness and knowledge of the information they are sharing, and with whom, to strengthen trust. Both governments and industry stakeholders should work together to raise awareness and encourage understanding.

Standardization is a key step to achieve interoperability. If identity solutions are to be used across national borders, applicable open standards and best practices for consumers and industry players must be adapted accordingly. There are various industry groups already working towards a common set of specifications but the market needs standards that embrace business process issues around assurance, privacy, and liability. As regulations and policies around these are finalized mobile identity can become an even stronger foundation for trust among all parties exchanging information.

Fundamentally, electronic, digital and mobile identities are intangible, which makes them difficult for service providers, citizens and government to understand, use and manage. Legislation and regulations are important as a means of making sure that the identity authentication standards that are defined and the solutions that are adopted are appropriate.

Ultimately mobile identity solutions must be easy to use, fundamentally secure and private, and they must promote interoperability and the establishment of trust. This is, of course, no small matter, but it is essential that policy makers play their part, so as to ensure that individual countries' and societies benefit most from the continued emergence of online activities, while minimizing their attendant risks.

7. Conclusion

Ultimately, the incredible value of digital services to state institutions and citizens, as a means of assuring greater social protection and to drive adoption of online services in the wider economy, is dependent on developing and delivering trusted digital identities.

Figures from SIA and BCG projecting identity-based digital public services will deliver $50 billion in projected annual cost savings by 2020 are significant. However, the analyst expects the wider economic benefits to reach $522 bn by the end of the decade[29].

There's little doubt mobile provides a compelling medium to deliver on these numbers. However mobile identity should not be viewed as a separate solution, but as an integral and essential component to any digital identity strategy. In effect, provision for mobile service delivery and authentication should be built in to every plan and policy decision.

However all activity must be predicated on the principle that identity is, by definition, uniquely personal and owned and managed meticulously by the individual. Citizens therefore need the tools to do so. Clear online dashboards, where users view and manage their multiple identities combined with simple to use solutions, will allow the mobile device to become a powerful and convenient point of identity management and control.

Governments and state-run institutions have a key role to play in the context of digital service provision and also driving secure, trusted and easy to use authentication and access via the mobile phone. In addition to acting as service providers, governments also have a responsibility to develop the frameworks in which mobile identity and its ecosystem of providers and users can thrive.

These frameworks must be flexible and technology neutral, in order to encourage consistent approaches, to remove barriers to entry and reduce complexity of design and costs. Crucially, they must establish trust across services and among all stakeholders.

Governments, citizens and economies across Europe, the Middle East, Africa and Asia are already enjoying the wide-ranging benefits of their own mobile identity programs. The next stage of implementation promises to increase the scale, reach and complexity of mobile identity-supported digital public services. With governments and the industry ecosystem cooperating effectively, the social and economic value will only increase with time.

29 Enabling the eGovernment 2020 Vision: the Role of Trusted Digital Identity, SIA & Boston Consulting Group, March 2014, http://www.secureidentityalliance.org/index.php/resources

8. Bibliography

- Abdul Montaqim, Internet Retailer, June 2012
- Valimo Mobile ID, Complementing the national citizen eID with Mobile ID, May 2012
- BBC News, Warning about online fraud as information theft rises, July 2012
- Sean Gallagher, ars technica, Nov 2012
- GSMA, Mobile Privacy: Consumer research insights and considerations for policymakers, Feb 2014
- European Commission, The Impact of Broadband on Growth and Productivity, 2008
- Boston Consulting Group, The Value of our Digital Identity, Nov 2012
- GSMA, Estonia's Mobile-ID: Driving Today's e-Services Economy, June 2013
- GSMA, Mobile Birth Registration in Sub-Saharan Africa, A case study of Orange Senegal and Uganda Telecom solutions, April 2013
- GSMA, Mobile Identity Global Review, Feb 2013
- GSMA, Mobile Identity: A Regulatory Overview, Feb 2013
- GSMA, Personal Data Infographic, 2014
- Gemalto, BankID deploys Gemalto's Valimo Mobile ID solution nationwide in Norway, May 2014
- GfK/GSMA, Mobile Identity Study, May 2013
- GSMA, Finland: Forum Virium Helsinki, Dec 2012
- GSMA, Estonia's Mobile-ID: Driving Today's e-Services Economy, July 2013
- SIA, eServices in Estonia: a success story, June 2014
- O2, O2 Solutions for Health, May 2014
- GSMA, Najj7ni: Mobile learning services for improving education, English language skills and employment opportunities in Tunisia, Feb 2014
- GSMA, Smoother, Smarter Transport in the UAE, Jan 2014
- GSMA, Germany: T-City Friedrichshafen, October 2012
- SIA / Boston Consulting Group, Enabling the eGovernment 2020 Vision: the Role of Trusted Digital Identity, March 2014

Floor 2,
The Walbrook Building
25 Walbrook,
London EC4N 8AF UK
Tel: +44 (0)207 356 0600

personaldata@gsma.com
www.gsma.com