IDENTITY MANAGEMENT AND ITS IMPACT ON THE DIGITAL ECONOMY

October 18, 2016.
Room Andrés Bello 3

IDB
Improving lives

Identity Management
and its impact on the Digital Economy

Alejandro Barros[1], Alejandro Pareja[2]

October 2016

Contents

Introduction

This document aims to provide information about the topics that will be covered in the seminar titled “Identity Management and its Impact in Digital Economy". It consists of two sections. The first one describes the main aspects of identity management and its economic impact. The second section mentions the current alternatives and challenges, which will be developed during the seminar.

Legal identity and a reliable **national identification system** are fundamental in order to have **access to a number of services,** both public (e.g., education, health, security, justice,

---

[1] Alejandro Barros, International Consultant, abc@alejandrobarros.com, www.alejandrobarros.com

[2] Alejandro Pareja, Modernization of the State specialist, Institutions for Development (IFD)
Institutional Capacity of the State Division (ICS), Inter-American Development Bank, http://www.iadb.org/, apareja@iadb.org

social benefits and electronic government in general) and private (e.g., financial, retail and commercial services). On the other hand, national identity systems have to **contribute to reducing transaction costs, facilitating public policy execution, improving public service quality and satisfaction, and developing the private sector.**

National identification systems comprise not only all the institutions responsible for offering identity-related services but also the consideration of all demand-side stakeholders. Demand is represented basically by **three participants: citizens, enterprises and the own government.**

Identity management is the combination of processes and systems, that foster the use and usability of people's identifying data. Both, management and use have to adhere to personal data protection regulations and be effective, secure and citizen-centric. Identity management requires: 1) a **governance model and a business model**; 2) an appropriate, up-to-date **legal framework**; 3) the **simplification and standardization of processes and systems**; 4) the establishment of **interoperability** mechanisms that facilitate coordination between the different organisms, and 5) the promotion and coordination of the **identity ecosystem**.

With the arrival of **digital economy**, transactions and interactions (which were done in person before) started to be carried out more and more through interconnected information systems and the Internet (on-line interactions). This has made necessary to consider the **digital identity** of every person, which is understood as the hardware or software elements that allow a person to be identified and authenticated; obtain permission to access to certain information resources, and carry out transactions through the Internet or private networks.

Identity Management

People and both public and private organisations require to verify reliably the identity of the other party for many types of interaction. Until a few years ago, the identification process was based on physical credentials which one way or another proved their holder's identity, such as national ID cards, driving licenses or other documents.

In the world of information systems that operate in the Internet, this identification process has gotten complex. Nowadays, it is necessary to identify people remotely without physical interaction; without knowing the other party previously in most cases, and often having the process carried out by a computer. On the one hand, this implies challenges regarding privacy, data protection, and likelihood of fraud. On the other hand, this implies the need to check and adjust technologies, governance schemes and legal frameworks[3] that may be getting outdated.

In this complex new context, the process of people identification depends on what the final objective is, i.e. the interactions and/or action that are wanted to be carried out. The following table shows the main cases of use.

[3] Laws that regulate the use of Electronic Signature

Interaction types	Description	Example of mechanism	Example of use
Register into a information system	Creation of a user in a new site or private network	In some cases, the registration as a user can be done online, while in others it has to be done in person. In the first case, a one-time password[4], which is sent to the user's phone or mailbox, is typically used. In the second case, the password is received personally and the person who receives it assumes the responsibility for the digital identity.	Digital identity in Chile – *Sistema Clave Única*[5] (a single electronic identity for getting access to all of the online government services enabled for that).
Identifying oneself and being authenticated	It takes place when a person tries to **get access** to some information system.	User and password	Accessing to websites
Obtaining **authorisation** for accessing a particular information resource or a service	There may be a pre-established permission scheme according to the different user profiles or it may be required for a complementary authentication request with the objective to increase the security level in high-risk operations.	Generally, second password or one-time password mechanisms are used.	Electronic funds transfer (EFT)
Giving permission	The user gives permission for an action	Electronic signature (digital certificates)	Contract signature

This identity management process may require multiple activities. Some of these may be done personally and others may be done remotely. Identity management has to consider the whole process: 1) the birth registration; 2) the enrolment in an identity system with the respective concession of a physical or digital[6] credential; 3) the use of the digital credential in the platforms for which it was intended (including

[4] An example of one-time password (OTP) is the numeric code sent to some device that the user has (mobile phone, e-mail, among others).

