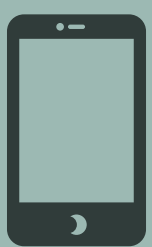
Personal Data

Mobile Identity

A Regulatory Overview

Second edition

January 2015



Introduction

This paper is the second edition of the paper published by GSMA in February 2013 which provided the regulatory overview of the GSMA mobile identity services. The paper provides a review of the regulatory background and key policy issues associated with digital and mobile identity services. The objective is to inform and stimulate discussion on the key policy principles required for the successful development of mobile identity services.

The paper forms part of a broader series of mobile identity related documents published by the GSMA Personal Data Programme including technical white papers, case studies and service blueprints. For more information, please visit **www.gsma.com/personaldata.**

Background

Digital identity is often defined as the set of electronic credentials or attributes required in order to gain access to a particular service or resource in the real or virtual world. However, definitions of digital identity may vary according to different regulatory contexts. For example, under the new European Union (EU) Regulation on Electronic identification and Trust services for electronic transactions in the internal market (also known as eIDAS Regulation)[1] it is defined as *"the process of using personal identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person".*

Mobile identity is essentially an extension of digital identity provided via mobile networks and devices – for example via SIM-based solutions or by using mobile devices, user's attributes and credentials to form part of a personal identity.

Examples of mobile identity services range from the provision of authentication solutions that allow secure access to online personal and financial data to the identification of the user for higher security services, such as e-government, e-health, digital payments and online banking. For the latter the use of second and multiple factor authentication technologies or mobile signature solutions based on Public Key Infrastructure (PKI) add robust identity proofing for identity validation.

Mobile represents an ideal platform for digital identity based services not only due to its capability to provide these services on the move (wherever a user takes his or her handset) and through a secure medium, but also because of mobile technologies such as Near Field Communication (NFC). NFC-enabled service examples include providing users with authenticated access to physical buildings, facilities and borders through their mobile, and access to transport systems, m-ticketing and domestic utilities[2].

Digital identity, the digital economy and the importance of trust

Digital identity is increasingly recognised as a key enabler of the "digital economy"[3] and as such is becoming progressively important to governments and regulators. An EU study by MICUS consulting indicated that the digital economy in Europe could contribute an increase in the annual economic growth rate of +1.09% across the EU 27 Member States[4]. Other studies have analysed 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[5]. A more recent study by Boston Consulting Group[6] has also indicated that 'going digital' could offer great advantages to governments across the globe conserving up to $50 billion in annual savings by 2020. In the same study, the wider economic benefits are expected to reach $522 billion by the end of the decade.

Building "trust" online is critical to facilitate the growth of digital identity services and digital economies as a whole, and is a preoccupation of governments and regulators around the world. "Trust is a must, and we have to have trust if the full value of the digital environment is to be utilised" stated the new European Commission's Vice President responsible for the Digital Single Market; Andrus Ansip, during his first Parliamentary hearings in October 2014[7].

