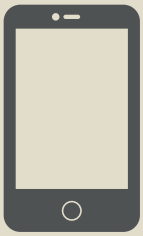
Mobile Identity

Mobile Identity

A Regulatory Overview



Introduction

This paper provides an overview of the regulatory background and key policy issues associated with digital and mobile identity services. Its 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. These include technical white papers, case studies and service blueprints. For more information, please go to http://www.gsma.com/mobileidentity/.

Background

At a simple level, digital identity is a proxy for, or supplement to, the real identity of an individual (or organisation) – and as such it can be viewed as the digital representation of a set of claims made by one party about itself or another entity in a given domain. These subsets of claims or attributes are typically conveyed to get a person or a thing recognised within a system or organisation (for example, whether or not that identity is allowed to enter a certain website or get access to services such as a bank account). 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 European Commission's proposed regulation on electronic ID[1] it is defined as *"the process of using personal identification data in electronic form unambiguously representing a natural or legal person"*.

Examples of digital identity services range from the provision of secure access to online personal and financial data and eGovernment services (for example e-Health or tax filing services), the use of multiple factor authentication technologies for digital payments and online banking, to digital signatures based on Public Key Infrastructure (PKI) and biometric-based electronic identity cards or tokens.

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 and service credentials to form part of a personal identity. Mobile represents an ideal platform for identity services not only because it is capable of providing identity services on the move (wherever a user takes his or her handset) and through a secure medium, but also through newer 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 per cent across the EU 27 Member States[4]. Many 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].

Building "trust" in the online environment 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. As EU Commissioner Neelie Kroes stated in her speech on EU Cyber security "the big opportunities of the digital economy will not be realised if people are worried about security and do not trust networks and systems"[6].

Trust is at the heart of digital identity. Trust is crucial in the context of delivery and consumption of electronic interactions between parties including users, 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 consumers 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.

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.

- **Consumers**, as users of both commercial and eGovernment identity services, should have the ability to minimize and contextualise the digital credentials they use to authenticate themselves or be recognised by online, whilst also demanding more secure, anonymous and safer online environments.
- **"Trust service providers"** or Certificate service providers play a critical role in issuing digital certificates for electronic identification and for other services that provide authenticity, integrity and non-repudiation to electronic transactions. The trust service provider role can be provided by many different organisations from mobile network operators, banks and other financial institutions to large public administration institutions, depending on the market and national legislation.
- **Other commercial entities** operate at many different points within the value chain and often provide varying services / roles depending on market circumstances. Such roles include acting as relying parties or verification authorities (for example web site or application providers) that serve to verify the end-user's authenticity, without necessarily sharing any of the user's personal identity data.
- **"Open trust frameworks"** and federated identity models (for example Open Identity Exchange (OIX)[7] and Mozilla's Persona) are large scale networks made up of multiple actors (such as policy makers, assessors, auditors and dispute resolution specialists) that provide a set of technical, operational, legal and enforcement mechanisms for information exchange relating to identity management. These are typically self-regulated industry identity initiatives.
- **Governments** may act as direct providers of essential online eGovernment services and as Registration Authorities to guarantee the identity of a subscriber to a trust service provider[8]. Governments play a key role in fostering the use of digital identity within the private sector. Most importantly, governments 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, so that trust is secured and maintained.
- **Regulators**, Data Protection authorities and supervisors/auditors that control, certify and audit digital certificates have varying roles that depend on national circumstances.

The challenges for policymakers and regulators

The legal and regulatory framework for mobile identity management generally revolves around issues of authentication / 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 adopted by the European Commission when considering its 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 regulatory framework is comprised of a number of separate directives and regulations that cover the following elements:

- Electronic identification, signature and trusted services for electronic transactions;
- Data protection and privacy regulations;
- Technical standards;
- Other sector regulations such as e-commerce regulation.

The extent to which these regulations are part of a harmonised and consistent framework is still being determined by EU policy makers. 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 and trust and reputation become more important assets within the economy, policy makers need to ensure consistency between the different legal and regulatory instruments that affect digital identity management. Such consistency and legal certainty will be required to ensure harmonisation across borders, to provide business efficiencies and fair competition across different platforms, and consistent experiences for users, thereby 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 the public and private sectors, are increasingly being introduced or considered around the world.

For example:

- In the USA, a National Strategy for Trust Identities in Cyberspace (NSTIC) has taken steps to create secure online identities for Americans;
- In the UK, the Cabinet Office has recently launched an Identity Assurance Programme (IDAP) to provide citizens with secure access to online public services. A government certification programme is also being developed to enable any organisation, including mobile network operators and other private sector providers, to become an authorised identity provider;
- In the European Union, electronic ID cards now exist in Belgium, Estonia, Finland, Germany, Italy, Portugal and Spain, and mobile signature solutions are also available in Finland, Norway, Spain, German, Poland and Latvia.

