Inter-American Development Bank

Institutional Capacity and Finance Sector

TECHNICAL NOTES

No. IDB-TN-196

Identification and Governance Policies

The Legal, Technical, and Institutional Foundations that Influence the Relations and Interactions of the Citizen with the Government and Society

Mia Harbitz
Iván Arcos Axt

September 2011

Identification and Governance Policies

The Legal, Technical, and Institutional Foundations that Influence the Relations and Interactions of the Citizen with the Government and Society

Mia Harbitz
Iván Arcos Axt

Inter-American Development Bank
2011

http://www.iadb.org

The Inter-American Development Bank Technical Notes encompass a wide range of best practices, project evaluations, lessons learned, case studies, methodological notes, and other documents of a technical nature. The information and opinions presented in these publications are entirely those of the author(s), and no endorsement by the Inter-American Development Bank, its Board of Executive Directors, or the countries they represent is expressed or implied.

1300 New York Ave. NW, Washington D.C., U.S.A.
Contact: Mia Harbitz (MIAH@iadb.org)

Abstract[*]

The conceptual framework for this discussion and technical note focuses on the fundamental principles that govern the relationship and interactions between the citizen, government, and society (also denominated C2G, C2B and G2B). Due to the speed with which the interfaces and virtual interactive processes between the citizen and the State are growing, the instances in which the authentication and authentication of one's identity are required are also increasing.

It is a concern that policies relating to legal identity and personal identification are not being developed at a similar velocity. This technical note seeks to shed light on some of the principles that deserve further attention in the public debate and, although it focuses on the frameworks that govern civil registration and identification, the fundamental principles examined here are also valid within the context of the interoperability of other registers which, however, fall outside the scope of this paper.

There is a *sine qua non* requirement at the core of any system of electronic government that seeks to facilitate transactions: the verification of the identity of the entities, or of the contracting parties, that participate in said transactions. The cornerstone is the citizen's legal, unique, safe, and verifiable identity. Three fundamental parameters must be in place before electronic transactions can be carried out: a legal framework at the macro level, an institutional framework at the meso level and, at the micro level, a technological framework that enables transactions to be made.

Keywords: Identity management, civil registration, identification, interoperability, e-government

JEL Codes: 031, 033, 038

[*] Mia Harbitz is a Senior Specialist at the Institutional Capacity of State Division of the Institutional Capacity and Finance Sector (ICF/ICS) and Iván Arcos Axt is a consultant with the IDB.

Table of Contents

INTRODUCTION

At present, information and communications technology (ICT) systems are employed by the public sector to provide solutions for electronic government. This requires government to function in an integral manner, so that service provision and implementation can be oriented towards citizens, the so-called citizen-centric approach.

In order to achieve citizen-centric service provision, various countries have developed interoperability architectures that are designed to integrate public services and thereby make them easier to access. Interoperability architecture can be defined as the combination of policies and technical components needed to enable data exchange and verification between diverse State-entity information systems. Systems, however, that permit interoperability between databases or information systems do not always adequately consider ex ante the legal and organizational dimensions needed to protect users from fraud or identity theft.

At the same time, the arrival of the Web 2.0 (O'Reilly, 2006) has meant that the rules governing personal virtual interaction and communication have changed and become more complex. Many of the changes have occurred with little prior discussion and many of them, however positive they may be, have ramifications that sometimes leave the citizen defenseless. Of particular interest among these changes is the introduction, within the computing community, of the concept of Identity 2.0. This idea, however, only refers to a simple open code designed to facilitate those Internet transactions that require the identification of the interested parties.

The following examples of some of the milestones that have signaled important changes are worth mentioning: i) Facebook, a website designed for users to share information; it recently reached 500 million users. Much of the information shared is of a personal nature; ii) the announcement by the CEO of Google, the world's biggest and most important search engine, that "No anonymity is the future of the Web," iii) the implementation of electronic government policies and their promotion by multinational organisms; and iv) post-September 11 security issues that have influenced the creation and existence of new identification systems. These facts, which might at first seem unconnected, portray a situation that has only recently been considered a global phenomenon: the growth in the use of ICTs and the need for a means of verifying and accrediting identity that provides adequate levels of security and interoperability in the use of these new technological instruments. In turn, the importance of matters such as the protection of personal information, the legal typification of related offences, personal information property rights, database interoperability and smart identity cards for use in secure commercial transactions has also been revealed. Governments tend to tackle these matters in different ways and with diverse emphasis. The policies that relate to these matters, however, require a common base to sustain them and make them viable, which is the institutional capacity of the government that sets the policies. In countries lacking adequate institutional conditions, the policies implemented will be less effective, no matter how modern they are. These topics, however, have up until recently been largely absent from the regional public debate.

This technical note seeks to highlight the relationship that exists between a country's level of governance, the success of digital government strategies, and the identification policies that government implements, as well as the interdependence between them. Belgium, Chile, and Mexico were chosen as case studies, because they share characteristics making them in some ways comparable. Moreover, amongst other reasons, they are all OECD-member countries, they have well-defined digital government strategies, and they are in the process of implementing (with differing degrees of progress) a state-of-the-art electronic identification (e-Id) card.

Results arising from analysis of the three cases reveal a diverse degree of progress, despite the fact that legislation governing identification policy and establishing electronic government was introduced at roughly the same time. There are also differences in the adoption of Open Source software and its use, a subject that merits further exploration regarding its employment in developing countries.

Within the context of the adoption and acceptation of electronic public service provision to citizens, it is obvious that the debate concerning the right to privacy and, consequently, personal data protection, is still in its infancy in Latin America and the Caribbean (LAC). It is notable, however, that of the three countries analyzed, only the Mexico City's Penal Code considers identity theft to be a crime.

It is the authors' opinion that in an evermore-connected world, the role and the rights of the citizen are not being sufficiently taken into account. The concepts of identity management and interoperability should be approached via the notion of Identification 2.0, a holistic concept that not only considers the technological issues, but also takes into consideration legal and institutional aspects in order to safeguard every citizen's unique, legal and safe identity.

1. INTEROPERABILITY

1.1 Interoperability

Interoperability is a term originally associated with information systems and can be defined as the capacity and the processes of interconnecting isolated environments (or silos) with the aim of enhancing veracity and communication between all parties in a virtual transaction. The topic of interoperability acquires particular importance within the context of electronic service provision for citizens, the registers that contain personal data and the processes that require identity authentication.

Citizens and users are increasingly able to access more services from a single point, either via the Web or a personal customer care point. People are no longer content to send off a number of forms and present an endless list of documents of proof to carry out a transaction. On the contrary, they expect a complete delivery service in the shortest possible time. Time itself has become a scarce commodity, and having to resort to government offices can be expensive; therefore, customers do not wish to spend hours in lines or trying to find out which government agency is the one they need to deal with. This trend, recognized by governments, is one of the drivers of electronic government development. Reduced costs and improved service delivery quality are objectives that can be easily reached when processes are redesigned, databases are integrated, and, ideally, certain tasks are centralized. In many of these cases the information systems must also be redesigned; systems that previously operated alone must now become capable of exchanging information with other systems and forming part of an interoperable network.

Interoperability, therefore, constitutes one of the principal characteristics of any digital government strategy. It can be defined as the capacity that information systems and the procedures to which they lend support have for sharing and modifying information and enabling the mutual exchange of information and knowledge.[1] Interconnection—that is, the possibility of communicating between two or more points to create a bond between them, either temporarily for a certain transaction or on an ongoing basis via the Web by connecting two or more machines—appears to be the basic requisite for interoperability.

Interoperability and interconnection are about getting equipment and applications from diverse origins to work jointly within a network. Interoperability comes into play when archives have to be shared between computers with different operating systems, or when all

[1] *Real Decreto Español* (Spanish Royal Decree) by which the *Esquema Nacional de Interoperabilidad* (National Interoperability System) is regulated within the sphere of the *Administración Electrónica* (Electronic Administration) 4/2010, 8 January 2010.

the diverse equipment needs to be controlled from a central console. It is more complicated than simply connecting various computers within a network. The protocols should also make it possible for each piece of equipment to communicate with any other within the network.

Interoperability enables the State to provide services through a single point of access, thereby facilitating for the user not just the search for information, but also the verification of personal information (identity) involved in each transaction. This is, however, merely the first step (or, rather, the second if we consider interconnection itself to be the first); system integration is the next step. Interoperability allows information (or data) to be mixed. Integration enables information to be taken from its original context and placed in another, without its meaning being altered. It allows information to be obtained from many sources and then centralized. Conversely, it can diffuse our information through multiple access points. Finally, it allows the information that we possess to be mixed with that of others, for mutual enrichment (Leiva Aguilera, 2008).

1.2 Practical Examples of Interoperability

1.2.1 e-Participation

E-Participation represents the use of ICTs by democratic actors within the political and administrative process, at both the national and the international level. Taghi (2009) establishes that participation in general, and electoral participation in particular, results from the combination of two factors: government programs aimed at promoting participation, and people's willingness to practice it. This therefore includes supply as much as demand. In this context, electronic electoral systems must guarantee the same basic properties of traditional voting; that is, the secret and informed vote. For this purpose, Taghi defines four stages of participation, depending on the use of the available technology:

1. A complete absence of available electronic formats: the traditional paper format is used and everything is conducted manually.
2. Online access to electronic information. There is an official website and the candidates can be registered electronically. This must also incorporate an electronic payment system, which presupposes the existence of a certain level of interoperability.
3. Electronic election: the election is carried out using online systems. However, without an electronic signature, the authorization of both the candidates and the electors has to be conducted at terminals operated by a centralized electoral agency. The degree of interoperability is greater.

4. e-Election: the use of electronic signatures dispenses with the need for voting terminals, as votes can be emitted from any terminal connected to the Internet. There is full interaction between the electoral agency and the final user (e.g., via SMS or e-mails).