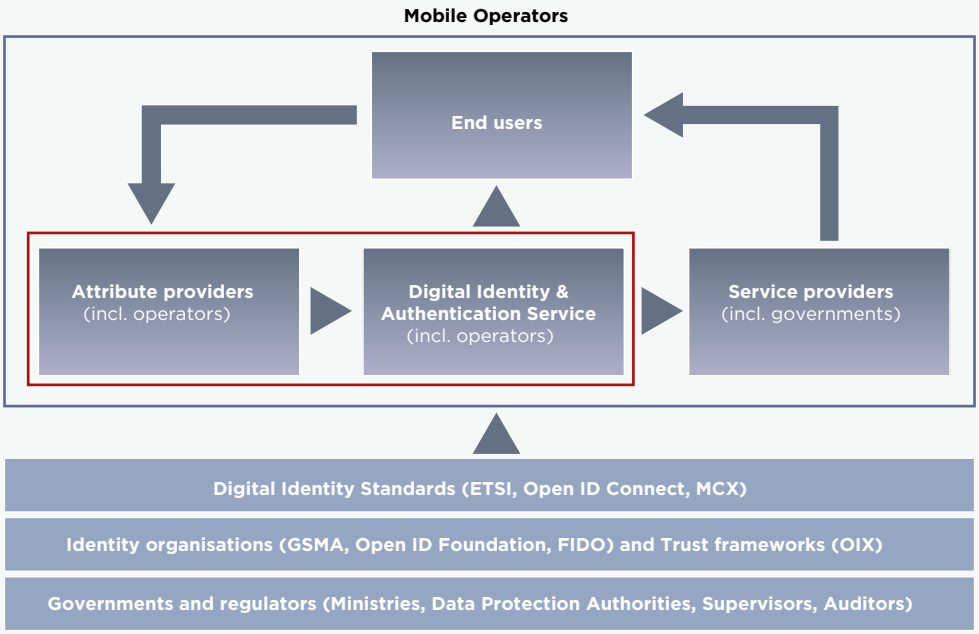
Trust is at the heart of digital identity which is a key tool in the context of delivery and consumption of electronic interactions between parties including consumers, governments and the private sector. In order to provide digital services, companies and public administrations need to distinguish between trusted and non-trusted counterparts in cyberspace; they also need to be recognised as trusted parties themselves. Likewise from a consumer perspective, as they provide increasing amounts of sensitive identity data in order to access online services, they require stronger authentication methods (beyond simple username/password schemes) and are increasingly demanding more security, privacy and safer online environments.

By providing assurance regarding the identity claimed by parties engaged in an online relationship or transaction, digital identity reduces uncertainty inherent in transactions at a distance. This facilitates the migration of economic and social interaction online and releases the benefits of innovation to create trust based digital services.

Market players and key stakeholders

The digital identity ecosystem is increasingly complex, with a wide range of business models and participants operating at different points in the value chain with diverse roles, interests and priorities.

DIGITAL IDENTITY VALUE CHAIN AND THE ROLE OF MOBILE OPERATORS



- End users or consumers of both commercial and e-government identity services have their own unique digital identities or credentials. As such they should have the ability to minimize and contextualise the data used to authenticate themselves or be recognised online, and be assured the environment is secure, anonymous and safe.
- Service providers (SP), or 'relying parties', are organisations such as online retailers, banks, governments or health providers that require proof of identity and information about the users in order to grant them access to a service or resource. A service provider would outsource the credential and/or identity management to one or more authentication or identity providers (e.g. mobile operators). Upon receiving the user request to login via their chosen method, the authentication provider validates the user, and the confirmation of this is relayed to the Service Provider who can then grant access.
- Attributes providers typically hold verified data on users (name, date of birth, gender, age, address, phone number, etc.). These attributes might relate to the user or, in the case of mobile operators, to the user's SIM account (such as pre vs. post-pay). Attribute providers can be banks, mobile network operators, governments, or even social networks. They either sell attributes to other parties, or verify that a piece of data on a certain individual is true. An attribute provider must ensure they comply with national laws on data protection and privacy, and generally obtain a user's consent before disclosing their personal data.

