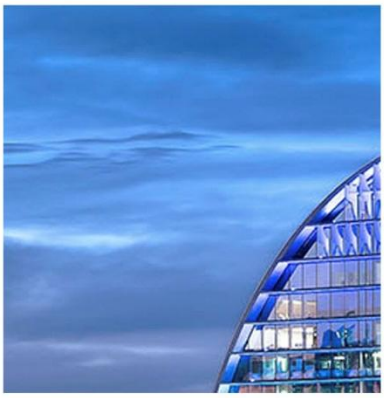
BBVA Research

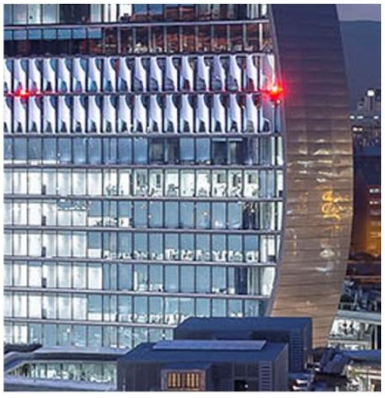
Nº. 18/01

WORKING PAPER

Digital Identity: the current state of affairs

Ana I. Segovia Domingo / Álvaro Martín Enríquez





BBVA | Research

Digital Identity: bthe current state of affairs

Ana I. Segovia Domingo / Álvaro Martín Enríquez

Abstract

In a world where the rise in the use of the Internet is increasing exponentially, the ability to prove your identity is crucial for the economic, financial and social development. Individuals and companies need identity solutions valid across different services, markets, standards and technologies. New technologies like blockchain, biometrics and AI can help to deliver secure identity services, in particular by governments and financial institutions, and solutions should meet both the objectives of ensuring secure identity and improving user experience.

As public identities have been created by different authorities, and since a global public or private identity is not a realistic option in the short term, interoperability and the collaboration between different entities to offer complete solutions is decisive. In the long run, to become a trusted identity provider across different industries could represent a big business opportunity for financial institutions.

Key words: Digital identity, Digital Regulation, Blockchain, Cybersecurity, Biometrics.

JEL classification: F6 (Economic Impacts of Globalization), K24 (Cyber Law), O33 (Technological Change: Choices and Consequences, D18 (Consumer Protection)

BBVA | Research

Index

1. Introduction

The Internet has changed the way we interact in our normal lives in an irreversible way. Back in the mid 1990s, in the early days of the World Wide Web, the capacity for anybody connected to the Internet to access information, simply by clicking on hyperlinks, was revolutionary.

The economy and society evolve very fast towards a world where interactions are mainly digital, and we have just started to see what a fully digital economy might look like: the revolution lies in the possibility for individuals to establish communications with remote computer systems which are able to take into account who they are in order to deliver information and services in a personalised way, in a global world that transcends national borders.

Traditionally**,** our identity systems have been based on physical interactions and documents.[1] **The capacity to prove that you are who you say you are is a fundamental component of economic, financial and social development.**[2] It allows us to access services (public or private) such as healthcare, education, financial services, justice... The World Bank estimates that 1.1 billion people in the world are not able to prove who they are[3].

The distance of time and location between buyers and sellers is the new normal, and implies the irruption of a large amount of new digital players, threats and opportunities. One of the main drivers for the future growth of online business is the existence of a reliable and strong digital identity that allows new players and incumbents (both public and private) to operate in an efficient and safe way.

Private companies, governments and regulators search for comprehensive solutions that enable clients and citizens to identify themselves. Our current systems for managing identity and data security are clearly deficient due to the fact that they are still largely based on the physical world. [4] In the financial services field, for example, most banks are still asking clients to show, at a branch, a physical ID card or a birth certificate to open a bank account. There are projects underway all over the world trying to find enhanced trust digital identity solutions. It is expected that these efforts will intensify in the next few years.

On the one hand, the number of actors in the market that will come online is expected to grow exponentially over the coming years. On the other, the development of new technologies, such as the IoT[5] phenomenon, will lead to the explosion of objects, from refrigerators to shipping containers, coming online as well. If all of these entities start to communicate with each other, standards will be needed to establish who or what they are.[6]

For financial institutions, the identity issue has played a significant role in business. In this time of change it is necessary for banks to create a strong and trustworthy digital identity schemes that can support their current expertise at verifying identities in the physical world. There are many hurdles on the path of adapting the analog world identity model to the digital one, such as lack of security, no interoperability, cyber attacks, a lack of user control over the data, etc. Companies and countries need to be able to find solutions that protect users and keep people's information private and secure while they offer more convenient products and services.

1: World Economic Forum & Deloitte. (2016).
2: GSMA (2016).
3: World Bank. Identification for Development (ID4D).
4: Pentland, A.,Shrier, D., Hardjono, T., & Wladawsky-Berger, I.
5: Internet of Things.
6: UBS (2016).

2. Digital Identity: Definition and Management

Identity is a conceptually complex term. It has been defined in different ways and contexts over the years. At a basic level, we can say that identity, in general, is any set of characteristics that define a person and can be used to uniquely identify that person.

As a consequence, **digital identity would be the digital version of a person's physical identity,** the digital representation of the individual. There is a significant number of digital identity definitions:

- The International Telecommunication Union (ITU) defines identity as a "representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context."[7] This concept emphasizes the context.

- The International Organisation for Standardisation (ISO) states that digital identity is an "item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has a recognizably distinct existence."[8] This definition implies that, apart from a person, other entities, like devices, might have a digital identity.

- The World Economic Forum[9] recently defined digital identity as a **"collection of individual attributes that describe an entity and determine the transactions in which that entity can participate".** This definition, as the previous ones, emphasises the idea of the usage of the identity. The WEF categorizes attributes into three groups: inherent (age), inherited (behaviour) and assigned attributes (ID number). These attributes differ for members of three main user groups: individuals, legal entities and assets. The attributes enable entities to participate in transactions by proving to their counterparty that they have the specific attributes required for that transaction. [10]

7: International Telecommunication Union (ITU). (2010).
8: ISO/IEC 24760-1:2011.
9: World Economic Forum & Deloitte. (2016).
10: European Commission (2016)

Figure WORLD ECONOMIC FORUM ATTRIBUTES CLASSIFICATION

	For individuals	For legal entities	For assets
INHERENT ATTRIBUTES Attributes that are intrinsic to an entity and are not defined by relationship to external entities	• Age • Height • Date of birth • Fingerprints	• Industry • Business status	• Nature of the asset • Asset issuer
ACCUMULATED ATTRIBUTES Attributes that are gathered or developed over time. These attributes may change multiple times or evolve throughout an entity's lifespan	• Health records • Preferences and behaviours (e.g., telephone metadata)	• Business record • Legal record	• Ownership history • Transaction history
ASSIGNED ATTRIBUTES Attributes that are attached to the entity, but are not related to its intrinsic nature. These attributes can change and generally are reflective of relationships that entity holds with other bodies	• National identifier number • Telephone number • Email address	• Identifying numbers • Legal jurisdiction • Directors	• Identifying numbers • Custodianship

Source: World Economic Forum (2016)

Digital identity: essentially human

Although the previous definitions are accurate, they are focused on the determination of the transactions the entities can participate in. They seem to place at the same level of importance the transactions that a person makes and the ones made by an asset or a legal entity.

Are these definitions simplifying the digital identity to the extent that they consider it mainly a tool to participate in online transactions? They assume that companies, individuals and things are equal partners in delivering business value, which is not necessarily true.

We understand digital identity as being essentially human. Therefore, the main pillar that every identity definition must rely on is the human factor. The regulation also supports this idea: for instance, in Europe, the recently approved eiDas Regulation, that provides a framework for electronic identification schemes in Europe, denies the idea of the existence of a full identity for legal persons when it states that only natural persons are allowed to have electronic signatures. Under eIDAS, the "signatory" will always be a natural person. Therefore, certificates for eSignatures cannot be issued to legal persons anymore.

Digital identity, in our view, is a uniquely human concept, and what makes it different from the rest of the entities is the self-consciousness characteristic of the individual. As René Descartes said, "Cogito ergo sum". I think, therefore I am, at least until developments in the field of artificial intelligence render this approach obsolete. As a working definition for this paper, we will define the individual as a personal entity.

New dimension of identity in the digital world. Unbundling identity

The way of moving an individual entity into the digital world has involved the creation of a digital representation of ourselves. **But that does not necessarily mean that this representation of ourselves is always by means of our full identity.**

The use of new technologies has facilitated the **unbundling of identity,** whereby we can share selected attributes of our identity online. The new scenario allows us to combine different attributes or data in the use of identity in different contexts. And every combination of the data necessary for any given purpose is different.

The idea of a person siloing different aspects of his/her personality, or none of them, into different web-presences seems strange but is not new: Back in the 1990s Roger Clarke introduced the definition of digital persona[11]: "In Jungian psychology, the *anima* is the inner personality, turned towards the unconscious, and the *persona* is the public personality that is presented to the world. The persona that Jung knew was that based on physical appearance and

11: Clarke, R. (1994).

behaviour. With the increased data-intensity of the second half of the twentieth century, Jung's persona has been supplemented, and to some extent even replaced, by the sum of the data available on an individual."

The digital *persona* would be, for Clarke, *a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.*

David Birch also states that "We'll have to construct a more digital notion of identity, where different attributes are used in different circumstances"[12].

Figure Digital Identity: A fragmented landscape

Source: BBVA Research

When we interact online, sometimes we do not want to provide our real data, or we do not wish to be identified at all, and we decide not to use our identity to act.

As a consequence, we can affirm that a personal entity can act on-line in two different ways:

- Using some or all attributes of his identity
- Using other attributes that are not part of his identity (fake attributes) or in an anonymous way.

In this context, we would define digital identity as the set of attributes that links a personal entity with his online interactions.

12: Birch, D. (2014).

Digital identity, veracity and level of assurance

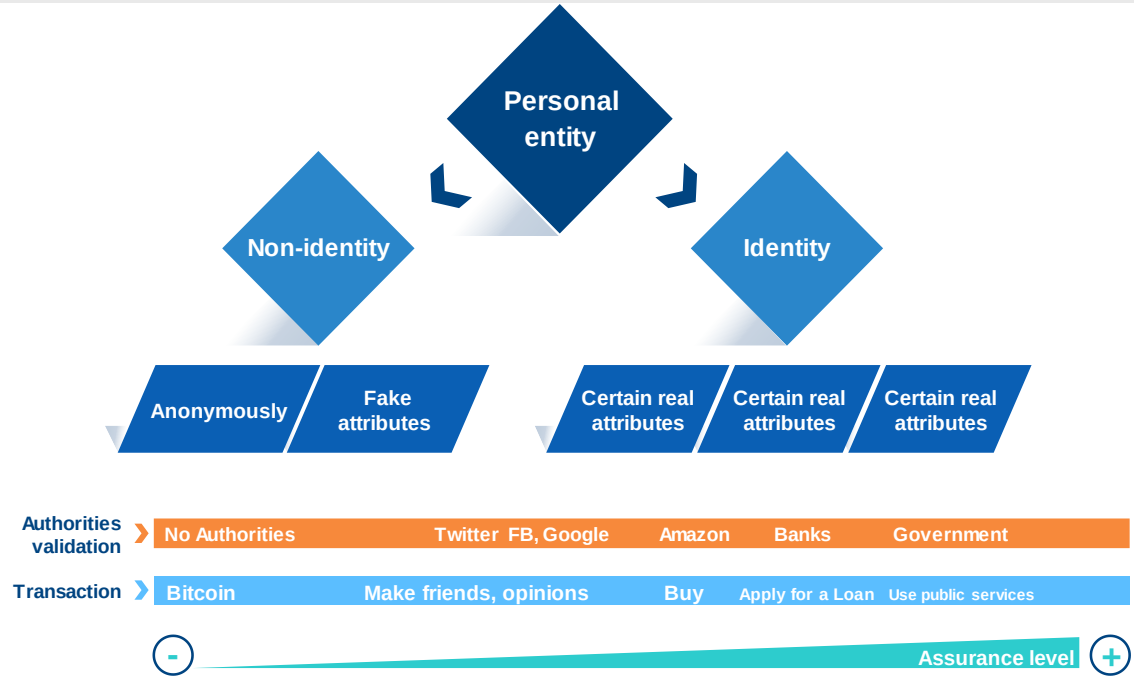
Veracity is a concept deeply linked to identity. Should we consider identity as a synonym of veracity? Only to a certain extent. We assume that all the attributes that configure our identity are true, but, as for certain transactions, we use only some of them; sometimes what we show is true but it is a partial aspect of our identity and we tend to hide the aspects of our personality that are not very favourable for us.