[5] Clave Única - https://www.claveunica.gob.cl/

[6] A digital credential is an identifier used by a person to interact with an information system. For example: user and password, digital certificate or biometric information (fingerprint, iris, etc.).

attributes and permission); 4) the potential revocation as a result of security problems (identity theft) or expiration, and 5) removal from the system. The system has to ensure the security and traceability of the information in compliance with the organisation's regulations or even with national or international regulations.

Enrolment in the National Identity System

Enrolment is the process through which a person is given a unique identity number after having his or her filiation information and registered. In countries that have a national identity document, it is usual to register other biometric data and the images of the fingerprints too. Some countries, such as India, have also started to register images of irises.

In some cases, one or more chips (where the registered personal information is recorded, including fingerprint minutiae for comparisons) and occasionally a digital certificate for electronic signature are added to the document[7]. In these cases, in order to make use of the digital identity recorded in the document, the person will require a device that will allow the reading data of the document (chip reading).

Digital Identity Authentication

With regards to digital economy, the main activity of the identity management process is the authentication. Historically, the authentication has been based in three elements (factors) that, depending on the risk level of the process to be carried out, are used to improve the method's reliability and robustness. These three factors are:

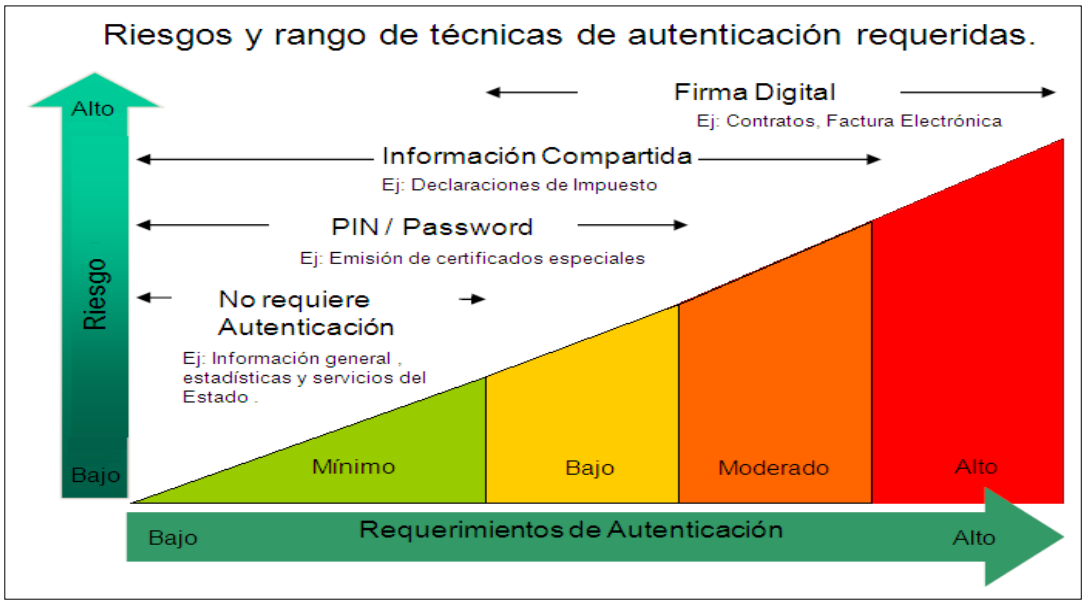
	Description	Examples of use
Something the **person knows**	It refers to something the person knows, keeps in secret and uses when registering.	• User and password or PIN (personal identification number) • Challenge (secret-answer question)
Something the **person is**	It refers to some physical feature of the person, usually known as biometric characteristic.	• Fingerprints • Iris images • Face shape • Voice
Something the **person has**	It refers to some physical or technological element the person has.	• Identity document, particularly the electronic one (known as eID or eDNI in Spanish) • Smart card, for example, credit card. • Token-like device • Digital certificate installed in a PC or in the cloud • Certificate installed in some device (smart card, USB token, mobile phone[8])

[7] This document is usually known as National Identity Document or National ID Card.

[8] In the case of mobile phone use, this has been solved using a second chip, which serves as certificate repository. In general, telecommunication companies do not play a role in the management of the second chip.