- Digital identity providers assert the identity of the user to the service provider and take responsibility for the authenticity of that identity based on identity proofs already validated for the individual. In practice, they manage the user's credentials, and can be clients to attribute providers, to ensure that the user is who he/she says they are, and has the attributes he/she claims to have. In mobile and electronic signature implementations, trust service providers or certificate service providers (as they are defined in the eIDAS Regulation in Europe) play a critical role in issuing digital certificates for electronic identification and for other services. They enable a user to digitally sign a consent, authentication, and authorisation request hence providing a non-repudiation audit trail for the relevant service or transaction.
- Digital authentication providers merely check that a user has the right to lay claim to an identifier. They perform the same tasks as digital identity providers, but without knowing who the individual is, i.e. they only match the user with an account. The individual remains anonymous to them and to the service provider, and his/her attributes are not known or shared. The pseudonymous customer reference used for the GSMA Mobile Connect[8] solution is an example of a digital authentication provider[9]).
- Digital identity standards (such as Open ID Connect[10]) provide a set of authentication protocols that help build interoperable authentication technologies. They are often developed by not-for-profit organisations, such as Open ID Foundation, FIDO Alliance[11], etc., who want to help build open, scalable, interoperable and robust identity solutions.
- An important role is also played by Trust frameworks, such as the Open Identity Exchange (OIX)[12], which are large scale networks made up of multiple participants in the identity and authentication ecosystem, aimed at providing mutual assurance of the reliability of online transactions.
- Governments may act as both service providers and policymakers. As providers of essential online e-government services, they play a key role in fostering the use of digital identity within the private sector. Governments and public administrations can also act as registration authorities to guarantee the identity of a subscriber to a digital identity provider.
- Regulators, Data Protection Authorities, Supervisory Authorities and Auditors regulate, control, certify and audit digital identity certificates. As policymakers they have a key role in facilitating effective regulation of digital identity both at a national and regional level, by helping markets adopt a consistent framework for identity management and improving privacy protection and regulation, to secure and maintain user trust.

The challenges for policymakers and regulators

The legal and regulatory framework for mobile identity management generally revolves around issues of authentication and identification. Given the wide variety of digital identity applications, it is difficult to formulate a common or single definition of digital identity on which policy and regulatory issues can be based. One approach, as used by the European Union when they adopted their own eID regulation, is to take a 'process based' perspective. This incorporates the legal and regulatory framework around the processes of identification and authentication and more specifically around the inherent data that is processed over electronic networks and through digital identity related electronic transactions.

For example, in the European Union the new regulatory framework is comprised of a number of separate directives, regulations and technical standards that cover the following elements:

- **Electronic identification, signature and trusted services for electronic transactions;**
- **Data protection and privacy regulations;**
- **Technical standards;**
- **Other sector regulations that may apply depending on use cases.**

The extent to which these regulations are part of a harmonised and consistent framework is still being determined by EU policymakers. However, consideration of each of these topics gives a good insight into the nature of regulatory and policy issues around mobile identity, which other policymakers may need to consider when assessing their own frameworks and regulatory requirements.

As markets develop, trust and reputation become ever more important assets within the economy, so policymakers need to ensure consistency between the different legal and regulatory instruments that affect digital identity management. Such consistency and legal certainty will be required not only to ensure interoperability of services across the globe and consistent experiences for users, but also to provide business efficiencies and fair competition across different platforms, thereby encouraging market deployments while enabling innovation, competition and market growth.

Electronic identification, signature and trust services

In recent years national strategies to define standards and regulations for trusted digital identities, both for public and private sectors, are increasingly being introduced or considered around the world. Key jurisdictions have recognised that a central ingredient to a successful digital identity marketplace is to develop an overarching "Trust framework" which provides a set of technical, operational, legal and enforcement mechanisms for information exchange relating to the management of digital identities. These on-going initiatives are expected to have a major impact on the standards, regulatory and legal requirements for digital identity at global level.

For example:

- **In the USA, a National Strategy for Trusted Identities in Cyberspace (NSTIC)[13] has taken steps to create secure online identities for Americans.**
- **In the European Union, the eIDAS Regulation[14] marks a major new development in the regulation of digital identity. On 17 September 2014 a new Pan European Framework for electronic identification and trust services (i.e. electronic signatures, electronic seals, time stamping, registered electronic delivery and website authentication) came into force.**
- **In the UK, the Identity Assurance Programme (IDAP)[15], a government certification programme, is being developed to enable any organisation, including mobile network operators and other private sector providers, to become authorised digital identity and attribute providers in the UK.**

National Strategy for Trusted Identities in Cyberspace (NSTIC)

Within NSTIC, the US government has taken steps to create a user centric "Identity Ecosystem" of public and private sector organizations which utilize secure, efficient, easy to use and interoperable identity solutions to access online services in manner that promotes confidence, privacy, choice and innovation. Published by the White House in April 2011, NSTIC is a response to the call for action from the Cyberspace Policy Review[16] to build a cybersecurity-based identity management vision and strategy for Americans. The Strategy will enable American citizens to choose between multiple identity providers and digital credentials to conduct more secure, convenient and privacy enhancing transactions when online.