1.2.2 e-Taxes

In Chile, 86.9 percent of taxpayers deal with the Inland Revenue Service (SII by its name in Spanish, *Servicio de Impuestos Internos*) via the Internet, according to figures published by the SII for the year 2006.[2] This is due to SII's intensive use of ICTs and, in part, to its ability to interoperate its database with that of the Civil Registry and Identification Service (SRCeI by its name in Spanish *Servicio de Registro Civil e Identificación)*, thanks to the joint work undertaken by both institutions within the framework of the electronic government strategy defined by the Chilean Government and to the technological specifications that enable the computer systems of both institutions to work in concert.

1.2.3. Public Procurement

The adoption of ICTs to modernize public procurement systems has increased transparency levels for this kind of administrative procedure, and has contributed to decreasing the levels of corruption in one of the most sensitive areas for the State administration, given that public resources are invariably involved in this type of transaction. Through use of interoperable systems, governments can exchange information about bidders and see if, for example, they have been previously subject to criminal procedures, or whether they have been disqualified in some way. It is possible, moreover, to establish the participating businesses' compliance with tax and employment obligations.

1.2.4. Travel Documents

The International Civil Aviation Organization (ICAO), a specialized agency of the United Nations (UN), promotes the standardization of international travel documents, such as passports and visas, which contain information that can be read by an electronic scanner (so-called Machine Readable Travel Documents, or MRTD). This new type of document contains standardized information providing details of the bearer's identity, including a digital image. This standardization allows participating countries to gain access to the

[2] Presentation of the *Servicio de Impuestos Internos* (Inland Revenue Service) review. Adimark Gfk. January 2006

information contained therein, and to accept documents issued in other countries that comply with the MRTD characteristics. In this way, interoperable systems can facilitate information inspection at borders, and increase security levels.

1.3 The Benefits and Risks of Interoperable Systems

The number, speed, and complexity of economic and social transactions is increasing so rapidly that the State's capacity to analyze and utilize them, and thereby its capacity to maintain and make possible society itself, is in serious danger of being overloaded (Fenwick, John, and Stimac, 2010). The use of interoperable public administration systems, however, means that this risk factor can be managed.

Both the origin and the development of electronic government are due more to a political decision than a technical one. ICTs can be used as tools for change whenever there is clear political willpower to lead the necessary transformations within the State administration's structures, procedures, and cultural organization. A country's institutional capacity is therefore of utmost importance.

This political willpower is sustained, principally, by the benefits that the implementation of electronic government strategies brings about for the State and for its citizens. These benefits include enhanced user satisfaction levels, increased governmental efficiency and effectiveness, greater social inclusiveness, improved entrepreneurial competitiveness, and greater transparency and openness (Dinsdale, 2002). The real benefits, however, will depend on the actual polices that are designed and applied. For example, the saving produced by electronic government can arise from task automation, the generation of new services, or even from abandoning the paper format, which can also link electronic government policies to environmental policies.

Of particular interest for benefits analysis are the savings in transaction costs that arise from the implementation of digital government strategies. Although diverse methods exist, such as Cost-Benefit Analysis (CBA), the Initial Return Rate (IRR), Current Net Value (CNV) and Return on Investment (ROI) methods, and key behavior indicators, it is the analysis of transaction costs, according to the OECD (2005), which provides a quick and easy way of estimating the potential savings in electronic government projects.

At the same time, the risks of implementing electronic government strategies must not be ignored, particularly with regard to the eventual widening of the digital divide. This can be understood to be "the gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard to both their opportunities to access information and communication technologies and to their use of the Internet for a wide variety of activities."[3] The State's political resolve thus becomes of prime importance for all electronic government initiatives. Electronic highways should not be constructed without first considering that the citizens must have the adequate tools and opportunities to enjoy the benefits they bring. After due prior consideration of factors such as Internet access or the percentage of PC users in at the national level, some possible measures that could be adopted to prevent or mitigate the negative effects of implementing this kind of strategy might be:

- During the initial stage, offer electronic services as addition to the usual service provision
- To ensure access to electronic services in public or remote places
- To establish intermediaries to solve problems for users who are not digitally aware or educated
- To provide free training programs
- To promote and encourage the usability of websites and web portals

Last, but by no means least, are the additional existing risks, such as the use of ICTs to obtain personal information to be used for fraudulent ends, or for purposes that vary from the one originally declared. The first, generally known as identity theft, will be examined at greater length below. The second, known as function creep, is especially sensitive with regard to identity polices. In this case, a series of personal data is collected with the citizen's authorization to effect adequate identification (the declared intention), but is subsequently employed for other purposes not specifically authorized by the person, such as, for example, surveillance (non-declared intention). With regard to fraud and identity theft, the unlawful obtaining and use of information is causing great concern. Some countries, therefore, have enacted legislation that prohibits the sharing of information between different public services.[4]

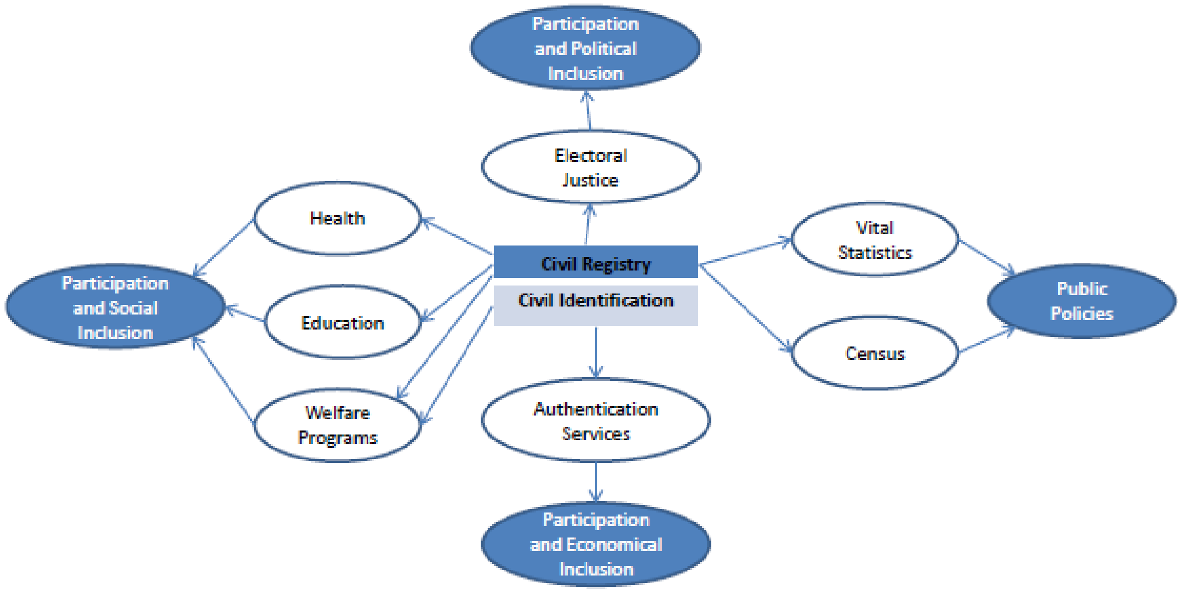
[3] OECD. Glossary of Statistical Terms http://stats.oecd.org/glossary/detail.asp?ID=4719

[4] Chile, for example, has *art. 21 ley 19628* (Article 21, Act 19628) concerning personal data protection and *art. 2 del D.L.645/25* (Article 2, Act 645/25) regarding the *Registro General de Condenas* (General Sentences Register).

2. IDENTITY AND IDENTIFICATION

One of the fundamental requirements for an interoperative platform to obtaining function efficiently and safely, thus enabling services to be provided electronically to the citizen, is the verification and authentication of the user's identity. Identity management must therefore also become a public policy priority. This can be understood as a combination of policies, systems, rules, and procedures that define the agreements between an individual and an organization concerning the entitlement to and the use and protection of personal information (Harbitz and Benitez, 2009). The following section presents the fundamental principles of identity management, and its relevance and importance in the construction of interoperable platforms.

Figure 1. Conceptual Model of Civil Registration and Identification Interfaces



Source: Authors' elaboration.

2.1 The Right to a Name and Nationality

Article 6 of the Universal Declaration of Human Rights (1948) establishes that "everyone has the right to recognition everywhere as a person before the law." A name is an attribute of this nature, as it enables a person to be legally adjudged as having sufficient aptitude to be entitled to certain rights and obligations. This was specifically recognized in Article 18 of the American Convention on Human Rights, also called the San José de Costa Rica Pact, inspired by the Universal Declaration of Human Rights, which established that "every person has the right to his or her own name, and to the surnames of his or her parents, or of one of them." Moreover, it also establishes that a law should "regulate the manner of ensuring this right for all, if necessary through the use of supposed names." The right to a name, therefore, as a specifically recognized human right, does not arise from the particular legislation of each country, but is rather inherent in the human person as such, being moreover inalienable and imprescriptible.

The State is not only obliged to recognize this but, moreover, is obliged to act as a counterpart to these rights, meaning that it must comply with certain obligations to give, to do, or to omit. Finally, this right is closely linked to the most important human right, the right to life, given that as soon as one commences to be, so too he or she begins the right to be recognized as such.

2.2. Legal Identity

Legal identity represents the State's obligation to enable each person to exercise his or her right to a name. This is defined as a "mixed condition obtained by the registration of birth, or from civil registration, which grants the person an identity (name and nationality) as well as unique and personal identification variables, such as biometric data related to a unique identity number" (Harbitz and Boekle, 2009). This definition contains three elements. The first is represented by a legal act: the registration of a vital event (birth) carried out by a public agency. The second refers to the diverse variables that allow the person registered to identify himself as such. The third expresses the causal relationship that exists between civil registration and civil identification.