Fake identities are possible in contexts like Twitter or Facebook and Google, where the identity is not fully verified, but even those profiles on Facebook or Google that do not seem to be real are removed: nicknames and pseudonyms are considered breaches of the terms of service. [13]

What is really important, in order to interact online, is the validation that others do (identity providers or validators) **of the attributes that we share to prove our identity.**

As the level of assurance becomes more intense, a higher degree of veracity is required due to confidence being crucial in trade relations. We have to provide more proofs of our real attributes to open a bank account or send our income tax declaration than to make friends in Facebook. That is **why identity providers with a high level of assurance, like public authorities or financial institutions, will be the leaders of the future ID market.**

Figure Identity Unbundling



Source: BBVA Research

13: Krotoski, Aleks (2016).

Identity and personal data

It is obvious that the set of attributes that configures identity always involves the processing of personal data. The information related to our physical, psychological or behavioural attributes that is registered, stored or collected represents the type of information that data protection and privacy regulation covers.

Nevertheless, we cannot confuse personal data with identity attributes: while all the identity attributes are personal data, personal data is not always an identity attribute: for instance, the address is a piece of personal data, but, as several persons can have the same address, this isolated data is not an attribute of identity and only when it is combined with other elements could it be considered an identity attribute.

As exponential technologies grow, the amount of personal information companies own about online users is growing exponentially too. In fact, according to IBM, 90% of all of the data in the world has been created in the last two years[14].

Every object the individual uses, every time he transacts and everywhere he goes generates digital evidence. As more and more users depend on the information they provide or which is inferred by their behaviour, not using these new ways of communication is no longer a realistic option.[15]

Users are often not aware of the extent to which the collection and use of their data is already taking place, so they are not always fully in control of their digital identity. **Only when the user knows exactly when, where and to what extent such information is being collected will he be able to control his digital identity and take measures to protect it.** [16]

Today, the gathering, packaging and selling of people's online data is already a big business. According to the Boston Consulting Group[17], in the European economy the applications built on the use of digital identity can drive significant value growth for public and private institutions: At a 22% annual growth rate, the annual economic benefit is in the position of reaching €330 billion by 2020.

The sharing of personal data in a private, controlled, secure and convenient way is critical for the future of digital identity, with respect to which the user must be the owner of his personal information. [18]

14: IBM (2016).
15: Future Group new ideas for a free and safe Europe (2007).
16: International Bar Association (2016).
17: The Boston Consulting Group (2012).
18: Thomas, J. (2017).

Identity management approaches

The OECD defines Identity Management[19] "as the set of rules, procedures and technical components that implement an organisation's policy related to the establishment, use and exchange of digital identity information."

Traditional approaches to digital identity management have been focused on the creation of **static digital identities,** based on cryptographic tools like digital signatures and digital certificates. Some of the problems of these technologies are related to a lack of a good integration with Internet-based services; for PC-based online access, users sometimes also need to have ad-hoc readers to use their smart card. As a result**, eIDs are not always integrated into third party services as broadly as was originally intended**.[20] There are also concerns about its adequacy over a long period as these technologies need to be periodically verified to remain trustworthy. This model has been adopted in the implementation of almost all national eIDs and in traditional KYC processes.

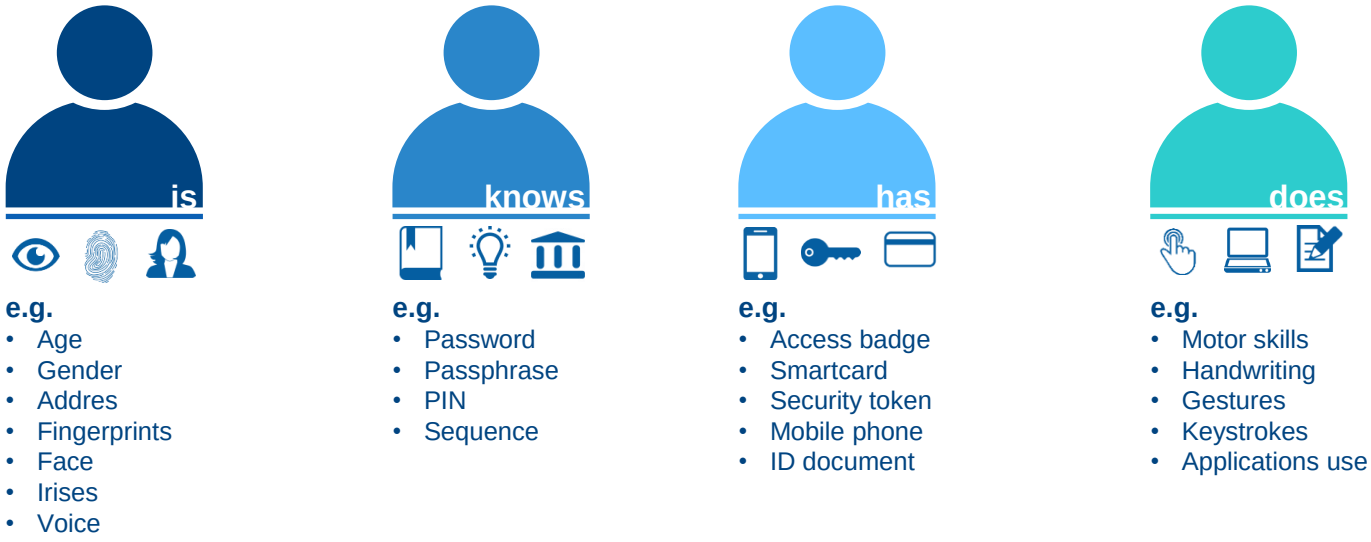
The second approach to digital identity management is **dynamic verification** based on an iterative process. This form of digital identity uses multiple sources (including, for instance, the user's mobile phone, his social media activity, geolocation, etc.). To support this system's assurance level, continous assessment and monitoring is critical. These identities are usually self-asserted, because it is the individual who communicates his attributes, and therefore the level of assurance is low. Nevertheless the user experience is very satisfactory due to there being no friction around the onboarding process. One example of this type of verification is Facebook Connect. In the financial services field, according to the ITU, it is not clear that this approach will be reliable enough to meet strict KYC and anti-money laundering (AML) requirements.

Current trends are heading towards a mixture of both approaches[21]: using both static and dynamic factors. Nowadays, the systems tend to establish a single identity for each individual based on the following elements:

- What the individual knows (password, PIN, security code)
- What the individual has (identity card, bank card)
- What the individual looks like or how he behaves (biometrics spanning physical/behavioural features)
- Where the individual is (mobile number, geo-location, IP address, social network site)

19: OECD (2009).
20: ITU (2017).
21: Accenture (2013).

Figure What a person



Source: World Bank

As a result of poor user experience associated with the use of passwords, some companies, such as financial institutions, have been migrating to new digital identification systems that meet both the objectives of ensuring secure identity and improving user experience. Behavioural biometrics technology, for instance, is able to learn patterns in user behaviour in order to build an identification model. The software analyses the way users interact with the different devices (phone, PC, tablets), how they hold the mouse, make keystrokes, how quickly they move, the pressure with which they hold the phone, etc. Over time, these biometrics are interpolated through algorithms and are able to define a unique pattern for each user in order to determine his or her identity in a certain way.[22]

One element that differentiates this technology from static biometrics in verifying identity is that the data are collected in a passive way and it does not interrupt the user activity, a key element of the user experience.

22: Segovia, Ana (2017).

3. Identity Providers

As we mentioned before, the key issue to operate with our digital identity is the validity that others give to the veracity of the attributes of our digital identity.

A digital identity needs a provider, but there is not a globally accepted identity provider. ISO standards for identity management state *that a digital identity authority is the entity in whose domain a particular digital identity is valid.* The identity authority and identity provider sometimes rely on the same entity.

Several attempts have been made to create a universal identity provider, with projects like OpenID[23], which seeks to offer a universal digital identity accessible across all platforms but, so far, it has experienced some problems in its implementation.

Which are the main digital identity providers?

Public Sector

Traditionally, in the physical world, governments have been the main providers of identity means. The documents, such as passports or ID cards, managed by public authorities have constituted a legally validated way to prove that these credentials correspond uniquely to a single individual. The passport is the typical example of a proof that a person has fulfilled the requirements for traveling and entering other countries. **National eIDs are usually issued in order to provide access to government services**.

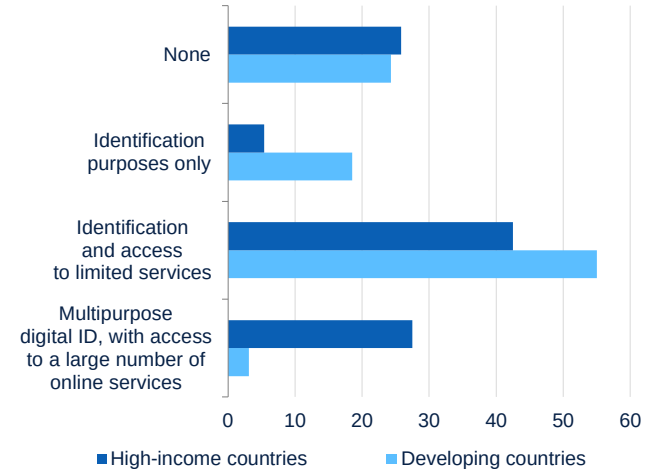
The notion of a public ID card issued and valid for the analogical and digital spaces has been materialized for millions of people. [24] In some countries, citizens and public and private organizations are starting to experience the benefits**. The European Union is also trying to provide a framework to enable the mutual recognition of the identity systems of EU Member States.** The aim of a global digital identity is to reach the same level of efficiency in the virtual world: to have a valid digital ID that allows citizens to participate in several domains.

At a global level, by early 2017, 82% of all countries issuing national ID cards had rolled out eID programs, according to the World Bank[25]. *Most developing countries have some form of digital ID scheme tied to specific functions and serving a subset of the population, but only a few have a multipurpose scheme that covers the entire population. Eighteen percent of developing countries have a scheme that is used for identification purposes only; 55% have digital IDs that are used for specific functions and services like voting, cash transfers, or health; and* ***only 3% have foundational ID schemes that can be used to access a collection of online and offline services.*** *Twenty-four percent of developing countries have no digital ID system whatsoever.* [26]

23: OpenID Foundation. What is OpenID?.
24: Gemalto (2017).
25: Gemalto (2017).
26: World Bank (2016).

There are initiatives like the World Bank Group's Identification for Development[27](ID4D) that try to help developing countries to put into effect new systems that increase the number of citizens with official identification with the support of new technologies.

Figure Different types of digital ID schemes across countries



Source: World Bank

Figure National Digital Identity Schemes. Validated identity on State eID (via citizen registers)

Source: GSMA

Box 1

India's UID programme

One example of a national identity system is India's UID programme. The Unique Identification Authority of India (UIDAI) is a statutory authority established on 12 July 2016 by the Government of India, under the provisions of the Aadhaar Act 2016.

The UIDAI is mandated to assign a 12-digit unique identification (UID) number to all Indian residents based on their biometric and demographic data. The implementation of the UID scheme has required the generation and assignment of UID to residents and the definition of mechanisms and processes for interlinking. Aadhaar is the world's largest biometric ID system, with over 1.171 billion enrolled members as of 15 Aug. 2017. As of this date, over 99% of Indians aged 18 and above had been enrolled in Aadhaar.

According to a recent study conducted by MicroSave,[28] using Aadhaar has been beneficial in e-KYC processes for banks and telecom operators in India. For the future, if e-KYC is adopted for customer on-boarding by banks (for savings bank account opened through branches and alternative channels) an estimated Rs 10,000 crore (1 crore Rupees =10 million usd) can be saved over the next five years (by 2021).

27: (ID4D). World Bank.
28: Telecom News (2017).