Best practices indicate that a combination of at least two of these factors should be used for high-risk operations. In order to define the security level that corresponds to each case of use, not only the intrinsic risk should be considered, but also the type of interaction. The following illustration presents a diagram of the different possibilities.

Illustration 1: Management of credentials



Source: Own preparation

In the public world, digital authentication mechanisms are pretty basic at least in the region. In general, it is the user and password mechanism the one that is used. Regarding the digital signature, even though many countries of the region have regulated its use through laws on the subject, digital signature diffusion and utilisation are still very incipient. Probably this is the result of the usability difficulties that such mechanism has, which derive from the necessity of having a reader of the device where the certificate is stored (smartcard, USB token[9] or other).

In the region, the experiences of identity documents that include digital identification elements (certificates for signature, fingerprint minutiae or other personal data) are either incipient (e.g., Uruguay) or have not been successful in utilisation (e.g., Chile).

Nowadays, some complementary adaptive-type mechanisms have been adopted for some online services in order to authenticate people based on the user or client history (their navigation profile, geolocation, profile based on the use of social networks, etc.) as an additional security element.

[9] Example of a USB token - http://www.safenet-inc.es/multi-factor-authentication/authenticators/pki-usb-authentication/etoken-pro/

On the other hand, it is interesting to highlight some companies that have established business models (complementary to their current businesses) related to authentication (identity providers). That is the case of Google[10], Facebook[11] and others, which are being used by multiple public and private organisations as authentication mechanisms.

Identity Systems Governance

There are several governance models for identification systems. There are countries where a central public entity has specific capabilities, in terms of birth registration and enrolment in a national identification system (along with the corresponding issuing of a physical ID document.) In this category, all Hispanic American countries can be found.

On the other hand, there are countries that do not have a central public institution that takes part in enrolling and in issuing national ID documents (including, Canada, the US, the UK[12] and many Caribbean countries.) In such cases, de facto IDs can usually be obtained. As examples, we can mention: driving license, proof of social security, passport and/or election document. The aforementioned identification documents coexist and each social actor has the responsibility of defining which kind of ID document accepts as a proof of identity. In some cases, the multiplicity of identification-issuing agencies increases the risk of fraud, mainly when coordination between different agencies is weak.

Both in the Hispanic American and Anglo-Saxon systems, the accepted ID documents are derived from birth registration (either national or international), which is always the cornerstone of the system.

In some countries, both the identification number and document are issued from birth. In other countries, these types of documents are obtained, for example, when opening a bank account, when getting a driving license or in the case of voting.

As for digital identity, there are Hispanic American countries where the governing bodies of the identification system also manage digital identity, particularly for its use in relation to the state. In no case it is an exclusive supplier, but the trend is rather that each body implements its own authentication mechanism. Nonetheless, some countries of this region, like Chile and Uruguay, are making progress in the implementation of a single sign-on[13] scheme for the public sector. In some cases, the major driver of digital identity for the public sector is the civil registration office, while in other cases is the body responsible for electronic government.

[10] Google Cloud Identity & Access Management - https://cloud.google.com/iam/
[11] Facebook Connect - https://developers.facebook.com/docs/facebook-login
[12] A timeline showing what has happened with ID cards in the UK - http://www.bbc.com/news/10164331
[13] It is a property of access control in which users log in using the same username and password in any website, in this case, a government website.

Also, in countries that hold Saxon traditions, digital identity is managed in a distributed fashion (with no specific manager), having cases in which federated systems[14] are utilised, and also cases where different identification-issuers are not coordinated. In some cases, part of the management is outsourced, being the case of Chile, where the production of ID cards is handed over to an external supplier[15].
In the private sector, especially in the case of financial institutions, a tendency to develop self-standards for digital identity management is observed. This occurs due to criticality and the risks of the authentication process for this kind of institutions, and implies that there are few experiences of outsourcing service.

Financing Identity Management

Concerning basic ID (which is reflected in an identification document), provider institutions are financed by charging citizens for the document itself (even in the cases where it is mandatory) and through budgetary contributions, in proportions that vary depending on the case. These institutions also usually sell services related to identification[16], both to the private sector (particularly to the banking sector) and to the rest of the public sector.

The identity management systems, in many cases, are operated directly by the governmental institution, whose mandate is to register identification[17] of the people, as in the case of Uruguay. Other countries have outsourced some activities of the process, like Chile, which has externalised the production of cards and passports, an activity that is carried out by an external provider[18].