Two additional important facts are brought to light by this definition. The first is that the right to a name is understood to be exercised with the first element of the definition. In other words, it is the act of registration itself that denotes fulfillment of the State's duty, wherein the State is obliged to furnish all the necessary physical and legal elements to enable said registration to take place. The second fact is that, although the right to a name is satisfied by registration, identification is not completed merely by the existence of the aforementioned variables. It requires a subsequent act: verification. The act of identifying oneself establishes who one is; the act of verification establishes if one is really the person one claims to be. This will be further examined alongside the use of biometrics for identification purposes.

2.3 Civil Registration

According to the UN definition (1998), civil registration is a "public institution within the State that serves both general and individual interests by gathering, screening, documenting, filing, safekeeping, correcting, updating, and certifying with respect to the occurrence of vital events and their characteristics as they relate to the civil status of individuals and as they affect them and their families, and by providing the official permanent record of their existence, identity, and personal and family circumstances." This definition describes in general terms what each nation's legislation determines for their respective registration agencies.

The fundamental importance of the civil register is rooted in the fact that this register, by establishing a person's identity, enables access to, and exercise of, a series of human, civil, and political rights. The civil register is also the primary source of vital statistics information, and therefore a key institution in the development of public policy.

The birth certificate, in turn, is the confirmation of the fact of registration and constitutes the cornerstone of all policies relating to vital statistics, civil registration, and identification. This certificate sets out, in general, all of the details relating to the birth, such as; the minor's name, the names of the parents, and the date, time, and place of birth. It is in this document, for example, where changes in one's name or other particulars are recorded.

2.4 Civil Identification

Civil identification refers to the verification, registration, management and conservation of each citizen's personal data needed to establish unique identity (Harbitz and Benitez, 2009). Generally speaking, a unique identity number is assigned to each registration (numerical and/or alphanumerical code), which enables the registration to be monitored, controlled, and linked to the registered personal data (Harbitz, 2009). It is also common to find biometric details amid the registered personal data, usually the fingerprint and, depending on the level of technology available to a country, more advanced biometric data, such as facial features.

Finally, a public agency endowed with the relevant powers is responsible for this process. The administrative dependence of this agency varies from country to country (see Table 1).

2.5 Normative Framework

As the right to a name is a basic human right, the legal basis of every civil registry system has its roots in each country's political constitution. This is because, the declaration of human rights is an international public instrument, which is recognized by the signatory states as at par with constitutional law, as the constitution is the political/juridical instrument that contains all the rights and principles that limit the State's power and subordinate it to the rights inherent to every human being.

Although the constitution establishes the generic rights and obligations, it is, however, the laws and regulations (juridical instruments of the second and third category) which the State uses to fully define the right to a name, by establishing rights and obligations both for the State and for the persons therein, enabling a civil register system to be established and defining the identification instruments.

It is, nevertheless, difficult to draw the dividing line between a law and a regulation when it comes to creating and regulating this system. It is usually the constitution itself that establishes exactly which matters pertain to the law and which do not, moreover establishing whether the task of drafting outline legislation falls to the executive or to the legislative branch. Yet, it is generally understood that the law is responsible for creating the public organ or agency responsible for administering the system and establishing the limits of its competences, whereas the regulation is responsible for specifically determining how the said agency will carry out its functions. The advantage that the regulation has over the law is that its enactment and subsequent modification is easier and quicker, thus providing the necessary flexibility for an identification system to rapidly adapt itself to social, political, and technological changes. This advantage, however, is counterbalanced by precariousness in the permanence over time that a legal framework needs in order to be viable.

The aforementioned has become increasingly relevant due to the implementation of electronic government policies, which tend to redefine the relationships C2G, C2B and G2B, as they establish electronic platforms not only for information gathering, but also for service provision. Providing services in this way has particularly influenced the identification systems by requiring greater security levels in the transactions undertaken to acquire the services offered via this new platform. This has given rise to discussion among the computing community about so-called Identity 2.0, distinguishing it by its relation to identification within the new platforms developed. This discussion has, however, only taken place on a purely technical plane up until now.

2.6. Identification Policies and Instruments

Although attempts have been made to advance towards internationally accepted standards in the fields of identity and identification—in some cases successfully (especially with regard to travel documents)—, identification policies and instruments tend to be particular to each country, and usually respond to diverse visions of the State's role in the exercise of the right to a name.

Examination of the policies and instruments chosen suggests that it is possible to establish two groups of countries: those that have a specific instrument for identification purposes (for example, Chile and its identity card) and those that grant legal capacity to establish the facts of identification to instruments not specifically designed to that effect (for example, the United States and its driving license).

An identity card consists of a document issued to a person containing his or her photograph, name, sex, and signature, and enables that person to exercise certain activities, or accredits him or her with being a member of a certain group (Harbitz and Benítez, 2009). Countries that lack this type of document do not generally have a coherent policy with regard to the legal identification of their citizens. Rather, they usually have a combination of laws and regulations that create and regulate the State agencies that provide the diverse identification instruments in question. Their identifying function is often established more as a matter of custom rather than as a result of specific legislation (sometime reaching extreme cases wherein the value of the identifying document is decided subjectively by the person who requires it).

2.7. Biometrics and Authentication

It is important to distinguish identification from authentication. The former answers the question "who am I?" Authentication, however, responds to the question "am I really the person that I purport to be?" Although identity is something unique and unrepeatable, authentication is generally carried out based upon i) something that the person has, but which is "outside" of him (such as an identity card); ii) something that a person knows (a password); or iii) something that the person possesses physically (biometrical information). There is still no identification and authentication system that is fail-safe, given that there is always a minor risk of false rejections or acceptances. The possibility, however, that two fingerprints are identical is one in 64 billion, which would seem to imply a high degree of exactitude.

On the other hand, when false acceptances or rejections do take place, the rejection is due, in many cases, to human error, such as poor-quality fingerprinting, or a badly spelled name. A biometric system, therefore, is a means of recognition in which a person's identity is verified according to his or her physiological characteristics (something that a person is) or behavioral characteristics (something that the person generates), such as a fingerprint and the iris or the voice and handwriting (López García, 2009).

Biometrics, defined as the statistical analysis of a person's physiological characteristics, has become synonymous with the authentication of people's identities by using their unique characteristics via computerized systems (Hopkins, 1999). The great advantage of biometric systems is that they provide greater reliability in personal identification, given that a person's physiological characteristics are permanent and impossible (or extremely unlikely) to be shared. The role of computerized systems is due to their capacity to process, with greater speed and exactitude, large quantities of information in a short space of time. This is important, given that this kind of system is based on contrasting the basic unique characteristics of the individual with the registered biometric data. When population numbers are low, this process can be conducted manually. However, this becomes impossible (or rather, impractical), when the numbers are greater. Herein resides the need to automate the process by the use of computer technology.

This automation establishes two parameters, which in turn allow two types of biometrics to be distinguished: static biometrics and dynamic biometrics. Static biometrics includes and measures people's anatomy, such as fingerprints, iris and retina analysis, and facial recognition. Dynamic biometrics, in contrast, examines and measures people's behavior; voice patterns, handwritten signatures and gesture analysis, among others, are used for this purpose (Alcántara, 2008). Furthermore, biometrics allows for a unique electronic identity (eID) to be established, which is indispensable for gaining access to the services provided by an electronic government that is interconnected via interrelated silos and sites.

3. INSTITUTIONAL FOUNDATIONS

Technological solutions are basically useless if there is no political and regulatory framework enabling the systems that administer the citizen's interaction with government (C2G), the citizen's interaction with the private sector (C2B) or government's interaction with the private sector (G2B), to function.

3.1 Governance

Institutions are the framework made by people to facilitate human interaction. They can be formal (such as the State, for example) or informal (such as social behavior rules), but they constitute an essential imperative for human development (North, 1990). The effectiveness and efficiency of an institution like the State therefore becomes indispensable to guarantee the goods, services, laws, and regulations that make it possible for markets to prosper, and for people to enjoy full protection of their rights. Without the State, it is difficult to achieve sustainable development in either the economic or the social plane.[5] The State must have the capacity to pursue its objectives, and be responsible for its actions and achievements. It is not only the State's existence that is necessary, however. There must also be a combination of rules, processes, and practices that determine the behavior and activities of the actors involved (informal institutions). This framework shapes the space in which individuals and organizations develop and interact, and this capacity building can only be considered a success insofar as these institutions become permanent over time (Willems and Bumert, 2003). The concept thereby becomes associated with the idea that the greater the capacity, the greater the possibility of progress towards development, and that this progress will be sustainable. For the UN, for example, capacity building is seen as a key factor for international cooperation, given that, in its absence, the beneficiary countries will not acquire the necessary sustainability levels to ensure that the cooperation achieves the desired results.[6]

The State will work well, therefore, in the degree to which the government is capable of designing and building public policies, of administrating its resources fairly, efficiently and transparently, and of responding effectively to the demands of its citizens, in order to augment social well being. The idea of "good governance" begins with the capacity of civil society to legitimize governmental institutions in the exercise of their authority, and to establish checks and balances on the executive branch's actions that safeguard civil liberties and the functioning of democratic politics, that is, a party system, competitive and transparent elections, and a free and informed ballot. The idea of "good governance," therefore, for which the citizen's capacity to be listened to by the government and to demand accountability is fundamental,[7] immediately relates the problem of institutional capacity with three

[5] Report on global development. Summary. World Bank, 1997.