The objective of the strategy is to create an online environment where individuals and organizations can trust each other through a common way of asserting their identity at various Levels of Assurance (LoA). In practice, the strategy aims to reduce the social cost of current fragmentation in the authentication market, and fight identity theft and fraud by utilising a user centric approach with higher level of assurance credentials. In the long term this will result in higher levels of trust and higher volumes of electronic interactions and transactions.

There are four Guiding Principles that the Identity Ecosystem must adhere to:

- **Identity solutions will be privacy-enhancing and voluntarily–restricting the ability of service providers to link all of an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace. By default, only the minimum necessary information will be shared in a transaction. Equally important, participation in the Identity Ecosystem will be voluntary: the government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them.**
- **Identity solutions will be secure and resilient – to achieve this, the Identity Ecosystem will continue to develop in parallel with on-going national efforts to improve platform, network, and software security as well as efforts to raise awareness of the steps, both technical and non-technical, that individuals and organizations can take to improve their security.**
- **Identity solutions will be interoperable – to enable individuals to choose between and manage multiple different interoperable credentials. Further, identity solutions will support identity portability and will enable service providers within the Identity Ecosystem to accept a variety of credential and identification means.**
- **Identity solutions will be cost-effective and easy to use – but also bridge the 'digital divide'; available to all individuals, and accessible to the disadvantaged and disabled.**

These principles form the foundation for all of the Strategy's goals, objectives, and actions. One key role for the US Government in the implementation of the Strategy is to partner with the private sector to ensure that the Identity Ecosystem implements all four of the Guiding Principles.

On 17 September 2014 the National Institute of Standards and Technology (NIST) announced nearly $3 million in grants[17] to support projects for online identity protection to improve privacy, security and convenience. The GSMA, with the US's four major mobile network operators was revealed as one of the grantees, with the GSMA's Mobile Connect proposition as the foundation for the pilot. By allowing any organization to easily accept identity solutions from any of the four operators, the solution would reduce a significant barrier to online service providers accepting mobile-based credentials.

The eIDAS Regulation

The Electronic Identification and Trust services Regulation (eIDAS) will enable secure and seamless electronic transactions across EU Member States, making it easier and safer for individuals, businesses and public administrations in different countries to identify and authenticate themselves, sign documents and check the authenticity of documents online.

This new framework is the first EU law to require Member States to recognise electronic identifications issued in other Member States. It serves as a positive step towards simplifying and stimulating the digital and personal data economy as Europe moves towards the Digital Single market. It is a two-fold regulation predominantly related to:

- **Enable a system of voluntary and progressive mutual recognition and trust across EU Member States of eID schemes and trust service by public administrations.**
- **Provide greater legal certainty around using trust services across borders and replace the existing e-Signature Directive 1993/99 by increasing the level of harmonization required for e-signature and other online trust services, such as time-stamping, electronic delivery, electronic seals and website authentication.**

The eIDAS Regulation is expected to increase the effectiveness and transparency of public and private sectors' electronic services by providing legal clarity in terms of security and data protection requirements, national supervisory mechanisms and reinforced accountability and interoperability frameworks. The legislative approach is technology neutral and open to innovation, and its objective is to provide the basis for cross border and cross sector interoperability of strong forms of identification and authentication.

The eIDAS Regulation does not oblige EU Member States to introduce, or individuals to obtain, national identity cards, electronic identity cards or other eID solutions. Rather it provides a mechanism, and the regulatory conditions, for mutual recognition and interoperability as Member States notify the European Commission of the electronic identification schemes used at national level to access, at a minimum, public online services.

The new rules are expected to foster mobile identity adoption in Europe and internationally. However to ensure that these benefits are fully realised, the eIDAS implementation phase will require each national government and regulator to develop frameworks in which mobile identity services and its ecosystem providers can thrive. These frameworks must be flexible and technology neutral in order to balance the security and privacy regulatory requirements against the economic and social opportunities that mobile technology and data can provide.