A major new development in electronic identification regulation is also taking place within Europe. The current EU framework for electronic signature and digital certificates[9] is under review and a new set of rules on eIdentification, eAuthentication and eSignature (referred to as 'eIAS services') have been proposed[10].

The new framework is a two-fold regulation predominantly related to:

- A system of voluntary and progressive mutual recognition and acceptance across EU Member States of 'notified' electronic identification means and schemes.
- A general framework for the use of online trust services, such as time-stamping, electronic delivery, electronic seals and website authentication, and an explicit obligation to grant the same legal effect as handwritten signatures to qualified electronic signatures.

The proposed European rules seek to enable secure and seamless electronic transactions between businesses, citizens and administrations, thereby increasing the effectiveness of public and private electronic services, e-business and e-commerce. The legislative approach is technology neutral and open to innovation, and its intentions are to provide the basis for cross border interoperability of strong forms of identification and authentication, such as eID to access electronic public services or digital signature.

At the same time, the regulation will also introduce more stringent rules for service providers, in terms of security and data protection requirements, the national supervision of eSignature and related trust services, reinforced data protection and the obligation for data minimisation.

Additionally, these new rules will not oblige EU Member States to introduce, or individuals to obtain, national identity cards, electronic identity cards or other eID solutions. But it will be necessary to ensure the emerging identity ecosystem agrees common definitions and terminology, standards and practices to ensure consumer and citizen confidence as well as business efficiency.

Data protection and security

There is increasing evidence that consumers and citizens are concerned about their privacy and the misuse of their personal information. These concerns may undermine trust and confidence in online services, and the corresponding use of personal information for identity management purposes[11]. Ensuring the safe, secure and transparent use of data will, therefore, be 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 traffic and location data for example. The data may be used to provide value added services, such as commercial identity management services, only with a user's consent. Telecoms operators are also required to notify national regulators of security breaches and to notify individuals where such breaches may cause harm[12], 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 ensuring not only the security of data and identities, but also to the reporting and management of security breaches. In its new regulatory eSignature proposals the EC intends to give 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 ePrivacy 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 therefore 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 and to creating an internal market on digital identity management services.

Technical standards

There are many standards relevant to digital identity typically managed by international agencies such as the International Organisation for Standardisation ("ISO"[13]), 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 the 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[14].

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 management 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 will also often apply. In Europe for example, there are a wealth of directives that are related to e-payment services and are strictly relevant to digital identity, including the E-commerce Directive (Directive 2000/31/EC), the Payments Directive (Directive 2007/64/EC) and the E-money Directive (Directive (2009/110/EC).

Policy considerations

To unlock the potential of the digital economy and ensure the successful implementation of mobile identity solutions, policy makers should:

- Ensure consistency and harmonization between applicable legal instruments;
- Prioritise the implementation of user friendly identity solutions;
- Ensure transparency and the application of clear and consistent rules for privacy and security;
- Facilitate 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. But to ensure mobile's role and the benefits of mobile are realised, will require consistent approaches 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 trust and confidence.
- **Ensuring Government "acceptance".** Electronic eID is a key enabler for Government and business transactions online. Governments are playing a key role in unlocking the potential benefits of mobile identity by providing eGovernment services and accordant applications to the mass market, paving the way for further consumer and citizen service digitisation. However, the concept of eID should receive political recognition in its broader form, i.e. digital identity should be seen as a way for users to get access to a wide variety of digital rights and be inclusive of the softer forms of authentication used for more general online transactions and activities.
- **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.
- **Ensuring 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, 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.
- **Empower consumers.** Users 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 awareness and encourage understanding of how electronic identification works.
- **Allow for interoperability, standardisation and good governance.** Standardisation 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 place needs standards that embrace business process issues around assurance, 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 identity are intangible, which makes them difficult for governments, service providers and consumers / citizens 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 COM (2012) 238/2 which seeks to 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 "Global mID Review" and "The Mobile Identity Economy".

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

5 Sources: 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 World Economic Forum 2013 http://europa.eu/rapid/press-release_SPEECH-13-51_en.htm

7 See: http://openidentityexchange.org/

8 The registration will typically occur at a government institute of the entity domicile (e.g. a municipality) that is acquiring the electronic or physical token and credentials to be used for electronic authentication.

9 A community framework for the legal recognition of electronic signatures, EU E-Signature Directive 1999/93/EC

10 COM (2012) 238/2 and http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

11 See Eurobarometer: Attitudes on Data Protection and Electronic Identity in the European Union http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

12 See 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

13 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.

14 Current Mobile Signature Standards are stated in ETSI TS 102 203.

Mobile Identity

For further information, please contact
Marta Ienco, Regulatory and Policy Director,
Mobile Identity mienco@gsma.com