Private sector

Private sector firms need to verify the attributes of the customer to create a corporate Identity**. The private identity provider transforms individuals into users of their systems by the creation of their own credentials** (e.g. an online banking user). They require, to a greater or lesser degree, that the client send the physical documents that prove his identity in order to incorporate the data into the new identity. [29]

Federated identity

The providers presented so far manage isolated and centralized identity systems. Due to the increasing emergence of different services that require identity validation, **the current landscape demands identity provider systems that can administer identities and credentials for multiple service providers**. These are the so-called federated identity systems.

According to Gartner[30]**, *federated identity management enables identity information to be developed and shared among several entities and across trust domains.*** *Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization and other purposes, thus providing "single sign-on" convenience and efficiencies to identified individuals, identity providers and relying parties.*

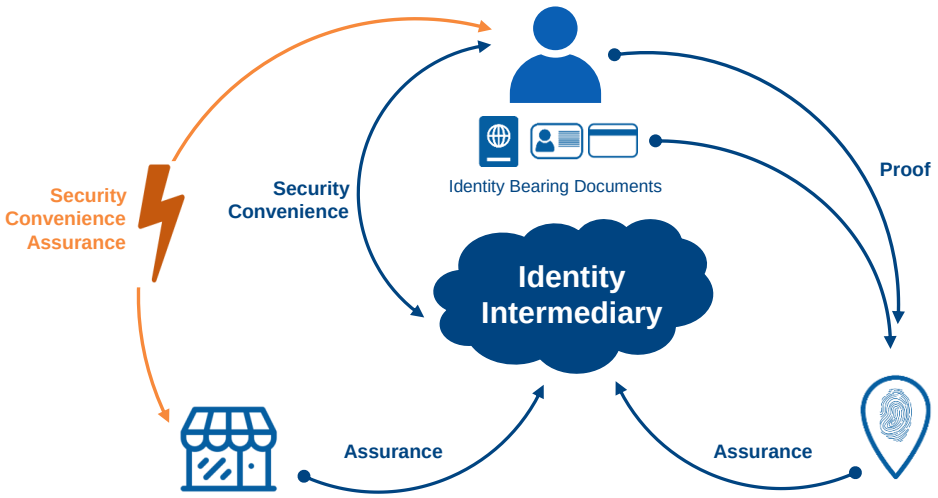
A classic example of federated identity is the use of government issued IDs for different private services. Public and private sector firms have a mutual interest in developing digital identity systems that allow the identification and authentication of users for different functions and services. Moreover, both public and private incumbents may rely on each other to build and manage identity schemes as complete as possible.

Collaboration models can be different depending on the type of the project and the scope of private sector involvement. Sometimes, private providers act proactively to use public IDs. In other instances, public authorities ask the service provider to rely on its ID. On several occasions, collaboration is set by a service agreement, in which a private firm plays a particular role in one or more steps of the digital identity lifecycle. In other cases the private sector is primarily in charge of the design, building and management of a project, usually for an agreed concession period.[31]

In these federated identity systems, **a third party or identity intermediary usually manages the identification process**. The identity data are transferred between different systems, and service providers and users can operate with the same credentials in different transactions with different service providers.

29: Telefonica (2016).
30: Gartner. Federated Identity Management.
31: World Bank Group, GSMA & Secure Identity Alliance (2016).
.

Figure The Federated Identity Management Landscape



Source: Secure Authentication and Attribute Sharing in Federated Identity Scenarios. Moritz Platt

In this scheme, service providers could be e-commerce, banks or e-government web applications and identity providers would be government entities or private providers.

In some European countries, like Estonia, Finland, Norway, Switzerland and the United Kingdom, for example, the private sector—and the mobile industry in particular—has played a key role in building national digital identity systems and authentication programs.

Figure Digital Identity Providers

One example of this federated identity in financial services is **BankID**[32]**,** a solution developed in Sweden by a number of large banks that can be used by members of the public, authorities and companies. The BankID network includes Danske Bank, ICA Banken, Ikano Bank, Länsförsäkringar Bank, Nordea, SEB, Skandiabanken, Sparbanken Syd, Svenska Handelsbanken, Swedbank and Ålandsbanken. Seven point five million people use BankID on a regular basis for a wide variety of private and public services. In Sweden 80% of the adult population has a digital identity and through the use of this Bank ID an individual can easily open a bank account and the financial institution will have reassurance, from an anti-money laundering (AML) perspective, that the customer's identity has been verified.[33]

32: Bank ID.
33: PWC (2016).

Box 2

The Estonian digital identification system

Estonia[34] has probably the most highly-developed national ID card scheme in the world. Its citizens can make arrangements regarding municipal or state services online in minutes. Since 2002, about 1.2 million credit-card sized personal identification documents have been issued that allow citizens to be identified and sign documents.

The system is based on two main principles:

- **a national register** (called the Population Database), which provides a single unique identifier for all citizens and residents.
- **identity cards** that provide legally binding identity assurance and enable electronic signing.

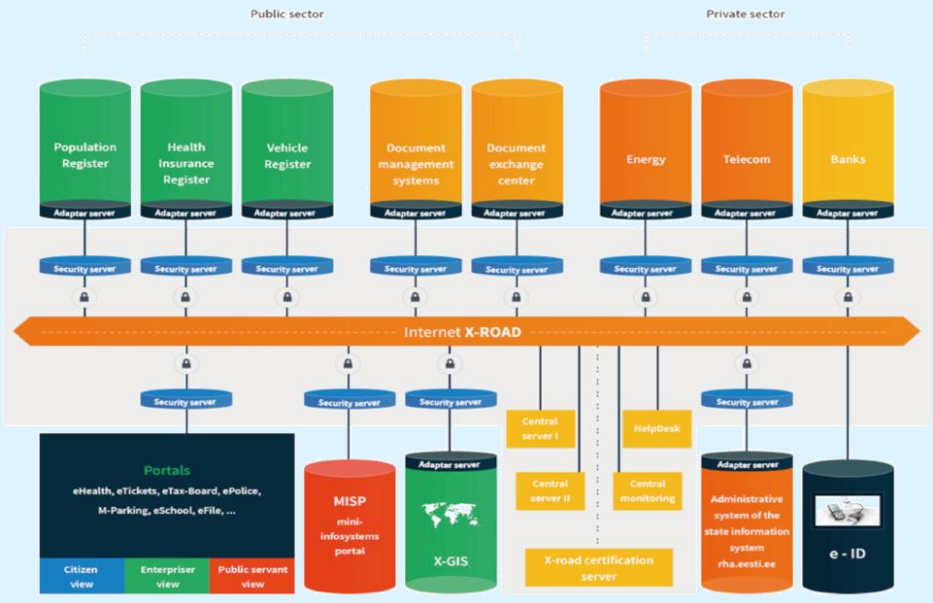
ID-cards are mandatory for Estonian citizens and they are valid both for digital and physical identification.

The digital functionality of the ID-card is based on an electronic chip and the two pin codes supplied with the card. By using a smart card reader and a computer connected to the internet, citizens can use the two core functionalities provided by the ID - card, both of which are essential to the development of e-government – personal authentication (related to the PIN 1) and digital signature (related to PIN 2).

In order to ensure safe communication between public databases and institutions that use different management systems and technologies, **Estonia has developed the X-Road**, a secure internet–based data exchange layer that enables different information systems to communicate and exchange data with one another.

In the X-Road environment, encrypted data are directly transferred through secure servers from one information system to another. **Data does not pass through the X-Road center and cannot be viewed there.** The center only has statistical information about data transfer.

Figure Estonian information system



Source: Republic of Estonia. XRoad Factsheet

34: Vassil, K. (2015).

4. Identity Drivers. Trends that are driving the need for digital identity systems

With customer interactions expanding to physical, online, social and mobile channels, firms are driven to develop new capabilities that will enable smoothly continuous, safe and robust identity recognition over time, and across different countries and industries.[35] The main drivers that we identify behind the investment in and development of digital identity systems are:

New user behaviour

***Rising customer expectations*.** Customers expect seamless, 24/7 omni-channel service delivery and they are ready to change quickly to services that offer the best customer experience.

For transactional purposes, mobile is becoming the dominant channel for Internet usage, so companies have been forced to offer identity validation via apps, as clients do not wish to go to the physical store or use PCs.

In financial services, banks have been using multilayered authentication for years via username and password schemes. Due to PINs and security codes being so easily forgotten, up to 30 percent of all support calls to call centers are password reset requests.[36]

Consumers are not happy with passwords and they prefer to reuse a single digital identity instead of changing constantly their credentials. This is the reason why companies are investing resources to find new convenient ways for customers to access using, for instance, behavioural biometrics as a replacement for passwords on mobile devices[37]. They neither understand why organisations need to ask for all the information they do nor what is done with that information once it is gathered. Customers also find it frustrating that they only receive a yes or a no, and not a why, when applying for credit products.

Need for Trust

Digital identity is a way for an individual or a business to prove who they are online with a certain level of trust. [38] As explained before, the more reliable a digital identity, the more complex online transactions the user will be able to make.

35: Accenture (2013).
36: Accenture (2013).
37: Segovia, A. (2017).
38: Telus (2016).

Proper Identity management in the analog world helps to address risks derived from human interactions and increases trust between the parties. This is crucial for economic and social development. If we translate this to the online world, a lack of a connection between a physical person and a digital identity will create additional uncertainties that do not exist offline. [39]

Safe digital identity management is essential to the security of the entity that validates access to its informational resources. Confidence is fundamental for the security of the individual who accesses these resources, particularly when he is the owner thereof (e.g. money in a bank, a medical record).

The impact of a lack of trust on internet businesses is very high. As a result of a lack of confidence, many consumers may hesitate to make online transactions. It is reported that, after a security breach, up to 12% of loyal shoppers stop shopping at a compromised retailer, and 36% keep shopping at the retailer but not so frequently[40]. For those who continue to shop, 79% are more likely to pay in cash instead of using credit cards. The same studies state that shoppers who use cash statistically spend less money after these events. Indeed, 26% say they will knowingly spend less than before. As a consequence, companies are forced to design and operate identity systems robust enough to protect data from being stolen by third parties for fraud purposes, due to the impact of potential losses in their businesses.

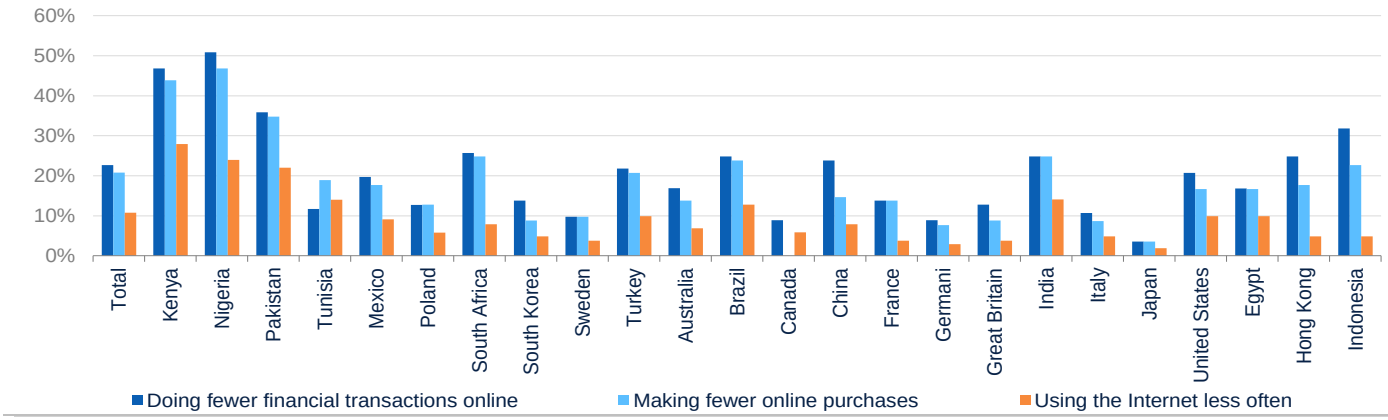
Increased concerns on privacy

In every project related to the implementation and management of an identification system, issues about privacy and personal data protection quickly appear.[41] **The privacy principle involves the idea that the data subject must decide how, where and by whom that information is used. Use of personal information comprises initial collection and all subsequent uses.**

Accurate data protection and respect for consumers' privacy are fundamental for transactional purposes. **If consumers do not feel that their data are protected, they will not transact online**. A recent global survey[42] shows that, in countries with a significant history of online fraud, 69% of consumers expressed that they are 'much more concerned' about their online security than they were just a year ago. This affected their online behaviour, with 51% less likely to do financial transactions online, and 47% making fewer online purchases.