UK Identity Assurance Programme (IDAP)

IDAP is a core element of the "Digital by Default" policy pursued by the Government Digital Service within the United Kingdom's Cabinet Office. It will help 25 government departments to redesign their digital services and make them "so straightforward and convenient that all those who can use them prefer to do so". IDAP will enable individuals to assert their identity online safely and securely, and give the government confidence that users of online services are who they claim to be.

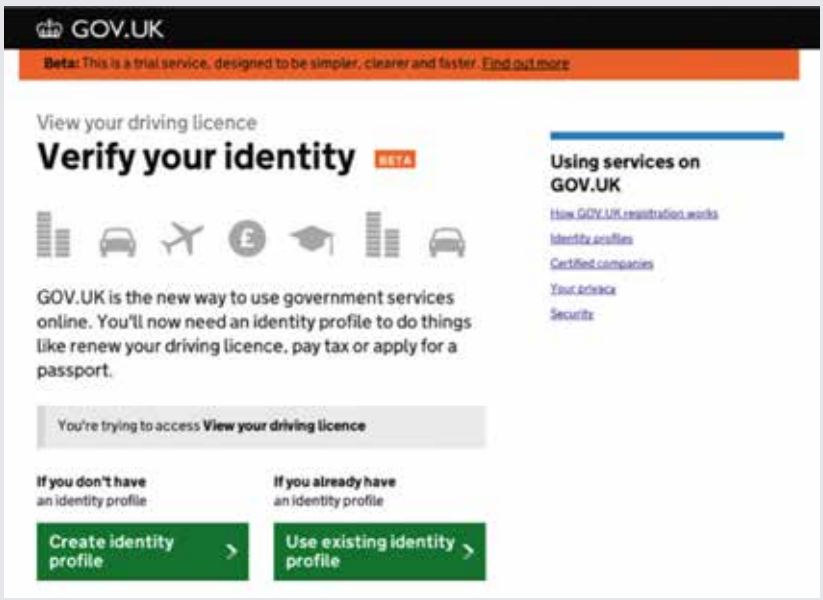
The UK government strategy is based on three key building blocks:

- **Building a "trust ecosystem" or "federated trust framework" of digital identity services which include the private sector.**
- **Articulate a set of standards, protocols and certifications under which organisations can collaborate to allow citizens to use assets they own to validate and verify their identity to 'relying parties'.**
- **Build a "hub" required to implement a "user led" federated identity approach to allow contracted private parties to authenticate identities without a central database or privacy being breached by unnecessary data.**

The first scheme to pilot digital identity assurance is being run through private sector bodies via a procurement process whereby a number of certified companies (including Experian, Mydex, Verizon, Digidentity and the Post Office) have been selected as first identity providers of the cross-government identity assurance framework in the UK. Furthermore a second procurement round for identity providers was announced in November 2014.

Through a standards based approach, the identity providers enable citizens to use evidence they own as part of the process for validating and verifying their identity. Once they have proven their identity with an identity provider, the individual authenticates via the identity provider who can assert the identity with multiple public services as and when required to by the individual.

IDENTITY ASSURANCE SERVICE IS A NEW SERVICE THAT WILL GIVE PEOPLE A SECURE AND CONVENIENT WAY TO SIGN IN TO GOVERNMENT SERVICES.



The Cabinet Office has published several reports and guidelines, including privacy principles, good practice guidelines on security, and others which are available on the Cabinet Office website[18].

According to the Good Practice Guide on Identity proofing and Verification of an individual, identity providers are required to verify an individual's identity according to the LoA and the proportionate strength and breadth of evidence required to achieve these LoA's. An evidence's strength is determined by its issuance process and security features. The breadth of evidence is achieved by requiring evidence from across a range of categories – Citizen, Money and Living.