[6] United Nations Department of Economic and Social Affairs http://www.un.org/esa/cdo/about.html

[7] For more information see http://www.dfid.gov.uk/Working-with-DFID/Funding-opportunities/Not-for-profit-organisations/Governance-and-Transparency-Fund-GTF-/Introduction/

dimensions: the development of human resources within each organization; organizational strengthening (referring to the organization itself and to the sum of the organizations with which it interacts in order to function effectively); and institutional reform (the institutional context or legal framework, and the economic, political, and social environment within which the public sector is situated) (Ospina, 2002). These dimensions affect both capacity itself and the interventions designed to build and/or strengthen it. Institutional capacity must therefore be based not only on the formal empowerment of its authorities (the institutional context), but, moreover, on the adequate social conditions that enable a democracy to function correctly. Finally, to draw a theoretical link between the concepts of citizenship and legal identity, a useful definition of good governance would be “to focus not only on the State’s institutional aspect, but also on the needs of its citizens” (Harbitz and Boekle, 2009).

3.2 The Administrative Dependence of the Civil Registries

The importance of administrative dependence lies in the fact that through it, it is possible to observe the differences and emphasis that each government displays in civil registration mattes. It is not the same, from the public policy design and implementation perspective, for a civil registry to depend on an electoral organ, the Ministry of Health, or an autonomous body. Budgets and competences are highly conditioned by administrative dependence.

Table 1. Institutional Location of Civil Registry Agencies in Latin America and the Caribbean

Ministry of Justice	Electoral system	Autonomous	Other
Brazil	Bolivia	Honduras	Argentina (Ministry of Provincial Government)
Bahamas	Colombia	Peru	Ecuador (Ministry of Telecommunications and the Information Society)
Barbados	Costa Rica	Guatemala	Guyana (Ministry of Interior)
Belize	Dominican Republic	El Salvador	Jamaica (Ministry of Health)
Chile	Nicaragua		Mexico (Secretariat of the Interior)
Haiti	Panama		Surinam (Ministry of Interior)
Paraguay	Venezuela		Uruguay (Ministry of Education and Culture)
Trinidad and Tobago			

Source: Harbitz and Boekle, 2009.

4. LEGAL FOUNDATIONS

4.1 Legal-Political Frameworks

The State's legal actions can be analyzed according to two principles: the principle of legality and the principle of power or sovereignty. The former is related to the fact that the State's action must always be contained within the existing legal framework. In other words, the exercise of its powers must be based on legal rules that define a competent organ and a set of matters that fall within that organ's jurisdiction. The State and its institutions can do only what the law authorizes, in contrast to private persons, who can do everything except that which is expressly forbidden by the legal framework. The power of sovereignty, however, establishes that the State does not relate to individuals on an equal plane but, rather, on unequal terms. These principles guide the attainment of the State's objective, which is understood to be the permanent pursuit of the common good. In democratic countries, the political-legal framework for the development of good government is normally set out in the political constitutions and in the regulatory framework deriving from them (laws, regulations, and decrees).

The concept of good government acquires added relevance when it comes to designing and implementing public policies, which can be illustrated by the case of electronic government and the legal identification policies that countries have established. Many countries can, either with their own resources or with foreign support, enlist experts to help with the development of projects oriented to the design and implementation of electronic government strategies. Weak institutionality, however, will be translated, for example, into low levels of confidence in the government, thereby hampering the success of these strategies by failing to provide solutions for the citizen or, rather, by transferring the lack of confidence in formal institutions into distrust of the new digital platforms. The same thing happens with civil identification systems, which are sustained by the confidence that the citizenry has in each respective instrument and by the usefulness that it represents. These factors, in turn, principally arise from the confidence that exists in the governmental agencies that administrate them, and the services that they offer. In contrast, deficient policy implementation can severely damage existing confidence levels.

4.2 Legal Framework for Biometrics Use

Biometrics allows for greater security and confidence levels, particularly with regard to establishing the identity of persons involved in a transaction. The most common way of identifying a person is therefore by using fingerprints, which are unique and unrepeatable and, therefore, irrefutable. The introduction of ICTs, however, has led to other biometric attributes being used, such as the iris, or voice or facial recognition. On one hand, these measures increase the security of authentication processes, but at the same time they increase the system's vulnerability due to the amount of personal information, which is no longer limited to just the fingerprint, that becomes available to third parties. It therefore becomes necessary to put adequate legal protection in place to avoid the misuse of the information gathered by either public agencies or private bodies.

5. TECHNOLOGICAL FOUNDATIONS

5.1 Electronic Government

The concept of electronic government relates to use, by the government, of ICTs to offer the citizenry the opportunity to interact with it via diverse electronic media, such as telephones, e-mail or Internet. It refers to how the government organizes itself, both legally and administratively, in order to provide the information required by customers, and to coordinate, communicate and integrate processes within the same organization (Almarabeh, 2010). The UN defines electronic government as the public sector's capacity and willingness to use ICTs with the aim of improving the knowledge and information contained in the service that it delivers to the citizen.[8] The OECD (2003), in turn, defines it as simply the use of ICTs, particularly Internet, as tools to achieve better governance. Both definitions include the fact that the objective of electronic government is to achieve substantial improvement in the public apparatus, by employing the available technical advances to achieve customer-based service delivery.

The origin of electronic government is due, to a large extent, to electronic commerce. It is, however, an error to emulate commercial measures when it comes to designing digital government strategies, as each responds to completely different relationships and is carried out in a totally different field of activity. Electronic commerce responds to the customer-business relationship within a context of a competitive market place, wherein each client is free to choose from an infinite number of suppliers.[9] Electronic government, in contrast to electronic commerce, is primarily based on the relationship between the State and the citizens and does not correspond to market characteristics. The services that the State provides

[8] United Nations e-government Program http://www2.unpan.org/egovkb/egovernment_overview/index.htm

[9] Infinite in the sense of the theoretical characteristics of a market with perfect competition.

through electronic government are on the whole monopolistic, and consumers find themselves obliged to use these services and pay a price that is unilaterally determined by the public agencies that provide them. Furthermore, the business model of both electronic commerce and electronic government differ, in that the former is oriented towards value creation for the client and the generation of earnings, whereas the latter is based on laws and regulations that provide citizens and enterprises with information and services, and also demarcates the inter- and intra-governmental relationships with other electronic governmental information systems. Finally, the acceptance of electronic government resides in the confidence inspired by government, the access to information that government provides, and qualitative improvements that the customer can perceive in the use of new instruments created for such purposes (Scholl, 2009).

5.2 Open Source Software

The electronic government strategies designed by each country tend towards the promotion of free or open source software. Moreover, many of these strategies contain directives or mandates aimed at making this kind of software obligatory within the administration. An example of this is given by the European Commission, which set up the Open Source Observatory and Repository (OSOSR) to exchange information, experiences and open codes (FLOSS for Free/Libre/Open Source Software), mainly within the public administrations of member countries.[10]

Open source software is not only acquired for free, but it is also possible to study and legally modify its source code (the code containing the instructions the computer must follow to execute the software) and to distribute it to other users without cost. This type of software is important for these kinds of strategies not only because it is free, which signifies an important advantage for developing countries, but also that the inherent freedom to modify it means that high levels of interoperability can be rapidly achieved. It is, however, important not to confuse the term open source software with either i) free software, or freeware, which is software ceded by its authors free of charge or ii) shared software, or shareware, which offers the possibility of downloading the software and using it for a certain period of time, but without having access to the source code and, generally speaking, without being able to use it indefinitely without paying a certain amount (Martinez Usero, 2006). Finally, open source software is technically considered to be synonymous with open code software.

[10] Open Source Observatory and Repository http://www.osor.eu

According to Von Hippel (2001) the projects that are generated around open source software create consumer communities that are managed completely by and for the users. Each one of these communities is capable of creating exactly what it needs without having recourse to a third party to act as an agent. Furthermore, they are not even obliged to generate everything that they need, as they can freely take advantage of improvements or innovations that are created by others. Unfortunately, this kind of software has experienced uneven development. To analyze this phenomenon, it is worth examining the Open Source Index (OSI), an initiative led by the Georgia Institute of Technology aimed at creating an instrument designed to compare and contrast this kind of software in different countries.[11] Its importance lies in the fact that it is one of the very few quantitative analyses conducted to explain why open source software initiatives have been successful in some countries and failed in others. According to this index, European countries currently hold the leadership, whereas the United States and Brazil stand out in the Americas. The OSI was compiled using information from one year only, although it is hoped that there might be an increase in the use of this tool, given the increasing importance that open source software represents for such contingent matters as cost reduction and transparency enhancement within public administration. The developers of open source software have been instrumental in gaining free access to government data. According to *The Economist*, the majority of databases offered by governments are in the beta version, which suggests that they are open to improvements.[12]

5.3 PKI Technology

Commercial transactions, usually carried out "face-to-face" do not require the use of complex security systems for the information provided. Nevertheless, the situation changes whenever the transaction is carried out by electronic means. Mechanisms that provide security for those parties involved need to be developed. This, moreover, also applies to the transactions conducted in matters of electronic government. It is in this area that Public Key Infrastructure (PKI) takes on a decisive role.

A Public Key Infrastructure is a security architecture introduced in order to provide increased levels of confidence in information transactions carried out over the Internet. The Belgian National Identity card is based, for example, on this technology, and comprises two certificates: one for verification and another containing an electronic signature. Furthermore,

[11] Open Source Index 2008, Red Hat, Inc. http://www.redhat.com/about/where-is-open-source/activity/

[12] Data and Transparency: Of Governments and Geeks. The Economist, 4 Feb 2010.

each key can only be used with a PIN code. The Chilean Identity Card, in turn, completed the incorporation of this technology in 2010.

The specific security functions provided by PKI are confidentiality, nonrepudiation and authentication. PKI is not in itself, however, an authentication or authorization medium. It is rather a technological infrastructure that provides support for these transactional needs. As it cannot itself inspire confidence, however, it requires all parties to have pre-established confidence levels, (Weise, 2001). Finally, in countries like Belgium, the use of this technology has provided an incentive for open source software development, especially with regard to the verification process.