39: OECD (2011)
40: Interactions Consumer Experience Marketing, Inc (2014).
41: Accenture (2013).
42: GSMA (2016).

Figure Impact of online privacy concerns on behavior



Source: GSMA (2016)

The rise of exponential technology

The current onboarding processes at many financial institutions are not adapted to the new customer demands. Fortunately, new technologies are emerging, improving the ability, speed and efficiency of the identity management systems, allowing companies to eliminate unnecessary processes and paperwork and improving the customer experience. Some of the most relevant are:

- **"Big data" technologies,** including cloud computing and data processing engines, allow companies to have a centralized infrastructure able to gather, classify and store vast amounts of information.
- **Biometrics** improve the ability to validate, with a high level of certainty, a client's identity, allowing for automated onboarding and remote access to services. There is a range of biometric solutions available at increasingly affordable prices. This technology enables automated recognition of users based on their physical (fingerprints, veins, iris) and/or behavioral characteristics (voice, keystroke and signature recognition). Valued at US$5 billion in 2010, the global biometrics market is growing at a CAGR of 18.5%, and is predicted to reach US$17 billion by the end of 2017. According to Deloitte[43] there will be one billion smartphones with fingerprint readers in use by the end of 2017. Nevertheless, by 2018, iris and face recognition will start to rival fingerprints.
- **AI and Machine Learning** are helping companies to identify complex patterns and relationships and use unstructured data sources to detect suspicious activities in a precise way.
- **Distributed ledger technology** could be used to centralize identity attributes storage and sharing among different firms. This system could allow the sharing of some sensitive individual data (the ones the user chooses) across several entities without compromising private information.[44]

43: Deloitte (2017).
44: PwC (2016).

Box 3

Blockchain and Identity

Blockchain technologies can provide a solution to many digital identity concerns, due to identity can be uniquely authenticated in an immutable and safe ledger. **Blockchain authentication is based on identity verification using digital signatures based on public key cryptography.**[45] With this technology, the only verification performed is whether or not the transaction was signed by the correct private key. We deduct that the person who has access to that private key is the owner.The owner's identity is not relevant.

"An innovative development in the world of customer onboarding in financial institutions is the use of blockchain technology to build Know Your Customer (KYC) utilities. **A KYC utility provides a centralized location where client identification and verification can be performed once per person, rather than several times by different organisations for the same customer."** [46]

There are several initiatives aiming at providing KYC utilities based on Blockchain. Some are located in Singapore due to this country is strongly fostering innovation in financial services. For instance, startup KYCK! uses IBM Blockchain and Bluemix to enhance the customer onboarding process in financial institutions. [47]

Diminishing costs

Digital identity systems are cheaper to run than physical ones. For organisations that need to verify customers' identities with a high level of assurance, it is much cheaper to use a digital identity already validated by a trusted third-party than to have to constantly gather and check the customers' IDs or driver's licences.

Deloitte has studied large retail banks and concluded that by streamlining processes and adding technology to eliminate paper, operating expenses can be reduced by as much as 25% (a reduction of between 60% and 70% of records management associated costs).[48]

For governments, an analysis by the Boston Consulting Group shows[49] that the efficiencies of digital identity systems could yield global taxpayer savings of up to $50 billion per year by 2020.

45: Blockchain Technologies. (2017).
46: PwC (2016).
47: IBM (2016).
48: Deloitte.(2012).
49: The Boston Consulting Group (2012).

5. The role of banks in digital identity

The OECD[50] has predicted a growth in the demand for digital identity management solutions and envisaged a substancial increase in consumer demand for privacy and protection from identity fraud.

The financial sector possesses an enormous amount of personal data due to the nature of its core business. This wealth of data will mean a world of possibilities. So far, the sector is just scratching the surface of what can be done with digital identity. One use case is related to the automation of processes, that could represent an important source of cost savings for banks. [51]

A largely untapped opportunity for banks is to become trusted providers of digital identity across different sectors. What are banks' key assets for entering this business? [52]

- **Banks have a long experience in validating identities**. First, in the physical world, and now in the digital one: as holders of digital accounts, they have had to work on designing secure processes to verify customer identity to match, and will be able to offer their knowledge to other industries, especially in terms of onboarding individuals, assets, and institutions onto digital systems. They are well positioned to act as identity intermediaries.
- Financial institutions are **typically trusted by consumers** above other institutions. As we mentioned before, the key issue in digital identity management is trust. The higher the level of assurance providers have, the more important the transactions they are allowed to do. After the public providers, in the private sector banks are the most reliable and they have to take advantage of this situation.
- Banks, due to the financial sector being so regulated, **are used to dealing with compliance standards** and can offer actors in other industries their expertise in identity-based networks. Regulations are increasingly requiring banks to do due diligence tasks on their customers in an effort to trace money laundering. To comply with these regulations imply an important investment for banks, in terms of money spent and the dedication of human resources to this task[53].
- **Some regulations are favouring the entrance of banks into the digital identity management business.** In Europe, the Second Payment Services Directive (PSD2) requires banks to give access to account data to third parties that may be potential competitors. **It also creates a chance for banks to leverage their relations with their clients** by offering Strong Customer Authentication (SCA) to third-party providers above and beyond what is required by regulation. "By doing this, the banks would accomplish two things: create a market for value-added services on top of the basic services required by PSD2 and strengthen the relations with the end-customer using the strong eID from the bank to access other services. It could also be used as part of an attractive value proposition to corporate customers of the bank."[54]

50: OCDE (2015).
51: The Boston Consulting Group (2012).
52: Galavski, R. & Robson, C. (2017).
53: Yurcan, Bryan (2016).
54: Nordseth, G. (2017).

Nevertheless, financial institutions have certain concerns in entering the identity management market due to:

- **Liability reasons** – in relation to consumer and/or reliant third parties. When things go wrong, who is responsible? What happens when malicious actors get introduced into the system?[55] Those are some of the questions that banks ask themselves before deciding to become digital identity providers. In this matter, regulation is critical. Institutions need laws that state, in a certain way, where the risk is allocated. As of today, under current anti-money-laundering and know-your-customer rules, banks are liable if they provide data from accounts to malicious or rogue third parties, whether this happens intentionally or, most often, not.

- **Identity thefts and risks to the banks' reputation** – massive cyber breaches can negatively impact the banks' reputation as digital identity managers. Due a recent cyber-attack suffered by Equifax (a credit monitoring company)[56], the social security numbers and other sensitive information belonging to 143 million Americans have been exposed.

- **High costs.** The costs of adopting the new identity systems are high and would have to be commercially viable for companies to adopt them.

The bank as a digital identity provider. Use Cases

All over the world, banks and public institutions are starting to develop new and secure ways for individuals to prove their identity. There is a point in allowing users to identify themselves once via a trusted provider, such as a financial institution, rather than having to share sensitive data with numerous third parties.

Some cases of financial institutions in the digital identity business are:

- **In the UK,** GOV.UK was launched by the Government Digital Service in May 2016. GOV.UK Verify is a building block in the transformation of UK public services and it was created to use government services online. The tool (via API or web) allows users to select and register with an identity provider, and then use their 'assured' identity to access digital services. Users are allowed to choose between multiple identity providers that then perform several background checks to verify that the person is who they say they are. **These checks, depending on the level of assurance the service requires, could include counter-fraud checks and activity history.** An individual accessing a government service, such as a Self Assessment tax return, will need to verify their identity from a panel of certified companies.[57] A financial institution, Barclays, is certified by GOV.UK to verify identities. When the user chooses Barclays, he is transferred to the Barclays Identity Service where their identity can be verified. Once the identity check is complete, the user will be returned to the government service. The user does not have to be a Barclays' client to register for an identity profile, but if he is, he can use some information from its online banking service to accelerate the process.

55: Hochstein, M. (2017).
56: Carman, A. (2017).
57: The Telegraph (2014).

- **Canada** offers another good example of banks entering the eID business. In 2012 the Canadian government launched a digital identity project called SecureKey. In a similar model to the UK, leading financial institutions (National Bank, Scotia Bank, Tangerine) manage the identification process for government services by means of a network called Secure Key Concierge. The system is storing the credentials of 7 million Canadian consumers and adds 250,000 new ones each month. The next step they are considering is to use blockchain technology to manage digital identities.

- In the **United States,** BBVA Compass partnered with Dwolla,[58] a payments provider, to develop an authentication process (FiSync) where customers use their same BBVA username and password to sign on at Dwolla without providing sensitive information. USAA is also using the firm's identity-as-a-service product, ID.me, to verify identity by remotely checking government issued identity documents. By using ID.me's Identity Gateway service users can link their official identity to a digital login which is accepted across different webs (such as the State of Maine or the Department of Veterans Affairs), without the need to create a new login or to prove identity at each site directly. [59]

- In **Germany**, Deutsche Bank is promoting an alliace between several firms in order to create a global digital identity in Germany. They pretend to create a single sign-on digital identity valid across different banking and other services platforms. The project will be launched by mid-2018.

Figure In the know. A roundup of ID projects in financial services globally

BBVA Compass
- Tokenized authentication on real-time payments with Dwolla
- Sponsored competition for identity startups

Canadian Banks
- Launched digital identity project SecureKey in 2012
- Announced in March that project would run on IBM's blockchain

Capital One
- Recently announcede B-to-B digital identity tools for consumer verification

Credit Union National Association
- Experimenting with a shared distributed ledger that gives members a cryptographic digital identity

Deutsche Bank
- Part of consortium seeking to bring universal digital identity to Germany

USAA
- Has acquired several digital identity firms
- Licensed technology to create new authentication tools
- Working to help digitize veterans' health records

Source: American Banker. May 2017

58: BBVA Compass (2015).
59: Yurcan, Bryan (2016).

6. Regulation of Identity

The current legal definitions of identity are not suitable to cover the full scope of our broad definition of digital identity. This is due to the difficulty implied when digital identity regulation is becoming a global issue and the legislation is still national[60].

Regulation related to digital identity only covers certain aspects of it and that is the reason why governments are starting to consider new rules to fill in the gaps. Some of the norms commonly involved in identity issues are:

Law of national identity schemes

One of the most relevant ways in which the law impacts on digital identity is through the establishment and regulation of national identity schemes. These national standards regulate legal identity implementation, authentication and verification and are created to serve as instruments of citizenship management and facilitate effective governance.

As we have mentioned before, there are different approaches to identity systems. Some countries have a national digital identity scheme, usually associated with credentials of a national identity card. Others have adopted identity cards only for certain purposes, with the result of a fragmentation in digital identity management.

In countries with national identity schemes in place, national law usually establishes a minimum set of attributes, but "there are no international standards regarding the minimum attributes that should be included." [61]

Interoperability

As identities have been created by different public authorities, and since a global public identity is not a viable option in the short term, **interoperability**, or the possibility that identities generated under different identity systems are recognised by other systems, **is crucial.**

One case of an attempt to achieve interoperability is Europe's eIDAS Regulation, which sets a legal framework for the mutual recognition of digital identities among European Member States. EU citizens will be able to engage in online relations with public authorities that provide them with seamless access to administrative digital services. By 2018 all public services in the European Union are obliged to accept the eIDs of other member states under the eIDAS regulation. Expansion to the private sector is the next step.

60: Rodrigues, R. E. (2011).
61: GSMA (2016).

Contract Law

Contract law covers some aspects of the digital identity related t**o electronic signatures, ID certificates, terms of service and agency** (a contractual agreement under which one person, called the agent, is authorized by another person, called the principal, to act on the principal's behalf).

One of the most obvious regulations of digital identities is the law of electronic signatures. There are two basic models in the adoption of regulation for electronic signatures:

- *The Civil Law model*, followed in most of Europe, most of Latin America and most of Asia, establishes prescriptive and specific laws relating to electronic signatures. Over fifty countries have enacted, and others are in the process of enacting, these laws[62]. Most of these countries have adopted the first international initiative in this matter: the UNCITRAL Model Law on Electronic Commerce[63], which indicates under which legal requirements electronic signatures must be deployed.

- *The Common Law model* (applied in the US, Canada, the UK and Australia, among others) follows a minimalistic approach where electronic signatures have the same legal validity as handwritten signatures.