Data protection and security

There is increasing evidence that consumers and citizens are concerned about their privacy and the misuse of their personal information online. These concerns may undermine trust and confidence in online services, and the corresponding use of personal information for identity management purposes[19]. Ensuring the safe, secure and transparent use of data is, therefore, key to securing the success of digital identity services.

In addition, data protection and privacy protection are currently subject to a patchwork of non-harmonised laws and telecommunications-specific rules, both at a global and European level. This does not assist in ensuring the necessary legal certainty for businesses, consumers and citizens, nor does it facilitate cross border data flows or cross border identity services.

For example in the EU, mobile and fixed line telecommunications operators are subject to rules not applicable to other Internet players, especially with regards to the use of account traffic and location data. The data may be used to provide existing customers with value added services, such as commercial identity management services, but only with their consent. Telecoms operators are also required to notify national regulators of security breaches and to notify individuals where such breaches may cause harm[20], and these security breach obligations currently do not apply to Internet-only players (i.e. internet companies that are not licensed network operators).

As eID involves the use of broader and more private sets of data among many more players, it will be necessary to develop a consistent and effective approach to ensure not only the security of data and identities, but also the reporting and management of security breaches. In the new eIDAS Regulation, the EU gives individuals the right to compensation for damage caused by poor security and to impose additional security obligations on service providers. Given that the current EU e-Privacy Directives already impose security and security breach notification obligations on telecoms companies, and given that the EC is planning to extend these obligations to other sectors, and introduce a Cyber Security Directive, it is crucial the EC adopt a consistent and uniform approach and ensure alignment of legal instruments.

The challenge for policymakers and regulators, whether in the EU or other parts of the world, is to establish a harmonised legal framework and to ensure legal clarity and certainty for service providers, consumers and citizens. This will be necessary to remove barriers and market distortions, as well as creating an internal market on digital identity management services.

Technical standards

Technical standards play an important role in fostering interoperability of mobile identity solutions. There are many standards relevant to digital identity typically managed by;

- **International agencies such as the International Organisation for Standardisation ("ISO"[21]), the International Telecommunications Union ("ITU"), and International Civil Aviation Organisation ("ICAO"); or**
- **Regional bodies such as the European Committee for Standardisation (CEN) and ETSI's Electronic Signatures and Infrastructures Technical Committee (TC ESI); or**
- **National Accreditation Bodies such as UKAS in the UK, ENAC in Spain, DAkkS in Germany, NAT in Hungary and so on.**

Issues covered include international standards for entity authentication assurance (i.e. ISO29115), standardisation of PKI systems, defining standards for qualified certificates, security management and certificate policy for trust service providers issuing qualified certificates; electronic signature syntax and encoding formats for security management. For mobile signature standards, this may cover technical requirements for interfaces between Mobile Signature Service Providers and those parties who choose to rely on mobile signatures for whatever reason[22].

Standardisation processes are often based on co-regulatory models, where standards are used as a tool to support the implementation of national legislation. Although many standards relevant to digital identity are already in place, there is a significant body of work still in progress and consequently, the overall standardisation framework is still uncertain.

Other sectoral regulations

Digital identity services can unlock new business opportunities across different sectors including mobile payments, mobile banking and mobile commerce. However, when identity management services are used within these specific domains, sectoral regulations may also often apply. In Europe, for example, there are a wealth of regulatory directives that are aimed to protect consumers and enhance the level of security of mobile payments via more stringent requirements on authentication and identification. These include the new Payment Service Directive (PSD2)[23], the e-money Directive (Directive (2009/110/EC) and the European Central Bank Recommendations on the security of mobile payments[24].