As for digital identity, there is normally little awareness of the involved costs associated with identity management, both in the private and public world. It is very common that these costs are included as part of the total cost of the technological platform. This makes it difficult to visualise alternatives with better cost-effectiveness.

[14] Fedarated Identity: individuals can use the same personal identification for logging into networks and systems of different areas or institutions - https://en.wikipedia.org/wiki/Federated_identity
[15] Morpho, French enterprise
[16] For example, a request for affiliation of a person using his/her fingerprints.
[17] Civil Registration Office
[18] Morpho - http://www.morpho.com/

In the following table the main cost components of digital identity management are shown:

Cost item	Description
Enrolment and revocation	• For low-risk services, enrolment may be conducted remotely, in an automated way and, consequently, with a low cost. However, when the service requires high-security mechanisms, it is very likely that the enrolment should be done onsite, so that the user can provide his/her ID, photo or fingerprints and can sign a contract of use. This implies considerable costs, both for the institution and the user (service offices, time, travels, authentication mechanisms, etc.) • In cases where the digital identity is included in the identity card, the enrolment process is subsumed in the process of obtaining the document. • As for revocation, resources must be allocated to attend to incidents that require locking and possible revoking of digital certificates, as a consequence of identity theft, death, etc.
Information management	• Corresponds to the technological support used, databases, encryption process and management of certificates (PKI platform[19]), software for managing identification data and other cyber security measures.
Devices	• Corresponds to the costs of devices that store credentials (tokens, smart cards), device readers, or the service that provides dynamic passwords.
User support	• Call centre to give support to final users, for instance, when a user forgets his/her password.

The following table shows, for reference, an estimate of annual operative costs of identity management per user. Values correspond to different studies undertaken for financial institutions and banks in the region (this estimates include the different cost items described in the previous table):

Type of mechanism	Annual cost per user (US$)
User-password	10
Dynamic password (one time password)	20
Digital signature (includes the cost of both the certificate and the storage device)	50

Source: compilation based on data from the financial industry

[19] *Public Key Infrastructure* is a platform used to generate, manage and revoke digital certificates that allows safely encrypting and decrypting communications and documents for the involved parties.

Economic Impacts of Digital Identity

From an economic perspective, we may consider two sets of consequences related to digital identity: on the one hand, impacts arising directly from digitalisation of existing processes that were previously only offered in person and, on the other, impacts associated with the emergence of new services and economic activities as a consequence of digital identity usage.

Having digital identity is a basic requirement for making online transactions. Therefore, all the benefits that the online mode brings, both in effectiveness and quality perceived by users, are possible thanks to a reliable system of digital identity.

It is therefore relevant to analyse the costs associated with the different channels of customer service, both for the institution and users. The table below shows the costs of three channels of customer service (in person/on-site, telephone support and online support) in some countries, expressed in US$ per transaction[20]).

Channel	Canada	UK	Norway	Australia
In person/on-site	7,42	15,32	14,01	19,61
Phone support	4,57	5,89	7,01	7,66
Online self-service	0,11	0,44	0,53	0,46

Source: K. Kernaghan – Brock University (2012), Transforming local public services using technology and digital tools and approaches – Local Government Association (2014), Digital government transformation – Deloitte Commissioned by Adobe (2015)

A very significant difference can be seen between the costs of online and on-site channels of customer service. In order to complete the impacts analysis, it is important to consider savings for users that utilise online channels, primarily by saving time and travels. This exhibits a greater impact. It is very difficult to determine this money-saving but, without doubt, it could be possible to make estimates in a man-hour (corresponding to an average income) per transaction.

Even though money-savings for citizens are clearly positive, it should be mentioned that by bringing services to virtual channels, a costs externalisation of these channels is taking place, for example, because of the need to have a device for logging in, the costs of digital certificates, connectivity services, etc.

With regards to the new economic activities emerged from the need for digital identity management, the following can be mentioned:

- Cyber security, which corresponds to all necessary mechanisms and systems (software, hardware) to ensure a good level of security in identification processes.

[20] In the private sector, that is, financial industry, similar costs are seen between onsite and remote channels.

- Development of software associated with the implementation of identification platforms, which is the case of the development of the single sign-on platforms that were mentioned earlier.