62: Adobe.
63: UNCITRAL (1996).

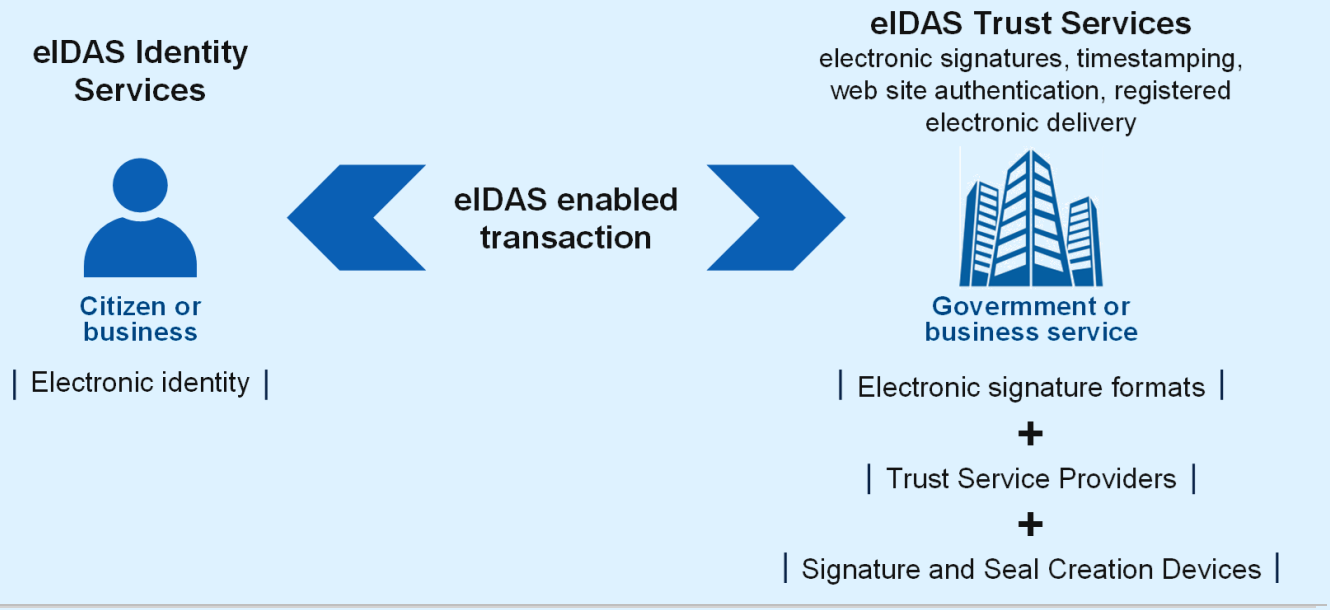
Box 4

In Europe, the eIDAS Regulation seeks to establish a single legal framework for recognising electronic signatures and identities throughout the EU. It forms part of a wider programme to create a single digital market in which identity is key, as some services can only be offered digitally in circumstances where the provider can reliably identify the user.

eIDAS creates an interoperability framework for the national eID systems to be recognized by public bodies across the EU, and it leaves it up to the Member States to define the terms of access to the online authentication of government eIDs for the private sector. “Banks are currently exploring how to use national eIDs to facilitate the cross-border use of electronic identification (eID) and Know-Your-Customer (KYC) portability based on identification and authentication tools under **eIDas** Regulation.” (European Comission)

eIDas also covers trusted services across Europe, and recognizes different levels of assurance. The trusted services now officially recognized are: electronic authentication, electronic seal, electronic time-stamp, electronic documents, electronic delivery services, and website authentication.

Figure Principal eIDAS components



Source European Commission

Data protection laws

Another crucial mainstay that establishes the framework of an identity system is data privacy regulation. **According to the World Bank[64], 50% of countries with a national identity card system do not have any data protection legislation in place.**

Digital identity management systems have a risk, inherent to their nature: **they can be used as a tool for surveillance**.[65] The administration of identity inevitably results in being able to determine the place where the user is and when he is there, the type of information he is using, the number of times the identity was used and so on. These issues impact directly on the privacy sphere of the user. If we wish to develop a fully digital economy, it is necessary for the countries to establish strong data protection laws that guarantee that the collection, storage and sharing of personal attributes collected in identity registration processes, is safe and appropriate. Specific public agencies must be created to ensure law enforcement and compliance by companies and public institutions.

Data protection law affects digital identity immensely, particularly in Europe where the main regulation on this matter is the General Data Protection Regulation (GDPR) that came into force in the EU in May 2016 and will be fully adopted by 25 May 2018[66]. The regulation includes both physical and digital identity management in a large number of provisions that reinforce the idea of an individual control over one's own data, the most important of which are: right to access, right to be forgotten, right to portability and right to data minimization.

Cross-border restrictions

Some countries have set cross-border restrictions on data delivery, storage and processing to protect their citizens from having their data moved without the user consent to a less strict jurisdiction. **As a result, requirements in one jurisdiction may not apply in another where similar activities are being carried out.** Sometimes there are direct conflicts related to these requirements *and may drive companies to have duplication of systems that could otherwise serve multiple countries, thereby unnecessarily increasing cost and fragmenting data, identities and credentials.* [67]

- **Criminal laws.** Another regulation related to identity is criminal law with respect to activities like identity fraud, phishing, account hacking, etc. Regulating digital identity through criminal law is primarily a national issue, and there are important differences in the approaches of different countries. In the international context there is not a criminal framework regulating digital identity crime when it usually has trans-national implications. The only international instrument providing a global international criminal law framework is the Council of Europe Convention on Cybercrime[68], signed in 2001, that seeks to address Internet and computer crime, and in which identity theft is included, by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.

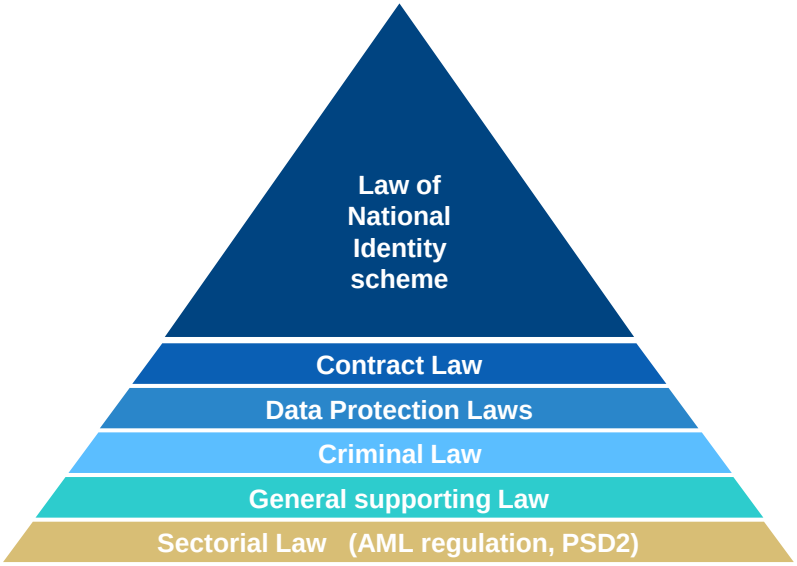
64: World Bank Group, GSMA & Secure Identity Alliance (2016).
65: Lips, Miriam (2008).
66: Urbiola, P. (2016).
67: GSMA (2016).
68: The Council Of Europe's Convention On Cybercrime. (2001).

- **General supporting laws**

  - **Regulation on liabilities** of identity providers also apply to digital identity. There is negligence when a person or company breaches a duty of care owed to another and the breach causes loss to the person the duty is owed to.

  - **Intellectual property** protection in its different forms is also relevant for digital identity. For instance, trademark law protects the commercial use of signs, or a combination of signs, that are part of our identity such as personal names, pictures, e-mails, etc.

Figure The rules comprising a typical trust framework for identity systems



Source BBVA Research

Other sectorial regulations that apply to digital identity are:

- **AML Regulations**. Anti-money laundering (AML) is a set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions. In most cases, money launderers hide their actions through a series of steps that make it look like money that came from illegal or unethical sources was earned legitimately. **In terms of identity, these regulations cover the digital onboarding of new customers in financial services.**

  AML rules and regulation moved towards global recognition when the **Financial Action Task Force (FATF) was formed along with a framework for international standards for fighting money laundering.** The FATF designs and promotes policies and standards to combat money laundering.

In Europe, despite some regulations related to the AML Directive[69] that are trying to harmonize the valid methods for identity verification, there are still some differences across the Member States**. For instance, in relation to remote onboarding of banks' customers, some EU Member States allow the use of non-face-to-face identification by means of videoconference while others do not.** As a result, financial institutions in these Member States can start distance banking relationships (including cross-border) whereas others are prevented from doing so in their own jurisdictions due to face-to-face identification still being compulsory. This situation creates an uneven playing field between banks located in different countries.

PSD2

As we mentioned before, the Second Payment Services Directive (PSD2) is an important regulation related to payments in Europe that affects the identity management scheme to open access to accounts to third parties.

69: Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

7. Challenges

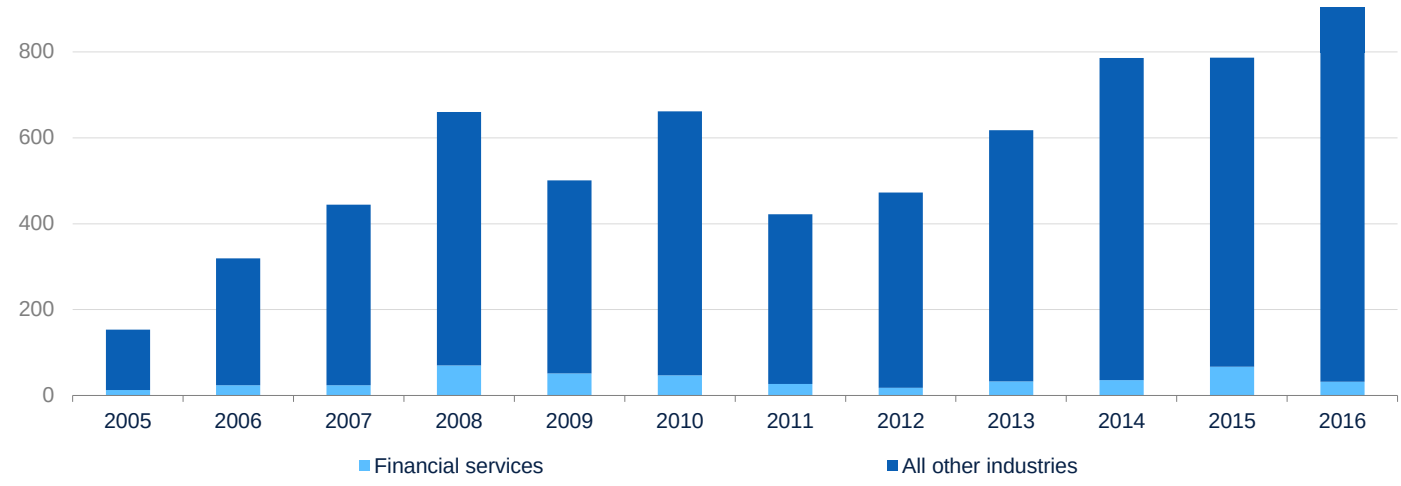
As the adoption of digital identities increases, some issues that incumbents need to address are arising. The most important are:

Cybersecurity

Security is becoming a relevant source of concern for companies. Identity management systems may be subject to serious compromises such as data theft, loss or cracking of passwords, token compromises, jeopardized system hardware, illicit communications surveillance and phishing.

In 2016, reported data breaches[70] increased by 40%, setting a record in the US. Major hacks resulting in the release of private information are increasingly common, and identity theft is widespread. Companies like Yahoo announced the largest data breach in history last year, affecting more than one billion accounts.