5.4 Legal Framework

The idea of electronic government, and the advantages that it brings, is in itself attractive for the political class, given that with few resources it is possible to rapidly achieve demonstrable results. It is, however, only a medium, which is sustained not only by a government's technical capacity but moreover by the institutional capacity of the government that implements it, and by the legal framework that provides a context and makes it viable.

The policies of electronic government require legal reforms that enable the adequate conditions for its development to be created, and the possible risks arising from ICT use to be confronted. Although these reforms ought to take place prior to the employment of new technologies, they should furthermore be able to adapt rapidly to technological changes. These reforms, however, do not guarantee a digital strategy's success. As previously mentioned, reforms can only be sustained within a country enjoying the sufficient institutional capacity to carry them through.

The most basic reforms are those that ensure the possibility of the electronic (on-line) availability of information needed by the government and by the services that it provides. These reforms are not, however, sufficient. An electronic government's accessibility depends on the diffusion and availability of the infrastructure that the ICTs depend on, which in turn depends upon the regulatory framework for telecommunications and services. Another aspect that affects electronic government, particularly with regard to the validity of electronic documents, security, privacy and on-line payment mechanisms, is the existing regulatory framework for electronic commerce. In addition, and with regard to the documents that the government holds, it is very important to examine matters of interoperability between diverse State agencies, and to take the citizens' rights of access to governmental information into consideration. Finally, legal penalties must be established that deal with crimes that affect electronic databases and the data contained therein.

In general, countries can undertake this reform process in two ways: either comprehensively, through the introduction of specific legislation within the sphere of electronic government, or incrementally, via laws and policies. A good example of the former is provided by the case of Italy. Italy has formalized its electronic government strategy within the Public Digital Administration Code.[13] The code establishes, via its more than 70 articles, principles, rights, and obligations affecting both the citizen and the government (Lisi, 2008). Chile, in contrast, adopted a digital strategy aimed at "developing actions to promote a deeper and more intensive use of information and communications technology by citizens, enterprises and the State itself."[14]

International standards are also being adopted via agreements between countries. A good example is the Ibero-American Charter of Electronic Government (*Carta Iberoamericana de Gobierno Electrónico*) which incorporates the Principle of Appropriate Technology *(Principio de adecuación tecnológica*), through which governments commit to choosing the "most appropriate technologies to satisfy their needs" and recommends "the use of open standards and open source software in favor of security, long-term sustainability and to prevent the privatization of public knowledge." It is important to mention that that this does not in any way signify that citizens are obliged to use a particular technology in order to gain access to the services offered by the administration.[15]

5.5 The Protection and Ownership of Personal Information.

As previously observed, electronic government policies have, in general, two objectives: to improve government efficiency and to provide services to the citizen. However, although the use of technology does tend to make life easier, it introduces at the same time new risks that have to be dealt with.

It is probable that the components of an electronic government policy will generate new databases containing personal information about the individuals using the new services offered, information which it is the government's duty to protect. However, in the current

[13] *Codice dell'Amministrazione Digitale* Legislative Decree 7 March 2005, n. 82, *Gazzetta Ufficiale* n. 12 16 May 2005 – *Supplemento Ordinario* n. 93.

[14] *Documento Estrategia Digital* (Digital Strategic Document) 2007-2012, Government of Chile, 2007.

[15] *Carta Iberoamericana de Gobierno Electrónico* (Ibero-American Charter of Electronic Government) XVII Ibero-American Summit meeting of Heads of State and Government. Chile 2007.

state of development of information contained in electronic media, neither the existing nor the new legislation clarifies the legal status of information held electronically, either in programs or in databases, or of the electronic transfer of this data. Likewise, the right of persons to maintain the privacy of all or part of the personal information that, either voluntarily or obligatorily, they provide to third parties is not clearly defined. Finally, there is much discussion regarding the ownership of the data provided by individuals. One approach is from the intellectual property rights perspective. This does not, however, solve the problem, but rather tends to deepen the divisions by encouraging the creation of a market for the data. Another approach is from the State extra-contractual perspective, wherein, although there is no firm contract between the State and the customer, the State is held equally responsible for the data it administers.

The obligation to protect the personal information gathered falls naturally to the information gatherer and administrator, meaning the State, irrespectively of whether or not it uses a private enterprise to gather and administrate information concerning personal identity. This duty to protect is expressed in diverse instruments drafted by international organizations such as the UN or the OECD, in which it is established that the responsibility to protect this information lies with the administrators. These organizations, moreover, recommend their member countries to legislate for this protection, and to establish sanctions and remedies for when the protection is violated.

The principles established by these instruments include the following: i) diverse rights of the individual to find out, obtain, and dispute the personal information currently in the administrator's hands; ii) to limit the gathering, use, and maintenance of the information obtained and; iii) the obligation of the administrators of the information to specify the purpose of information gathering, to ensure the quality of the information gathered (that it is up to date and accurate), to adopt all relevant protection mechanisms and to be legally responsible for control of the data (Del Villar, 2001).

The obligation to protect, and the principles that underpin it, find their maximum expression in the so-called Habeas Data, which consists of a constitutional right designed to protect, in a court of law, a person's image, privacy, honor, and freedom of information. All legislation regarding Habeas Data must endow the person with, at least, the following rights:

- Provide the registered individual with access to the control of the relevant personal and family information.

- Provide the adequate means whereby obsolete and erroneous information can be corrected.
- Ensure the confidentiality of important personal information.
- Provide the means whereby sensitive personal information that might harm the person's right to privacy—such as that concerning religion, political ideology, sexual orientation, or any other potentially discriminatory information—can be deleted or challenged (Gaudamuz, 2001).

5.6 Social Networks and Privacy

A curious phenomenon that relates to the debate surrounding privacy and personal data protection has been created by the advent of these social networks. They can be defined as a distinct combination of actors, either individuals or groups, linked to one another through a social relation, or a combination of social relations (Lozares, 1996). This phenomenon gained added relevance with the use of Internet, particularly following the so-called Web 2.0 technological revolution. This permitted the appearance of programs with user-oriented interfaces that enable and facilitate large-scale and, especially, multi-directional communication, thereby forming the Internet social networks. The so-called social network 2.0 first appeared at the beginning of the century, reaching its peak with the birth of Facebook and Twitter. The former is the star of the new networks, with something approaching 500 million users worldwide, a fact that has not been without controversy.

Facebook was created in 2004 with the intention of building a university community in which the user could find friends virtually and join diverse types of organization, in order to exchange contents. Although each user can personalize his account with the personal information that he sees fit, the minimum data requirements for gaining access are a name, an e-mail address, sex and date of birth. To this can be voluntarily added employment and educational information, as well as information concerning hobbies such as music or cinema. Furthermore, photos and videos can be added, among other things. This has now become one of the largest personal databases in the world, and the United States is the country with the highest number of users. This seems rather curious bearing in mind the negative reactions generated by attempts to establish a national identification system based on biometric elements in this country. In the light of this, one might conclude that the widespread rejection is caused by the fact that the State would be the receiver and administrator of the personal information required to set up this system.

5.7 Identity Theft

It is difficult to imagine an identity being stolen, as the use of personal information by a third party does not preclude the original owner of the identity from the possibility of using the same information. The OECD (2008) defines identity theft as the acquisition, transference, possession or use of personal information pertaining to a legal or a natural subject, in order to commit a fraud or a related crime. According to Forbes, a study carried out by Javelin Research found that the costs associated with identity theft in the United States in 2009 rose to USD 50 billion, USD 6 billion more than the estimated costs for the year 2008.[16]

Identity theft mainly occurs when personal information revealing a person's identity (which might include the name, social security number, or any account number) is usurped and used or transferred by another person, either with the aim of taking financial, political or social advantage, or for carrying out illegal activities. This crime, however, is not limited to just the document; it is related to identity itself. This phenomenon has become very evident alongside the growing use of ICTs, in which the verification and authentication of identity are less secure. Furthermore, these new technologies and means of communication are usually used in order to obtain confidential information about people, especially that which reveals the person's identity. This information is subsequently employed to gain illegal access to, for example, bank accounts or to contract details, in order to obtain financial advantages.

The legal typification of this crime is usually present in diverse national legislation (under the crime category of fraud or name usurpation). There are some countries, however, such as Mexico and the United Kingdom, that lack this legal typification altogether. There are also varying approximations and degrees of gravity concerning perpetration and punishment. Some countries, for example, establish specific aggravating circumstances in this regard (the United States, via its Identity Theft Penalty Enhancement Act modified this section of the US Code, which typifies fraud relating to activities connected with documents concerning identity, authentication and personal information, establishing aggravating circumstances that allow consecutive sentences to be imposed when any identification

[16] Greenberg, Andy. ID Theft: Don't Take It Personally. Forbes Special Report. October 2010.

medium pertaining to another person is used in perpetrating a crime).[17] Other countries have categorized a specific crime, which is differentiated from fraud and some, like Chile, have arrived at this point by the judicial interpretation of crimes already described in current penal legislation (in this case, via the crime of name usurpation).

Identity theft has numerous variants, several of which have arisen from the use of ICTs:

- Phishing: the attempt, by an individual or a group, to solicit personal information by the use of so-called social engineering techniques.
- Pharming: a method that consists in redirecting Internet users from an authentic website to a fraudulent site that replicates the original one.
- Smishing: occurs when a customer receives a text message (SMS) in which a company confirms that a service has been already contracted and will be charged, unless the order is cancelled at the company's own website. This website, however, is configured in such a way as to steal the affected customer's personal data.
- Vishing: occurs when the swindler invites a person to call a certain telephone number. On calling, connection is made to an automated service that requires personal information in order to proceed. The difference lies in the fact that the identity theft is not perpetrated through a website, which means that customers are more confident about divulging their personal data (OECD, 2009).