Policy considerations

To unlock the potential of the digital economy and ensure the successful implementation of mobile identity solutions, there are significant challenges that policymakers should address:

- **Ensure legal and regulatory certainty via flexible and technology neutral frameworks.**
- **Provide the right balance between protecting privacy and security and enabling the economic and social opportunities that mobile technology and data may bring.**
- **Facilitate the interoperability of secure electronic transactions across borders and across industry sectors.**
- **Minimise compliance costs for industry and address any other barriers arising from existing or new legislation.**

In order to meet these objectives, the key issues and considerations that need to be addressed include:

- **Mobile identity is at the core of digital society.** The mobile industry has a significant role to play to build trust in the digital economy. To ensure realization of the benefits of mobile, a consistent approach is required across the emerging identity management ecosystem. 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.
- **The role of Governments.** Governments also play a key role in unlocking the potential benefits of mobile identity by providing digital public services and accordant applications to the mass market, paving the way for further benefits to citizens, businesses and consumers.
- **Provide legal and regulatory clarity and certainty.** Uncertainty of regulation may hinder industry's willingness to invest. Policy makers should ensure that pro- investment policies are sustained, and harmonisation 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.
- **Application of principles on privacy and security.** Ensure the application of good principles around privacy and security while ensuring business efficiency and fair competition. In the emerging mobile identity market, the protection of privacy and security is a key issue, and industry, governments 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 and data portability, accountability and education for consumers and citizens.
- **Empower consumers.** Consumers need to understand the role of electronic identification, 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 consumer awareness and encourage understanding.

- **Allow for interoperability, standardisation and good governance.** Standardisation is a key step to achieving 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 place needs standards that embrace business process issues around security, privacy, and liability. As regulations and policies around these are finalised, 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 governments, service providers and consumers 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 solutions that are adopted are appropriate: they 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' societies and economies benefit most from the continued emergence of online activities, whilst minimising their attendant risks.

Endnotes

1) Regulation (EU) N 910/2014 which enable cross-border and secure electronic transactions and identification in the EU Digital Single Market.
2) For more information on mobile identity use cases please see GSMA papers on: Mobile Identity – Unlocking the Potential of the Digital Economy; http://www.gsma.com/personaldata/gsma-and-sia-mobile-identity-unlocking-the-potential-of-digital-economy;
A Mobile Connect Overview http://www.gsma.com/personaldata/mobile-connect-animation;
"Global mID Review" http://www.gsma.com/personaldata/mobile-identity-global-review-2013;
and various case studies published on http://www.gsma.com/personaldata/resources
3) Digital economy or internet economy generally refers to the network of economic and social activities enabled by digital infrastructures, content services and applications.
4) The Impact of Broadband on Growth and Productivity" http://ec.europa.eu/information_society/ eeurope/i2010/docs/benchmarking/broadband_impact_2008.pdf
5) "Cf. Álvarez Capón (2010): Catastro, políticas 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
6) Boston Consulting Group, The Value of Digital Identity 2012
7) Hearing of Andrus Ansip, Monday 6 October 2014, http://www.elections2014.eu/resources/library/media/20141022RES75838/20141022RES75838.pdf
8) A Mobile Connect Overview http://www.gsma.com/personaldata/mobile-connect-animation
9) For more information about the GSMA Mobile Connect solution please visit http://www.gsma.com/personaldata/mobile-connect-animation
10) http://openid.net/connect/
11) http://fidoalliance.org/
12) http://openidentityexchange.org/
13) http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
14) Regulation (EU) N 910/2014 http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32014R0910&from=EN
15) https://gds.blog.gov.uk/2014/01/23/what-is-identity-assurance/
16) http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
17) http://www.nist.gov/itl/nstic-091714.cfm
18) https://www.gov.uk/government/collections/identity-assurance-enabling-trusted-transactions
19) Eurobarometer: Attitudes on Data Protection and Electronic Identity in the European Union http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
20) e-Privacy Directive (2002/58/EC) and its amendments and http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=OJ:L:2002:201:0037:0047:EN:PDF
21) See ISO/IEC 24760, A framework for identity management; ISO/IEC 29115, Entity authentication assurance framework; ISO/IEC 9798, EntityAuthentication; ISO/IEC 29100, Privacy Framework; OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication; NIST Recommendations for establishing an identity ecosystem governance structure.
22) Current Mobile Signature Standards are stated in ETSI TS 102 203
23) http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2013/0547/COM_COM(2013)0547_EN.pdf
24) http://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9

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

mobileidentity@gsma.com
www.gsma.com