Figure Hacker heaven. 2016 set a record for reported data breaches in the U.S., though the financial companies' portion remains relatively small



Source: Identity Theft Resource Center *As of 11/22/16

Online **identity theft is the theft of personal information in order to commit fraud**. Identity theft techniques are diverse: from the sophisticated to less elaborate schemes, but also as a result of **online purchases** or other situations where consumers provide sensitive information such as credit card details or ID number. The thieves use victims' personal information for a variety of different unlawful purposes: *misuse of existing accounts, opening new accounts,*

70: Leary, J. (2016).

fraudulently obtaining government benefits, services, or documents, health care fraud, and unauthorized brokering of personal data.[71]

Data breaches cause harm on several fronts: clients see their personal information compromised; organisations see confidence deteriorated and their brand and reputation suffer. [72]

It is also important to mention that the use of social media is favouring cyberattacks. It looks like "our seemingly endless capacity for sharing, liking and retweeting has some negative ramifications, not the least of which is that it opens up the chances to be a target for identity theft"[73]. Experts emphasize that, while corporations and government agencies around the world are training their staff to think twice before opening any attachment or link sent to them by email, ***hackers have already moved on to a new kind of attack, targeting social media accounts, where people are more likely to be trusting***.[74]

Lack of standardization and interoperability

As we have explained before, identity management is fragmented, there is a lack of standard means to assign, list or share identities. Each identity provider (whether public or private) stores the information in a different way. **Data about users is gathered and stored in many different places.** Furthermore, millions of people around the world do not have official identities and are usually excluded from the protection of a State. In a digital society, the lack of such identity will make these individuals even more excluded.[75]

Moreover, identity systems do not communicate well with each other and, as a result, we experience frustration every time we have to register for yet another website, or, in the case of financial services, provide the same documents – yet again – when we open a new bank account.

Lack of user's control

Nowadays it is very difficult for individuals to have an idea of who is gathering information about them. Once in the digital world, it is very easy to store, copy or use our data, without consent.[76]

Regulatory uncertainty

The behaviour of commercial firms involved in the identity management industry is largely unregulated. Identity management practices change from industry to industry and are subject to constant evolution. The way in which these identity providers conduct their business is not open or accountable. **There is much progress to be made in converting digital identity management into more transparent and visible systems.**

71: OCDE (2008).
72: Boston Consulting Group (2012)
73: Velasco, J. (2016).
74: Frenkel, S. (2017).
75: UBS (2016).
76: UBS (2016).

8. What to expect next

Digital identity is bound to be an essential part of our personal and business lives as the technological and societal landscape continues to change. Although it is not easy to accurately predict the future, over the next years we expect to see some trends related to the eID market that will affect the financial market businesses:

Expansion of national ID schemes and federated systems

According to Gemalto[77], **the number of electronic National ID cards in circulation will reach 3.6 billion by 2021.** This figure reflects the fast adoption of electronic IDs systems and the future relevance of eGovernment and eCommerce services. Robust eID systems, according to Acuity, will provide substantial opportunities for national, regional, and global transaction infrastructures secured by a trusted digital identity scheme. The UN and World Bank ID4D[78] initiatives set a goal of providing everyone on the planet with a legal identity by 2030. The expansion of a fully interoperable ecosystem is expected where banks, telcos and other private companies can keep their operating costs down and governments are also able to reduce data security expenditure.

Greater demand for security and trust

Due to the increase in the number of cyber attacks, we expected that countries and companies will take measures to bolster security and combat ID fraud. Companies will, due to the increase of privacy and cybersecurity regulations, assume accountability for a trusted flow of data. Every private or public identity provider must explain how it operates with personal information.[79] Companies and institutions will increase data security expenses in order to safeguard digital identity.

ID will be more mobile in the future[80]

There are multiple signs that show that mobile phones will be the most suitable platform for a secure digital identity solution in the future (present everywhere, smart, secured by hardware or the SIM card). Mobile phones already have all the elements required to take the notion of identity into its next generation.[81]

Cooperation in the eID business

The eID business is a clear example of industry cooperation. Small software companies join forces with other suppliers and work mainly via partnership networks. [82] Companies work together to deploy biometric solutions for eID

77: Gemalto (2018).
78: World Bank. Identification for Development (ID4D).
79: Boston Consulting Group (2012).
80: Gemalto (2017)
81: GSMA (2017b).
82: X-Infotech (2016).

documents. In the future, more cooperation is expected in what the OECD called a "competitive necessity"[83] that leads businesses to create identity management partnerships in the operation of their digital services

Expanded application of new technologies

Further application of new technologies to identity will take place, supporting the transition from physical to digital ID:

Biometrics

Biometrics will continue to advance in identity verification technologies. As a result of poor user experience, high and rising costs and security breaches associated with the use of passwords, companies and especially financial institutions will continue the migration to new digital identification systems. According to Goode Intelligence[84], by 2020 there will be at least 120 million customers using mobile biometrics on a daily basis for their financial transactions.

Blockchain

It is expected that banking institutions and new fintech players will evolve to implement blockchain technologies that allow the safe sharing of user data. As already mentioned, the advantages of such systems are that the user has control over his data and decides what information he wants to share.

However, in order blockchain to develop to deploy its full potential, technological, organizational and regulatory changes must be done. Current local legislations still do not fit with the global nature that a blockchain scenario contemplates.[85]

Internet of Things

The IoT phenomenon will lead to the explosion of objects acting online as well. Standards to regulate them will be mandatory. According to CISCO[86], there will be 50 billion IoT connected devices by 2020. **In order to reach their full potential, authentication process has to evolve from traditional authentication to seamless verification**. To have a large amount of devices connected to the Internet of Things should not be a problem if authentication is easy and secure.[87]

Artificial Intelligence

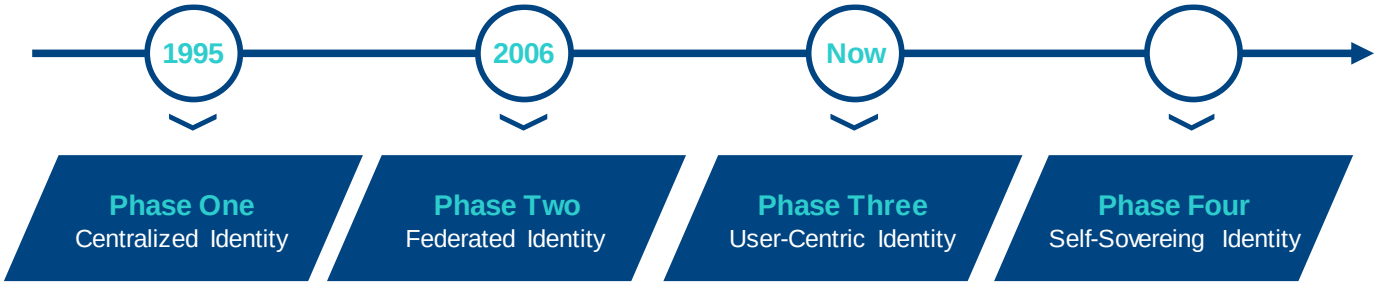
The development of artificial Intelligence **will enable stronger authentication procedures**, helping financial institutions with onboarding processes and also fighting identity fraud. It will also help to safeguard the banks' sensitive data by, among other things, keeping track of where it is stored and who has access to it. AI will maximise the amount of data available to be analysed and let algorithms learn processes and create patterns to infer user identity.

83: OECD (2007).
84: Goode Intelligence (2015).
85: ICAR (2017).
86: CISCO (2016).
87: Van Donselaar, Marcel van Kleef & Dominika Rusek (2016).

More user control of digital identity, the next step

As stated across this report, our identity is fragmented and replicated throughout the digital world, making the different instances difficult to link together.

Figure Identity evolution



Source: Allen (2016)

The identity management system is evolving: it is expected that federated identity systems keep developing and become interoperable. The user will increasingly take control of the use of his identity, effectively moving towards what is called a user-centric identity. This involves the idea of a credential provided to an individual that, acting on his own behalf, he can choose to use in a variety of online interactions with the guarantee of privacy and security around the verification process.

User-centric identity systems are developed **to give users more control by allowing them to choose identity providers independently of service providers.** The goal of a user-centric identity system is to enable the creation of identity providers that operate in the user's interest rather than in the sole interest of the service provider. [88]

But with these systems we still have the problem of security, since the user has to rely on a controller or issuer of his identity. Security authorities[89] have repeatedly warned against centralized system administration, which could easily be a target of cyber attacks, enabling both insiders and opponents to destroy system security with a single exploit. The best solution to this issue is to have authority distributed among many trusted actors so that the compromise of one or even a few authorities does not destroy the system security consensus. [90]

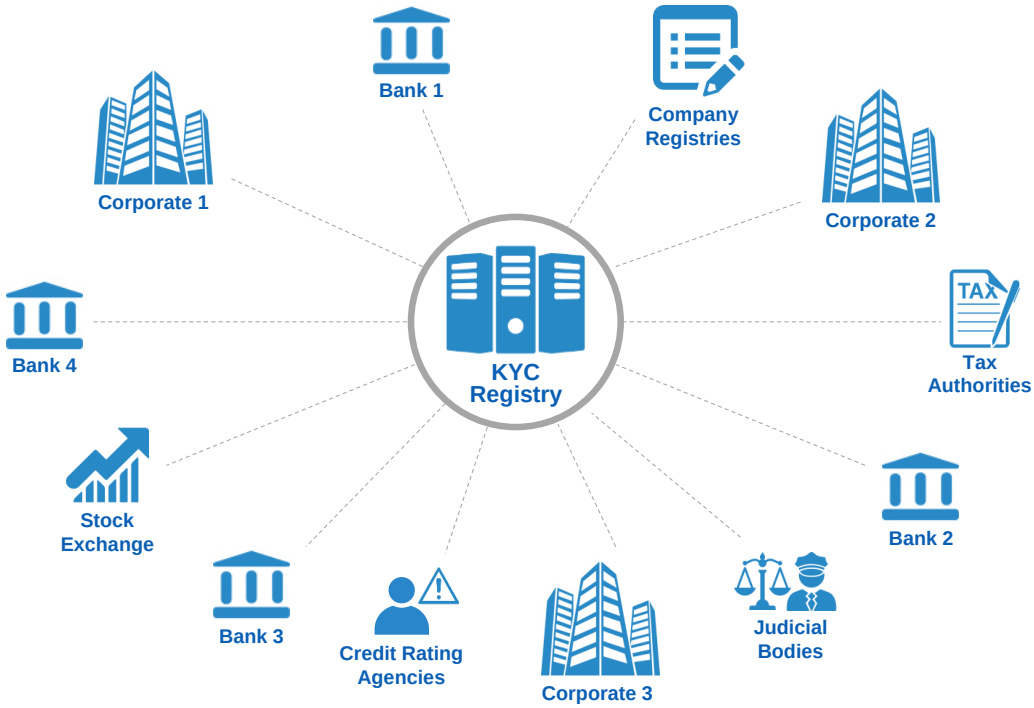
The next step would then be the **distributed identity system,** where the authority is distributed among many trusted actors. This is what is often called a **self-sovereign identity**[91]**.** This term, that has become increasingly used over the last decade, refers to an individual data control across any number of authorities, and it is the most recent envisaged step in the identity evolution. With the adoption of distributed ledger technologies, **the individual would not need to**

88: Lips, Miriam (2008)
89: Grant, J. (n.d.).
90: Pentland, A.Shrier, D., Hardjono, T., & Wladawsky-Berger, I. MIT (2016).
91: Allen (2016).

rely on a controller, issuer or processor to comply with regulations to get, duplicate, move, send or secure his data. This is where blockchain might come into play.

But is this last step in the evolution of identity **a mere aspiration that cannot be fulfilled**? Innovative banks are increasingly seeing their future as the guardians of identity in blockchain, where they would act as authenticators.[92] Such a system would allow clients to use a digital token, for instance, to verify their age when ordering a drink.

Figure Know your Customer and Blockchain



Source: Finextra

92: Yurcan, Bryan (2016).

9. Conclusions

The economy and society are moving very fast towards a world where interactions are increasingly digital. At a global level, **identification is a fundamental enabler of economic and political development** and it has become a key issue for the global economy. The OECD[93] has predicted a growth in the demand for digital identity management solutions and envisaged a dramatic increase in consumer demand for privacy and protection from identity fraud. It is essential to be able to rely on efficient access, storage and sharing of critical data in a secured and private way. [94]

The evolution towards a digital economy demands **different identity systems to be used in different domains that require different levels of assurance.**

Individuals and companies need identity solutions which are valid across services, markets, standards and technologies. New technologies like blockchain, biometrics and AI can help to deliver identity services, with solutions that should meet both the objectives of ensuring secure identity and improving user experience.