6. SUMMARY OF THE CASE STUDIES

In order to analyze the relationships existing between a country's level of governance, the success of its digital government strategy and the identification policies implemented by it, as well as the interdependence between them, three countries were chosen as case studies: Belgium, Chile and Mexico. These countries were selected because they share some characteristics that facilitate their comparison. These are, among others, that they are all members of the OECD, they all have defined electronic government strategies and they are all in the process of implementing, with varying degrees of progress, a state-of-the-art electronic identity card.

From the institutional capacity perspective, which is the all-important base for all electronic government strategies and identification policies, it is not difficult to see that, of

[17] US Code, Title 18, Part 1, Chapter 47 § 1028A.

the three countries analyzed, Belgium is the one where progress is faster and more profound. It has continuously developed diverse instruments for this purpose, in order to measure impacts and advances, thereby generating permanent improvements and, moreover, demonstrating constancy in its measurements. It has surmounted problems such as political administrative divisions and the digital divide, which Mexico will also have to tackle in the short term. Chile might be regarded as an average for all three countries. Although it is on almost the same level as Belgium with regard to civil identification, it has had to face difficulties, especially with regard to electronic government, which has meant that process is still not mature.

Table 2. The Historical Development of the Legal Frameworks Concerning Identity Management

	BELGIUM	**CHILE**	**MEXICO**
Identification policy	2001	2000	2001
Electronic government	1999	2001	2000
Open source software	2006	n/a*	n/a*
Identity protection	1992	2010	2009
Identity theft	n/a**	n/a**	2010

Source: Authors' elaboration.
* No existing legislation.
** No existing legislation that defines identity theft as a crime.

The civil registry, the most important institution in terms of establishing an identity, has undergone similar development in all three countries. Most citizens in these countries recognize the importance of recording vital statistics and seem to understand the process. However, development in identification has not been as evenly balanced. Once more, Belgium takes the lead both technologically and chronologically in identification matters, whereas Mexico is the most backward in this respect. Nonetheless, both countries share important aspects. The first, as previously mentioned, relates to political administrative division. In contrast with Chile, both of these countries are federal states, which implies the existence of a barrier when it comes to establishing a single civil identification instrument for the country as a whole. Furthermore, this might explain why civil registration and civil identification processes are conducted by distinct government agencies in each country (the municipalities in Belgium and the states in Mexico). Mexico might face another difficulty, as the new identity card will depend on information currently managed by individual state civil registries, which evince differing degrees of modernization.

Of the three countries, Chile is the only one in which the same agency is responsible for both the registration of vital events and for identification, which might have an impact on transaction costs when it comes to establishing interoperable systems. Belgium and, to a lesser degree, Chile, have understood that for their electronic government strategies to be successful, it is essential to count on high levels of interoperability between the bases that manage personal information.

As the process of building confidence around the new identity document is the responsibility of the State and its institutions, it is sustained by the degree of utility that the document offers to the citizenry. Electronic government has therefore proven to be very useful, considerably widening the document's possible uses. The creation of electronic databases containing personal information, however, has also increased the citizens' concerns regarding the management and protection of said information.

In all three countries, to a greater or a lesser extent, citizens have protested the accumulation of personal data by the State. However, many users in these countries exchange their personal information through social networks, which seems to suggest a degree of mistrust not in the instrument itself, but rather in the public institutions responsible for these identification policies, and regarding the management of the information that they administrate. None of the countries have defined explicitly who collects and manages the personal information. Herein lies the importance of having legislation that is adjusted to modern-day necessities. In Mexico's case, the legislation is weak, and weaker still when one considers the technology used for its new identification card *(*CEDI, by its Spanish name *Cédula de Identidad).* Mexico still lacks, amongst other things, a crime category for identity theft. Irrespective of the technology employed, adequate legislation is an important factor in this kind of policy, especially with regard to electronic government. This legislation represents or expresses the political willpower necessary to carry out this kind of modernization process.

Finally, open source software has undergone extensive development in Belgium, with the introduction of a new identity card, particularly with regard to the process of verification. It is possible to foresee that a similar phenomenon will occur in Chile and Mexico. This is doubly important, given that it not only implements one of the strategic guidelines of electronic government policies in the three countries, but it also opens up the identification systems market, a market in which the use of open source software previously had little importance.

7. CONCLUSIONS

Full interoperability has yet to become a reality in the majority of countries, but, without doubt, recent advances in ICTs may significantly advance the processes. The necessary efforts to build interoperability platforms for governmental service provision should not be limited to the implementation of information technology solutions. These platforms have to operate alongside the information systems of different State organizations, with a wide range of heterogeneous technology architectures, and with different conceptual models with regard to data management. The three dimensions that influence the construction of interopability platforms are technological, semantic, and organizational. What must be remembered is that interoperability platform development and implementation processes are complex, because they require profound organizational changes.

Additionally, there is a lack of adequate legal and institutional frameworks that establish legal, unique, secure, and safe identity for citizens and, above all, protect their identities, even in the most developed countries. In the short term, a dialogue is necessary regarding the governmental duty to ensure that identification and technology policies are developed alongside the institutional capacity of the state agencies responsible for implementing these policies. Another challenge that must tackled in the short term is the risk to good governance posed by the digital divide, especially the gap between rural and urban areas, which might negatively impact the poverty cycle.

Many countries are in the process of modernizing their civil and identification registries, and a profound and open analysis of the experiences of those countries with greater familiarity with identification system interconnection and interoperability is recommendable, in order to deal ex ante with the implications for both the State and the citizens. It is above all indispensable to set up an adequate legal framework for the new identity management systems.

Finally, there are worries regarding the institutional capacity of the state, which is another matter of fundamental concern for electronic government, and especially for the relations and interactions between the citizen and government. Identity management, with regard to the future and to the concept of Identity 2.0, is a subject that requires urgent attention from both governments and citizens to minimize exposure to fraudulent or malicious use of personal information by third parties. Identity management requires an up-to-date legal framework able to adapt to constant changes in the virtual media, institutions that are equipped and prepared for almost constant changes, and a well-informed citizenry that is capable of taking advantage of the benefits offered by an interconnected society in an increasingly interconnected world. Although there has already been talk of the Web 2.0 and Identity 2.0, due to the growing need for identity verification and authentication in information and communications technology systems, the notion of Identification 2.0 should be postulated as a holistic concept that considers not only the technological angle, but also takes the legal and institutional aspects into account, in order to ensure each citizen’s unique, legal, and safe identity.

REFERENCES

Alcántara, Jose F. 2008. *La sociedad de control: privacidad, propiedad intelectual y el futuro de la libertad*. Barcelona, Spain: El Cobre Ediciones.

Almarabeh, Tamara, and Amer AbuAli. 2010. "A General Framework for E-Government: Definition - Maturity Challenges, Opportunities, and Success." *European Journal of Scientific Research* 39(1): 29–42.

Council of Europe. 1950. "Convention for the Protection of Human Rights and Fundamental Freedoms." Roma http://conventions.coe.int/treaty/en/Treaties/Html/005.htm

De Cock, Danny et al. 2004. *The Belgian Electronic Identity Card (Overview)*. Belgium: Katholieke Universiteit Leuven.

Del Villar, Diaz de Leon and Gil Huber. 2001. *Regulation of Personal Data Protection and of Reporting Agencies: a Comparison of Selected Countries of Latin America, the United States and European Union Countries.* Washington DC: World Bank.

Dinsdale et al. 2002. *Guía práctica para el gobierno electronico: cuestiones, impactos y percepciones*. Canadian Center for Management Development (CCMD), Canada. Available at www.eamericas.org/archivos/CCMD1-02esp.pdf

Fenwick, William, Esq., Erin John, and Jason Stimac. 2010. "The Necessity of E-Government." *Santa Clara Computer and High Technology Law Journal* 25. Available at http://www.chtlj.org/sites/default/files/media/articles/v025/v025.i3.Fenwick.pdf

Guadamuz, Andrés. 2001. "Habeas Data vs. the European Data Protection Directive." *The Journal of Information, Law and Technology* (JILT). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz

Harbitz, Mia and Boekle-Giuffrida, Bettina. 2009. "Gobernabilidad democrática, ciudadanía e identidad legal: vínculo entre la discusión teórica y la realidad operative." Washington, DC: IDB.

Harbitz, Mia, and Benítez, Juan Carlos. 2009. *Glosario para registros civiles e identificación.* Washington DC: IDB.

Hopkins, Richard. 1999. "An Introduction to Biometrics and Large Scale Civilian Identification." *International Review of Law Computers & Technology* 13(3): 337–63(27).

Lapon Jorn et al. 2009. "Extending the Belgian eID Technology with Mobile Security Functionality, Security and Privacy in Mobile Information and Communication

Systems." Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer, Berlin/Heidelberg.

Leiva Aguilera, Javier. 2008. "Integración e interoperabilidad en los sistemas de información." Presentation of E-Docpa (Electronic Documents in the Principality of Asturias) Oviedo, Spain. Available at www.edocpa.com/images/ediciones/ponencia_25.pdf

Lisi, Andrea. 2008. "The Digital Administration Code in Italy: Light and Shade. Curentul Juridic, The Juridical Current, Le Courant Juridique." Romania: Petru Maior University, Faculty of Economics Law and Administrative Sciences and the Pro Iure Foundation.

López García, Juan. 2009. "Algoritmo para la identificación de personas basado en huellas dactilares." Barcelona, Spain: Universitat Politècnica de Catalunya.