- Establishment of private authentication services, like the ones mentioned earlier (Facebook Connect, Google and others.) Technological operation of authentication platforms.

- Development and production of authentication devices (tokens, smart cards and dynamic password systems.)

- As for the case of digital certificates, there are other related activities, such as certificate providers, certificate-issuer enterprises[21] and devices for its storage (token, smart cards.)

- Some activities are reduced or simply disappear, such as all activities associated with customer service processes (counter, personnel, etc.) As a result of online interaction, the number of customer service offices and their associated costs must also be adjusted.

Challenges and Issues to Discuss in the Seminar

After reviewing the current context of identity management, the main challenges will be discussed in this section and will be then analysed during the seminar. Some of the factors that should be addressed when defining a model of eID are:

- Regarding **enrolment for basic identification** (which is reflected in the ID document) and, in such cases where biometric data is collected, our region has based on taking fingerprints, initially from one or two fingers and with a clear tendency to register all ten fingers. On the other hand, the Aadhaar project[22] from India carries out enrolment by taking all ten fingerprints, but also by capturing the image of the irises. It could be discussed which will be the tendency in the future and **whether it will be necessary or convenient that our countries implement an enrolment system that includes irises images or another biometric element (advantages and disadvantages).** In addition to specific technical considerations of the authentication process, privacy and usability aspects should be considered.

- With respect to **identity documents**, taking into consideration that (at least theoretically) biometric authentication could be done directly without data being saved in a card (through a scanner that captures the image which is

[21] In some countries there are certificate providers, both private enterprises and public issuers.
[22] https://uidai.gov.in/beta/

then transmitted to ABIS[23]), the question is **whether it is possible and convenient to move towards identity systems without a physical document (advantages and disadvantages).**

- As digital identity systems have been developed, both public institutions and enterprises maintain databases with **personal information from users.** Beyond the risks of theft of such information, there are risks concerning inappropriate use of it. The question is **whether it is possible to give users the chance of having control, either partially or totally, over who keeps their identity data, along with the capacity of authorising which data can be shared with which organisation and under what conditions.** It would be necessary to know which regulation is required and what would be the best way to implement such mechanism.

- What is the **most appropriate institutional framework**, in terms of efficiency and service quality, for digital identity management? What are the advantages and disadvantages of maintaining a decentralised process (with even uncoordinated actors) with respect to a more centralised one (with one or a small number of digital identity managers, with the eventual establishment of a trust framework between them)?

- **Should the state force all citizens to have digital identity?** What are the advantages? Why are there, among countries with an advanced information society development, countries that impose this obligation and those where there is no regulation whatsoever? The fact that a person has digital identity, does contribute to the development of both the electronic government and information society? or does not alter the levels of digital services usage?

- Which **identity management processes** that function in the public sector, have room for **collaboration with the private sector**? **Which processes would be possible or convenient to outsource?** Where can the private sector add more value than the public sector? Regulatory and technical aspects that should considered.

- Concerning **regulatory frameworks**, what changes are being required? For example, for the purpose of contemplating safe and appropriate management of databases that contains personal information from users, or for the purpose of contemplating the new technological possibilities, in terms of digital certificates for digital signatures.

- What are the actual levels of digital signature usage at a global scale? What are the most used types of **digital signature** and what are the trends associated with this aspect?

[23] Automated Biometric Identification System compares a biometric image against an image database to verify which corresponds with it. In the case of fingerprints, it is called AFIS (Automated Fingerprint Identification System).

- **Fraud and identity theft:** what are the main risks of fraud and phishing that may affect the identification process of the people? How are these risks mitigated?

- Should governments intervene in the extension of usage of digital identity? What are the projects and policies to be developed?[24]

- **Process of adoption of universal digital identity, lessons learned:** There are various examples of mass dissemination projects about identity and digital signature (the latter generally associated with the identification document) that were not accompanied by the adoption that was expected from citizens and enterprises. In other successful cases, adoption has been very gradual. What are the lessons learned about this? What could have been done differently in each case? What are the reasonable expectations about this?

- What kind of new services could arise in relation to identity? Are there services that become obsolete?

- **Cost analysis:** It is important to identify costs associated with digital identity management. This analysis can be an important resource for the national strategy, institutional design and regulatory update.

[24] https://www.theguardian.com/technology/2014/nov/06/govuk-quietly-disrupts-the-problem-of-online-identity-login