As current identities have been issued by different authorities, and since a global public or private identity is not a viable option in the short term, **interoperability**, or the possibility that identities generated under different identity systems are recognised by other systems to offer complete solutions, **is crucial.**

Financial institutions, under current regulation, **see themselves as relying parties in a federated system** rather than as identity providers using the information already gathered by other firms. It would be much simpler for them to know who they are dealing with if they could get fast access to a token or digital certificate that verifies the person's identity. [95]

Nevertheless, in the future, and depending on the development the regulation, to become a digital identity provider will imply to invest in the relationship with the clients, based on trust, which is a key element of digital services.

Legal certainty is crucial to guarantee the interoperability of services across different countries and sectors and similar experiences for users, but also to provide business productivity and a level playing field among the firms, in terms of competition, across different platforms. [96]

Regulators must also protect consumers, putting **data protection** in the centre of the framework of a strong and secure digital identity system. Governments need to build strong '**trust frameworks'** by regulating the different components of digital identity schemes.

Finally, the cybersecurity of the transactions is a key issue for the general adoption of trusted digital identity systems. Firms are forced to boost their cyber-defense strategies to reassure consumer confidence. If they succeed in this feat, their involvement in the transition from analog to digital would give them a powerful tool to fight off competition.

93: OECD (2015).
94: Pentland, A.,Shrier, D., Hardjono, T., & Wladawsky-Berger, I.
95: Yurcan, Bryan (2016).
96: GSMA. (2016).

References

Accenture (2013). *The future of identity in banking*.Retrieved from https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_9/Accenture-Future-Identity-Banking.pdf

Adobe (n.d). *Global Guide to electronic signature law.*Retrieved from https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-to-electronic-signature-law.pdf

Avetisova, Ksenia & Antti Kettunen (2017). Digital identity management as key component of future customer experience. *Tieto*. Retrieved from https://perspectives.tieto.com/blog/2017/01/digital-identity-management-as-key-component-of-future-customer-experience/

Bank ID (2014). This is Bank ID. Retrieved from https://www.bankid.com/en/om-bankid/detta-ar-bankid

BBVA Compass (2015). Dwolla begin rollout of real-time bank. Retrieved from http://newsroom.bbvacompass.com/2015-04-08-BBVA-Compass-Dwolla-begin-rollout-of-real-time-bank-transfers

Birch, David (2014). *Identity is the New Money*. London: London Publishing Partnership

Boston Consulting Group (2012). *The value of our digital identity*. Retrieved from http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

Carman, A. (2017). Equifax compromised 143 million people's Social Security numbers and other data. *The Verge*. 7 Sep. 2017. Retrieved from https://www.theverge.com/2017/9/7/16270808/equifax-data-breach-us-identity-theft

Christians, Joost (2016). *Identity Management in Financial Institutions: Digitalisation within Reach?* Tilburg University Master Thesis. Retrieved from http://arno.uvt.nl/show.cgi?fid=142702

Christopher, Allen (2016). The Path of Self Sovereign Identity. C*oindesk.* 27 Apr. 2016. Retrieved from https://www.coindesk.com/path-self-sovereign-identity/

CISCO (2016). *Internet of Things: Connected means informed*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

Clark Jones, A, Fitzpatrick, G., Hartenstein M., and others. Digital Identity. UBS (2016). *The value of our digital identity*. Retrieved from UBS

Clarke, Roger (1994). The Digital Persona and its Application to Data Surveillance. *The Information Society 10,2*. 77-92. Retrieved from http://www.rogerclarke.com/DV/DigPersona.html

The Council Of Europe's Convention On Cybercrime. (2001). European Treaty Series 185. Retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Deloitte (2012). *Is it time to go paperless?: Records management: The cost of warehousing bad habits*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/za/Documents/financial-services/ZA_ItsTimeToGoPaperless_24042014.pdf

Deloitte (2017). Technology, Media & Telecommunications: UK predictions 2017. Retrieved from http://www.deloitte.co.uk/tmtpredictions

European Commission (2016). Questions & Answers on trust services under eIDAS. Retrieved from https://ec.europa.eu/digital-single-market/en/news/questions-answers-trust-services-under-eidas

Van Donselaar, Jan Jaap, Marcel van Kleef & Dominika Rusek (2016). The future of Digital Identity and Internet of Things. *Deloitte*. Retrieved from https://www2.deloitte.com/nl/nl/pages/risk/articles/future-digital-identity-internet-of-things.html

Frenkel, Sheera (2017). Hackers Hide Cyberattacks in Social Media Posts. *The New York Times*. 18 May 2017. Retrieved from https://www.nytimes.com/2017/05/28/technology/hackers-hide-cyberattacks-in-social-media-posts.html

Future Group new ideas for a free and safe Europe (2007). Public security, privacy and technology in Europe: Moving Forward. *European Commission.* Retrieved from http://www.statewatch.org/news/2008/jul/eu-futures-dec-sec-privacy-2007.pdf

Galavski, R. & Robson, C. (2017). Why Financial Institutions (FIs) will drive the Digital ID revolution. *Deloitte.*Retrieved from https://www.linkedin.com/pulse/why-financial-institutions-fis-drive-digital-id-rob-galaski/

Gemalto (2017). Digital identity trends: 5 forces that are shaping 2017. Retrieved from https://www.gemalto.com/govt/identity/digital-identity-trends

Gemalto (2017). National ID cards: 2016-2018 facts and trends. Retrieved from https://www.gemalto.com/govt/identity/2016-national-id-card-trends

Goode Intelligence (2015). Over 1.1 Billion Users of Mobile Biometrics for Financial Services by 2020. Retrieved from http://www.goodeintelligence.com/wp-content/uploads/2016/11/Mobile-Biometrics-For-Financial-Services_Dec15_news_release__04122015_FINAL1.pdf

Grant, J. (n.d.). Identity in Cyberspace: Improving Trust via Public-Private Partnerships. *NIST.* Retrieved from https://www.healthit.gov/sites/default/files/nstic_onc_7.11.12_mtg_grant.pdf

GSMA (2016). R*egulatory and policy trends impacting Digital Identity and the role of mobile: Considerations for emerging markets*. Retrieved from https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf

GSMA (2016b). T*he future of digital identity in building a successful digital society.* Retrieved from https://www.gsma.com/identity/the-future-of-digital-identity-in-building-a-successful-digital-society

Hochstein, Marc (2017). How liability stands in way of banks' digital ID ambitions. *American Banker*. 21 Jun. 2017. Retrieved from https://www.americanbanker.com/news/how-liability-stands-in-way-of-banks-digital-id-ambitions

International Bar Association (2016). *Digital identity: principles on collection and use of information*. Retrieved from https://www.ibanet.org/LPD/Digital_Identity.aspx

IBM (2016). *10 Key Marketing Trends for 2017*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN

IBM (2016). IBM Blockchain Helps FinTechs and Banks Address KYC Challenge. Retrieved from https://www-03.ibm.com/press/us/en/pressrelease/51054.wss

ICAR (2017). *Blockchain technology and its effect on the financial industry*. Retrieved from https://www.icarvision.com/en/blockchain-technology-and-its-effect-on-the-financial-industry

Ienco, Marta (2016). *Digital identity as a key enabler for e-government services*. GSMA. Retrieved from https://www.gsma.com/identity/wp-content/uploads/2016/02/MWCB16-Digital-Identity-as-a-Key-Enabler-for-eGovernment-Services-Marta-Ienco.pdf

Interactions Consumer Experience Marketing, Inc (2014). *Retail's reality: shopping behavior after security breaches*. Retrieved from http://www.retailperceptions.com/pdf/Retail_Perceptions_Report_2014_06.pdf

International Telecommunication Union (ITU) (2010). *Baseline identity management terms and definitions*. Recommendation ITU-T X.1252. Retrieved from http://www.itu.int/SG-CP/example_docs/ITU-T-REC/ITU-T-REC_E.pdf

International Telecommunication Union (ITU) (2017). *Identity and Authentication*. Focus Group Technical Report. Retrieved from https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_Report_IdentityandAuthentication.pdf

ISO/IEC 24760-1:2011: Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts. Retrieved from https://www.iso.org/standard/57914.html

Thomas, Joyrenes (2017). Digital identity: an opportunity for financial services?*Payments, cards and mobile*. 8 June 2017. Retrieved from http://www.paymentscardsandmobile.com/digital-identity-opportunity-financial-services/?utm_content=buffere0e71&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Online identity: is authenticity or anonymity more important?. *The Guardian.* 19 Apr. 2016. Retrieved from https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity

Krotoski, Aleks (2016). Online identity: is authenticity or anonymity more important?. *The Guardian.* 19 Apr. 2016. Retrieved from https://www.theguardian.com/technology/2012/apr/19/online-identity-authenticity-anonymity

Leary, Judy (2016). The Biggest Data Breaches in 2016. *Identity Force*. 16 Dec. 2016. Retrieved from https://www.identityforce.com/blog/2016-data-breaches

Lips, Miriam (2008). Identity management in information age government exploring concepts, definitions, approaches and solutions. *Victoria University of Wellington*. Retrieved from http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/1577/article.pdf?sequence=1

Login Radius (2017). An Introduction To Digital Identity. *LoginRadius Blog*. Retrieved from https://blog.loginradius.com/2017/07/introduction-digital-identity/

Van Liebergen, Bart et al. (2017). Deploying Regtech Against Financial Crime. Institute of International Finance, IIF. Retrieved from https://www.iif.com/publication/research-note/deploying-regtech-against-financial-crime

McGrory, Ramsey (2013). The Data Providers: One Quadrant Chart To Rule Them All. *ad exchanger*. 21 Feb. 2013. Retrieved from https://adexchanger.com/data-driven-thinking/the-data-providers-one-quadrant-chart-to-rule-them-all/

Nordseth, Gunnar (2017). A year of new regulations and new opportunities. *Signicat.* 28 Mar. 2017. Retrieved from https://www.signicat.com/blog/2017-year-new-regulations-new-opportunities/

Nordseth, Gunnar (2017). Are we heading for an identity crisis in fintech? *Fintech Futures.*4 Jan. 2017. Retrieved from http://www.bankingtech.com/2017/01/are-we-heading-for-an-identity-crisis-in-fintech/

OECD (2007). *At a crossroads: "Personhood" and Identity in the information society*. STI Working Paper 2007/7. Retrieved from https://www.oecd.org/sti/ieconomy/40204773.doc

OECD (2008). *The Scoping Paper on Online Identity Theft: Ministerial Background Report DSTI/CP(2007)3/FINAL*. Retrieved from http://www.oecd.org/sti/40644196.pdf

OECD (2011). *Digital Identity Management for Natural Persons*. Retrieved from http://www.oecd-ilibrary.org/science-and-technology/digital-identity-management-for-natural-persons_5kg1zqsm3pns-en?crawler=true

OECD (2009). The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers, *OECD Digital Economy Papers, No. 160*, OECD Publishing, Paris. Retrieved from http://dallenx.doi.org/10.1787/222134375767

OECD (2015). *Developments in digital identity. SPDE Roundtables 1-2 December 2015*. Retrieved from https://one.oecd.org/document/DSTI/ICCP/REG(2015)12/en/pdf

OpenID Foundation (n.d.). *What is OpenID?* Retrieved from https://openid.net/what-is-openid/

Pentland, A.,Shrier, D., Hardjono, T., & Wladawsky-Berger, I. MIT (2016). *Towards an Internet of Trusted Data: A New Framework for Identity and Data Sharing.* Retrieved from https://www.nist.gov/sites/default/files/documents/2016/09/16/mit_rfi_response.pdf

Perez Burgueño, P. (2012). *Aspectos jurídicos de la identidad digital y la reputación online.* Retrieved from http://www.adcomunicarevista.com/ojs/index.php/adcomunica/article/view/50

Platt, Moritz (2014). *Secure Authentication and Attribute Sharing in Federated Identity Scenarios*. Retrieved from https://www.slideshare.net/mritzp/secure-authentication-and-attribute-sharing-in-federated-identity-scenarios

PWC. *The future of onboarding*. Retrieved from https://www.pwc.com/gx/en/financial-services/pdf/pwc-the-future-of-onboarding.pdf

Rennie, D., McEvoy, J. (2016). *The value of digital identity to the financial sector*. Gov.UK Verify. Retrieved from ability