Lööf, Anna and Seybert, Heidi. 2009. "Internet Usage in 2009 - Households and Individuals." Eurostat Data in Focus 46/2009. Available at http://epp.eurostat.ec.europa.eu/portal/page/portal/product_details/publication?p_product_code=KS-QA-09-046

Lozare, Carlos.1996. "La teoria de redes socials." Barcelona, Spain: Departament de Sociologia, Universitat Autonoma de Barcelona. Available at www.raco.cat/index.php/papers/article/viewFile/25386/58613

Martínez Usero, José Angel. 2006. "La utilización del software libre y de los formatos abiertos en la administración pública." *Revista de Derecho Informático.* Available at http://www.alfa-redi.com/rdi-articulo.shtml?x=6504

Mariën Ilse and Van Audenhove, Leo. 2010. "The Belgian e-ID and its Complex Path to Implementation and Innovational Change." IDIS DOI 10.1007/s12394-010-0042-2. Breman, Germany: Institute for Information Management, Volkswagen Foundation.

Mahieu, Christine. 2010. "Belgian Federal eGov and ICT Measurement Initiatives." Belgian Federal Ministry for ICT. http://www.epractice.eu/en/cases/fedeviewa

North, Douglass C. 1990. *Institutions, Institutional Change and Economic Performance.* UK: Cambridge University Press.

OECD (Organization for Economic Co-operation and Development). 2005. *E-Government for Better Government.* Paris, France: OECD.

———. 2003. *The E-Government Imperative*. E-Government Studies. Paris, France: OECD.

———. 2008. *Belgium: E-Government Studies.* Paris, France: OECD.

———. 2008. *Policy Guidance on Online Identity Theft.* Paris, France: OECD.

———. 2009. *Online Identity Theft.* Paris, France: OECD.

O'Reilly, T. 2006. "Web 2.0 Compact Definition: Trying Again." http://radar.oreilly.com/archives/2006/12/web-20-compact.html

Ospina B., Sonia. 2002. "Construyendo capacidad institucional en América Latina: el papel de la evaluación como herramienta modernizadora." VII Centro Latinoamericano de Administración para el Desarrollo (CLAD) International Congress on State Reform and Public Administration, Lisbon, Portugal.

Scholl, Hans et al. 2009. "E-Commerce and e-Government: How Do They Compare? What Can They Learn From Each Other?" Proceedings of the 42nd Hawaii International Conference on System Sciences. Waikoloa, HI: Institute of Electrical and Electronics Engineers (IEEE).

Taghi Isaai, Mohamad, Firoozi Fatemeh, and Mahmood Hemyari Reza. 2009. *E-election in Digital Society.* Third International Conference on Digital Society. IEEE Computer Society: Cancun, Mexico.

UN (United Nations). 1998. *Manual sobre sistemas de registro civil y estadísticas vitales: La preparaciones del marcos legal.* Estudios de Métodos, Serie F, No. 71. UN

———. 1948. *Universal Declaration of Human Rights*. Geneva, Switzerland: UN.

———. 2010. E-government Survey: *Leveraging E-Government at a Time of Financial and Economic Crisis*. UN Department of Economic and Social Affairs. New York: UN Publishing Section.

———. 2010. *Human Development Index.* Geneva, Switzerland: UN:

Von Hippel, Eric. 2001. *Learning from Open-Source Software.* MIT Sloan Management Review. Boston, MA.

Weise, Joel. 2001. "Public Key Infrastructure Overview." Available at www.sun.com/blueprints/0801/publickey.pdf

Willems, Stéphane, and Baumert, Kevin. 2003. *Institutional Capacity and Climate Actions.* International Energy Agency. Paris France: OECD. Available at www.oecd.org/dataoecd/46/46/21018790.pdf

World Bank. 2010. World Governance Indicators. Washington, DC: World Bank. Available at http://web.worldbank.org/WBSITE/EXTERNAL/WBI/EXTWBIGOVANTCOR/0,,menuPK:1740542~pagePK:64168427~piPK:64168435~theSitePK:1740530,00.html

APPENDIX 1: CASE STUDIES

Belgium

Belgium occupies position number 16 out of the 184 countries in the electronic government ranking drafted by the United Nations Department of Economic and Social Affairs. Of the three countries analyzed, it is the one with the highest governance indices (World Bank, 2009) and is the only one that specifically includes identity policies within its electronic government strategy. Belgium is, furthermore, one of the six founder members of both the European Economic Community and the Organization for Economic Coordination and Development (OECD).

Identification Policy

Belgium was one of the first countries in Europe to have a civil registration system (from 1795 onwards) and issued its first identification card in 1919, which was at that time obligatory for anyone over the age of 12 and renewable every ten years. This policy was maintained until 2000, when the council of ministers approved a study into a new electronic identity card (eID). This study followed directly on from the publication, in 1999, of the European Directive on the electronic signature (De Cock, 2004). The purpose of this directive (as established in its Article 1) was to facilitate the introduction and use of the electronic signature and its legal recognition throughout European Union member states. In Article 5, it further established that each member state must ensure that its advanced electronic signature system satisfies the legal requirements of a signature, and is thereby admissible in a court of law.[18] Based on this study, in 2001 the Belgian Council of Ministers authorized the introduction of this new identity card for every citizen over the age of 12, and it became the most comprehensive system in Europe, with access to more than 600 applications.

The new identity card (eID) contains the bearer's name and nationality, a photograph of the bearer's face, a card identification number, and the unique identification number provided by the civil registry at the moment of birth registration. The card is issued by the municipality and is valid for five years.[19] Furthermore, it incorporates two certificates, one

[18] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999, on a Community framework for electronic signatures. Official Journal L 013, 19/01/2000 P. 0012 – 0020.

[19] For more information see http://www.ibz.rrn.fgov.be/fileadmin/user_upload/CI/eID/fr/8_documentation/newsletter/eID-RRN_Newsletter2_032009_fr.pdf.

for verification and another for the electronic signature. The electronic signature certificate is legally binding for online communication and interaction, except in the case of minors, given that they cannot legally sign documents or contracts. However, in spite of the far-reaching modernization of the identity document, the Belgian Government, due to the legal incompatibilities thrown up by the country's political-administrative divisions, decided against incorporating other identification methods (such as the social security card) into the new eID, something that would have been easy to do from the technical point of view.

The electronic signature certificate is only activated when the citizen reaches 18 years old. Similarly, the minors' identity card (Kids-ID) contains a certificate that becomes active at the age of 6 (Mariën and Van Audenhove, 2010). The identity card for minors, which is not obligatory, was launched in 2009 as part of the policies aimed at child protection. It is similar to the eID, but also contains the names of the parents and a telephone number in case of emergencies. A website was also created for this purpose (alloparents.be), where parents can activate the card and thereby access a 24-hour protection system for the registered minor. At present, the eID the population still views the cards with some skepticism. This is due mainly to security problems evinced by eID, and to the fact that many of the applications have not been widely accepted (Lapon, 2009). According to the European Information Society (EIS), the limited distribution of eID scanners has also contributed to the scant use of the card.[20] For this reason, in 2009 the federal government launched a national campaign titled "Your eID, as easy as can be" to disperse the diverse applications of electronic government service provision and to reduce the concerns regarding the safety of eID card use.[21]

Electronic Government

In 2001, Belgium's Federal Government Information and Communication Technology Service (Fedict, or *Service Public Fédéral Technologie de l'Information et de la Communication*) was created to modernize the country's federal public administration. The agency is responsible for the design and implementation of Belgium's electronic government policy. According to the United Nations (UN, 2010), among the 20 most-developed countries in electronic government matters Belgium occupies the 9th position in Europe and the 16th

[20] Future of Identity in the Information Society (FIDIS) http://www.fidis.net/resources/deliverables/hightechid/d127-identity-related-crime-in-europe-big-problem-or-big-hype/doc/4/

[21] e-Belgium http://www.welcome-to-e-belgium.be/en/

worldwide,. This is not a minor achievement when taking into considerations the barriers that Belgium has had to overcome, barriers that were duly noted in the OECD report on e-Government carried out in 2008.[22]

This report identified important obstacles that existed at the time of the Belgian policy implementation in 2001. The first is cultural. According to the survey, 25 percent of the population prefers to deal with legal formalities in offices in order to interact directly with the civil servant responsible. The second is the existing digital gap. A survey of information and communications technology (ICT) use in the home determined that in 2006 only 54 percent of households had Internet access and only 48 percent enjoyed access to broadband. The figures for 2009 showed that access had increased (67 percent and 63 percent respectively); however, in 2009 only an estimated 56 percent of individuals between the ages of 16 and 74 used the Internet daily or almost daily (Lööf, 2009). This led the Belgian Government to implement diverse initiatives aimed at measuring the impact and use of ICTs as well as the applications created within its electronic government strategy. The include the following (Mahieu, 2010):

2004 Fed-eView/A – 1st survey: carried out to measure the degree of back office development and the level of e-readiness within the federal administration.

2004-2006 Fed-eView/Citizen: conducted to identify customer necessities for the services offered by Belgium's e-government project.

2005 Design of the e-government monitor: an instrument designed to monitor the use and development of ICTs within the federal government, which is based on international best practices.

2008 Implementation of the e-government monitor: consolidation of the different surveys and evaluation instruments, development of new indicators, and the generation of new monitor-related joint public/private associations.

2009 Fed-eView/A – 2nd survey.

[22] In 2001 the OECD launched its e-government project that produces yearly reports on best practices and develops guidelines for addressing related issues such as cost/benefit analysis and e-services. It also explores how governments can best exploit ICTs to drive in good governance principles and achieve public policy goals by carrying out country peer reviews on this topic.