Republic of Estonia, Information System Authority (n.d.) *XRoad Factsheet*. Retrieved from https://www.ria.ee/public/x_tee/X-road-factsheet-2014.pdf

Rodrigues, Rowena Edwardina (2011). Revisiting the legal regulation of digital identity in the light of global implementation and local difference*. The University of Edinburgh Law thesis and dissertation collection.* Retrieved from http://hdl.handle.net/1842/8942

Roosendaal, Arnold (2010). Digital personae and profiles as representations of individuals. In M. Bezzi, P. Duquenoy, S. Fischer-Hübner, M. Hansen, & G. Zhang (Eds.), *Privacy and identity management for life* (pp. 226-236). Tilburg University. Retrieved from https://pure.uvt.nl/ws/files/1261497/Roosendaal_Digital_Personae_and_Profiles_as_Representations_of_Individuals_100831.pdf

Sarma, Amardeo & João Girão (n.d.). *Identities in the Future Internet of Things*. Retrieved from http://www.girao.org/joao/papers/wpc2009.pdf

Segovia, Ana (2017). Behavioural biometrics, a step further in digital identification for financial services. *Digital Economy Outlook. April 2017*. BBVA Research. Retrieved from https://www.bbvaresearch.com/wp-content/uploads/2017/04/DEO_apr17_eng_Cap_05.pdf

Skinner, C. The impossible dream: a digital identity for everyone. (2016) *The Finanser*. Retrieved from http://thefinanser.com/2016/05/impossible-dream-digital-identity-everyone.html/

Sharma, Ankur (n.d.). Why Your Digital Identity is the Base of all Business on the Internet? *Loginradius blog*. Retrieved from https://blog.loginradius.com/2016/01/digital-identity-base-of-all-web-business/

Smedinghoff, Thomas (2011). Introduction to Online Identity Management. *UNCITRAL 2011*. Retrieved from https://www.uncitral.org/pdf/english/colloquia/EC/Smedinghoff_Paper_-_Introduction_to_Identity_Management.pdf

Telefonica. (2016). *New Paradigms of Digital Identity: Authentication and Authorization as a Service (AuthaaS).* Retrievedf from https://www.elevenpaths.com/es/new-paradigms-of-digital-identity-authentication-and-authorization-as-a-service-authaas-2/index.html

Telecom News (2017).Telcos, banks can save up to Rs 10,000 crore, thanks to e-KYC.Retrieved from https://telecom.economictimes.indiatimes.com/news/telcos-banks-can-save-up-to-rs-10000-crore-thanks-to-e-kyc/51456336

Telus (2016). Demystifying Digital Identity: A Matter of Trust.IT World Canada. Retrieved from https://www.itworldcanada.com/sponsored/demystifying-digital-identity-a-matter-of-trust

The Telegraph. *How the government plans to 'verify' your identity online.* Retrieved from http://www.telegraph.co.uk/technology/news/11150072/How-the-government-plans-to-verify-your-identity-online.html

Theodorou, Yiannis (2016). Digital Identity: Regulatory trends and the role of mobile. *GSMA*, 3 Nov. 2016. Retrieved from https://www.gsma.com/mobilefordevelopment/programme/digital-identity/digital-identity-regulatory-trends-and-the-role-of-mobile

United Nations Commission on International Trade Law, UNCITRAL (1996). *Model Law on Electronic Commerce with Guide to Enactment*. Vienna: United Nations. Retrieved from https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

Urbiola, Pablo (2016). General Data Protection Regulation. *Digital Economy Outlook*. May 2016. BBVA Research

Vassil, Kristjan (2015). Estonian e-Government Ecosystem: Foundation, Applications, Outcomes. *World Development Report 2016: Digital dividends. Background paper*. [Washington DC]: The World Bank Group. Retrieved from http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf

Velasco, Jessica (2016). 4 Case Studies in Fraud: Social Media and Identity Theft. *Socialnomics*. 13 Jan. 2016. Retrieved from https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

World Bank (n.d.). *Identification for Development (ID4D)*. Retrieved from https://secureidentityalliance.org/public-resources/4-july-2016-report-digital-identity/file http://www.worldbank.org/en/programs/id4d

World Bank (2016). Digital Identity. Enabling digital development. *World Development Report*. Retrieved from http://documents.worldbank.org/curated/en/896971468194972881/310436360_20160263021000/additional/102725-PUB-Replacement-PUBLIC.pdf

World Bank Group, GSMA & Secure Identity Alliance (2016). *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation: Discussion paper.* Washington DC: International Bank for Reconstruction and Development / The World Bank. Retrieved from https://secureidentityalliance.org/public-resources/4-july-2016-report-digital-identity/file

World Economic Forum & Deloitte (August 2016). *A Blueprint for Digital Identity The Role of Financial Institutions in Building Digital Identity*. Retrieved from http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

X-Infotech (2016). Security Document World.*Friends and frenemies in the eID market*. Retrieved from http://www.securitydocumentworld.com/article-details/i/12899/

Yurcan, Bryan (2016). The Future of Digital Identity Is Up to Banks. *American Banker*. 27 March 2016.Retrieved from https://www.americanbanker.com/news/the-future-of-digital-identity-is-up-to-banks

Yurcan, Bryan (2016). How Blockchain Fits into the Future of Digital Identity. *American Banker*. 8 Apr. 2016. Retrieved from https://www.americanbanker.com/news/how-blockchain-fits-into-the-future-of-digital-identity

Yurcan, Bryan (2017). Banks can profit from digital ID movement (even if they don't control it). *American Banker*. Retrieved from https://www.americanbanker.com/news/banks-can-profit-from-digital-id-movement-even-if-they-dont-control-it

BBVA | Research

Working Papers

2018

18/01 **Ana I. Segovia Domingo and Álvaro Martín Enríquez:** Digital Identity: the current state of affairs.

2017

17/23 **Ángel de la Fuente:** Series largas de algunos agregados económicos y demográficos regionales: Actualización de RegData hasta 2016.

17/22 **Ángel de la Fuente:** Series enlazadas de algunos agregados económicos regionales, 1955-2014. Parte II: Otras variables de empleo, rentas del trabajo y paro.

17/21 **Ángel de la Fuente:** La evolución de la financiación de las comunidades autónomas de régimen común, 2002-2015.

17/20 **Maximo Camacho, Matias Pacce and Camilo Ulloa:** Business cycle phases in Spain.

17/19 **Ángel de la Fuente:** La liquidación de 2015 del sistema de financiación de las comunidades autónomas de régimen común.

17/18 **Víctor Adame y David Tuesta:** The labyrinth of the informal economy: measurement strategies and impacts.

17/17 **Víctor Adame y David Tuesta:** El laberinto de la economía informal: estrategias de medición e impactos.

17/16 **Liliana Rojas-Suárez y Lucía Pacheco:** Índice de prácticas regulatorias para la inclusión financiera en Latinoamérica: Facilitadores, Promotores y Obstaculizadores.

17/15 **Liliana Rojas-Suárez y Lucía Pacheco:** An Index of Regulatory Practices for Financial Inclusion in Latin America: Enablers, Promoters and Preventers.

17/14 **Ángel de la Fuente:** Las finanzas autonómicas en 2016 y entre 2003 y 2016.

17/13 **Carlos Casanova, Joaquín Iglesias, Álvaro Ortiz, Tomasa Rodrigo y Le Xia:** Tracking Chinese Vulnerability in Real Time Using Big Data.

17/12 **José E. Boscá, Rafael Doménech, Javier Ferri y José R. García:** Los Desplazamientos de la Curva de Beveridge en España y sus Efectos Macroeconómicos.

17/11 **Rafael Doménech y José Manuel González-Páramo:** Budgetary stability and structural reforms in Spain: lessons from the recession and options for the future.

17/10 **Ángel de la Fuente:** Series enlazadas de algunos agregados económicos regionales, 1955-2014. Parte I: Metodología, VAB, PIB y puestos de trabajo.

17/09 **José Félix Izquierdo:** Modelos para los flujos de nuevo crédito en España.

17/08 **José María Álvarez, Cristina Deblas, José Félix Izquierdo, Ana Rubio y Jaime Zurita:** The impact of European banking consolidation on credit prices.

17/07 **Víctor Adame García, Javier Alonso Meseguer, Luisa Pérez Ortiz, David Tuesta:** Infrastructure and economic growth from a meta-analysis approach: do all roads lead to Rome?

17/06 **Víctor Adame García, Javier Alonso Meseguer, Luisa Pérez Ortiz, David Tuesta:** Infraestructuras y crecimiento: un ejercicio de meta-análisis.

17/05 **Olga Cerqueira Gouveia, Enestor Dos Santos, Santiago Fernández de Lis, Alejandro Neut y Javier Sebastián:** Monedas digitales emitidas por los bancos centrales: adopción y repercusiones.

17/04 **Olga Cerqueira Gouveia, Enestor Dos Santos, Santiago Fernández de Lis, Alejandro Neut and Javier Sebastián:** Central Bank Digital Currencies: assessing implementation possibilities and impacts.

17/03 **Juan Antolín Díaz and Juan F. Rubio-Ramírez:** Narrative Sign Restrictions for SVARs.

17/02 **Luis Fernández Lafuerza and Gonzalo de Cadenas:** The Network View: applications to international trade and bank exposures.

17/01 **José Félix Izquierdo, Santiago Muñoz, Ana Rubio and Camilo Ulloa:** Impact of capital regulation on SMEs credit.

2016

16/21 **Javier Sebastián Cermeño:** Blockchain in financial services: Regulatory landscape and future challenges for its commercial application

16/20 **Máximo Camacho and Matías Pacce:** Forecasting travelers in Spain with Google queries.

16/19 **Javier Alonso, Alfonso Arellano, David Tuesta:** Factors that impact on pension fund investments in infrastructure under the current global financial regulation.

16/18 **Ángel de la Fuente:** La financiación regional en Alemania y en España: una perspectiva comparada.

16/17 **R. Doménech, J.R. García and C. Ulloa:**The Effects of Wage Flexibility on Activity and Employment in the Spanish Economy.

16/16 **Ángel de la Fuente:** La evolución de la financiación de las comunidades autónomas de régimen común, 2002-2014.

16/15 **Ángel de la Fuente:** La liquidación de 2014 del sistema de financiación de las comunidades autónomas de régimen común: Adenda.

16/14 **Alicia García-Herrero, Eric Girardin and Hermann González:** Analyzing the impact of monetary policy on financial markets in Chile.

16/13 **Ángel de la Fuente:** La liquidación de 2014 del sistema de financiación de las comunidades autónomas de régimen común.

16/12 **Kan Chen, Mario Crucini:** Trends and Cycles in Small Open Economies: Making The Case For A General Equilibrium Approach.

16/11 **José Félix Izquierdo de la Cruz:** Determinantes de los tipos de interés de las carteras de crédito en la Eurozona.

16/10 **Alfonso Ugarte Ruiz:** Long run and short run components in explanatory variables and differences in Panel Data estimators.

16/09 **Carlos Casanova, Alicia García-Herrero:** Africa's rising commodity export dependency on China.

16/08 **Ángel de la Fuente:** Las finanzas autonómicas en 2015 y entre 2003 y 2015.

16/07 **Ángel de la Fuente:** Series largas de algunos agregados demográficos regionales, 1950-2015.

16/06 **Ángel de la Fuente:** Series enlazadas de Contabilidad Regional para España, 1980-2014.

16/05 **Rafael Doménech, Juan Ramón García, Camilo Ulloa:** Los efectos de la flexibilidad salarial sobre el crecimiento y el empleo.

16/04 **Angel de la Fuente, Michael Thöne, Christian Kastrop:** Regional Financing in Germany and Spain: Comparative Reform Perspectives.

16/03 **Antonio Cortina, Santiago Fernández de Lis:** El modelo de negocio de los bancos españoles en América Latina.

16/02 **Javier Andrés, Ángel de la Fuente, Rafael Doménech:** Notas para una política fiscal en la salida de la crisis.

16/01 **Ángel de la Fuente:** Series enlazadas de PIB y otros agregados de Contabilidad Nacional para España, 1955-2014.

Click here to Access the Working Paper published

Spanish

and English

Contact details:
BBVA Research
Calle Azul, 4
Edificio La Vela – plantas 4 y 5
28050 Madrid (Spain)
Tel.: +34 91 374 60 00 and +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com