The Fed-eView/Citizen has been of particular interest. Created in 2005 by the Belgian ministry responsible for ICTs, its objective is to measure the needs of the citizens regarding the diverse electronic government applications and the use they make of them. This instrument has enabled customer priorities to be clearly established. According to results of the first survey, these include the following:

- Speed and flexibility: electronic services generate efficiencies such as the reduction in waiting or transfer time. It is, however, important that alternative channels, such as offices, are maintained in order to make the system more flexible.
- Friendly service provision: it is important to consider the level of digital illiteracy and thereby avoid causing customer frustration when it comes to implementing this kind of service.
- Personalized service provision: Belgian citizens are very concerned that the services provided electronically are relevant to them and are delivered in personalized form. In other words, they are more interested in the services themselves than in the agencies that deliver them.[23]

Finally, a further barrier exists that has to do with that the country's political-administrative division. According to the constitution, Belgium is a federal sate made up of communities (the French community, the Flemish community, and the German-speaking community) and regions (the Flanders and Wallonia regions, and Brussels). No hierarchical relationship exists between them. They each have their own executive and legislative branches that act within the sphere of their own powers.[24] The leadership of the country is thereby in the hands of different agencies, which exercise authority according to the limits set by the law. This leads to varied emphasis on electronic government implementation, given that each government level has its own priorities and interests. According to the OECD (2008), there are few incentives within the public sector to work in a coordinated fashion and thereby realize the benefits that e-Government brings.

This has prompted the federal government to launch the Belgian Government Interoperability Framework (BELGIF), which promotes interoperability not only among different levels of government within the country, but also within Europe.[25] For this purpose, an agreement concerning e-government issues was negotiated between all levels of

[23] Epractice.edu http://www.epractice.eu/en/cases/fedeviewc

[24] The Belgian Constitution. Legal Department of the Belgian House of Representatives. Belgian House of Representatives 2007.

[25] BELGIF http://www.belgif.be/index.php/Main_Page

government (the International Congress of E-Government (ICEG) working group, aimed at implementing this regulatory framework. The introduction of the eID card was another initiative designed to improve interoperability, and it has led to, among other things, the alignment of navigation structures within the various portals belonging to each government (OECD, 2008). Finally, it is significant that the use of a single personal identity number, based on birth registration, and the use of a unique company identification number (in order to distinguish between natural and juridical persons) are the basis of the federal government's e-government strategy, especially with regard to the process of authentication required by provision of services.

Open Source Software

Belgium has become one of the leading European countries in open source software development and promotion. This country has hosted the annual Free and Open Source Software Developers' European Meeting (FOSDEM) since 2000.[26] Furthermore, eID has provided encouragement for the development of this kind of software, especially with regard to identity card authentication. In 2010, Fedict announced three new Open Source eID-related projects: the eID Applet (which allows the eID to be used via a search engine), the eID Middleware (which permits the signing of documents and e-mails), and the jTrust (the Java library, which enables eID solutions to be validated).[27]

Privacy Protection

The right to privacy is constitutionally enshrined in Article 22 of Belgium's constitution. This article established that every citizen has the right to respect for private or family life, except in some cases with clearly established exceptions. In 1992, moreover, the government enacted the Data Protection Act, establishing strict conditions regarding rights and obligations for both the citizens whose information is being processed and for agencies that process the information. A privacy protection commission was created for this purpose, as an independent authority responsible for implementing and guaranteeing compliance with the law. This law, however, applies only to the processing of personal information by automatic means and to data processing within an archive system, whether in automated form or not.[28] This law was modified in 1995 following the ratification of the European Directive on data

[26] FOSDEM Free and Open source Software Developers' European Meeting http://www.fosdem.org/2011/

[27] OSOR Open Source Observatory and Repository for European Public Administrations http://www.osor.eu/news/be-three-eID-projects-published-as-open-source

[28] Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data. Belgian Official Journal. 18 March 1993

protection.[29] This directive is framed within the European Convention on Human Rights, to which all EU member countries are signatories and which, in Article 8, enshrines the right to "respect for private and family life, for the home and for correspondence."

Identity Theft

In 2004, the Belgian federal government recognized identity theft, within the context of electronic transactions, as one of the priorities in its crime prevention and combat strategy, and highlighted the need for greater cooperation and coordination between government agencies, with emphasis placed on the user/citizen or eventual victim.[30] Furthermore, in conjunction with the International Consumer Protection and Enforcement Network (ICPEN), Belgium has developed diverse initiatives aimed at preventing this kind of offence. However, the Belgian Penal Code does not have a specific law that punishes identity fraud and identity theft, nor is there a legal definition of identity-related crimes.[31]

Chile

Chile occupies position number 34 amongst the 184 countries on the United Nations (UN) electronic government-ranking list (2010). The situation, however, is the opposite of Belgium's. In Chile, the current identification policy contains and specifically contributes to the development of electronic government in the country, through the introduction of a new identity card. Although there is currently no specific penal category for identity theft, this offence has been categorized under the description of name usurpation.

Identification Policy

In 1884, the Civil Registration Act was passed, as part of the so-called "lay laws" that resulted from the breakdown of diplomatic relations between Chile and the Vatican State, and thereby initiated the Chilean State secularization process. In 1943, the Civil Registry Service began to assume the tasks previously conducted by the Identification Service *(Servicio de Identificación*), which operated at that time under supervision by the Investigative Police (PDI, or *Policía de Investigaciones*). This process ended in 1980, with the final merger of the identification and civil registry service offices.

[29] Directive 95/46/EC.

[30] Framework Note on Integrated Security. Belgium Service for Criminal Policy 2004.

[31] Fidis Belgium The debate about identity-related crime. http://www.fidis.net/resources/deliverables/hightechid/d127-identity-related-crime-in-europe-big-problem-or-big-hype/doc/4/

Currently, the 470 offices that the Service of Civil Registry and Identification (SRCeI, or *Servicio de Registro Civil e Identificación*) has throughout the country are interconnected through a central database. Additionally, there are also mobile offices with satellite links, capable of reaching people and places far outside the customer care centers. Furthermore, a virtual office was created in 2001 (*Oficina Internet*) to issue birth, death and marriage certificates, and free cancellation of lost or stolen identity cards, driver licenses, and passports to help prevent identity fraud. In 2008, the virtual office issued more than 1,800,000 certificates online.[32] At first, however, some areas of the public administration refused to accept the validity of these documents, due to the change of design and paper quality; fortunately, this situation has improved over time. A new identity card was introduced in 2002, which incorporates digitalized images of the bearer's photograph, signature, and fingerprints, which are gathered and stored centrally. The identity card is obligatory for every resident over 18, and costs CLP 3,600 (approximately US$6.50).

In the case of Chile Solidario*,* a conditional cash transfer program that was set up in 2002 as a government strategy aimed at combating extreme poverty the State subsidizes nearly 80 percent of the cost of the identity cards for beneficiaries of the program, reducing the final cost to the user to only CLP 500 (approximately US$1). This is done because all beneficiaries of the program must have a valid identity card.

The *SRCeI* has, at present, two databases, one pertaining to the civil registry and the other to identification services. These two databases have the capacity to interoperate both between themselves and with other governmental agencies, such as the police and Inland Revenue. This is not, however, carried out by use of a single code, but rather through the use of a Unique National Registration Number (RUN, or *Rol Único Nacional*), which is assigned to each person during his or her birth registration. The *SRCeI* is currently installing a new electronic platform, as well as new identity cards and passports that are compliant with ICAO recommendations. In this way, it hopes to improve in interoperability among public organizations, citizens, and the private sector and, moreover, to enhance the confidentiality and integrity of the information that this service manages. The new smart card will have a microchip and digital certificate support for the electronic signature and its authentication. It is expected that the security of electronic transactions will be thereby enhanced, particularly with regard to the government's digital strategy.

[32] Public accounts of the *Servicio de Registro Civil e Identificación*. Chile, 2009.

Electronic Government

The Ministerial Committee for Digital Development *(Comité de Ministros para el Desarrollo Digital*), created in 2007, is responsible for designing and executing the public policy that enables the actions needed to increase the use of ICTs throughout the country. This policy is set out in the country's 2007–2012 digital strategy, and its primary declared objective is "to contribute to the country's economic and social development by harnessing the potential offered by the use of information and communications technology to improve the quality of education, enhance transparency, increase productivity and competitiveness, and achieve better governance through greater citizen participation and commitment."[33]

This strategy lays out four main strategic guidelines: institutional design, digital development programs and projects, IT industry development strategy and the digital development technological policy. The latter establishes an appropriate legal framework for personal data protection; the incorporation and widespread employment of standards to promote interoperability and enable access to ICTs; the use, promotion, and development of open source software and the improvement of data security in information exchange and electronic transactions.

Open Source Software

A survey to determine the extent of open source software use throughout the public administration, commissioned by the digital strategy and carried out by the Department of Computer Sciences at Chile's Catholic University, produced the following results:[34]

- The use of open source software applications is low and, in a high proportion of application types, marginal. According to the results obtained, there seems to be some mistrust of applying tools based on open source software due to lack of professional backup as a commonly available service and the scarcity of professionals providing maintenance for this kind of software solution.
- There are certain tools, such as those related to databases, which have gained ground in comparison with commercial solutions, due to the competitive advantages (costs) that have allowed them to be successfully introduced into the administration.
- According to the survey's results, the disadvantages associated with open source software have meant that its adoption has not been considered an immediate priority

[33] Comité de Ministros Desarrollo Digital (Ministerial Committee for Digital Development) Estrategia Digital Chile 2007-2012. December 2007.

[34] *Estrategia Digital* (Digital Strategy) *Uso de Software Libre en el Estado*, 2008–2009 Edition.

by the public agencies consulted. An opportunity for further development does occur, however, where the ICT areas are smaller and the measures offer cost reduction prospects. The implementation of open source software in smaller functional areas allows implementation to be more easily monitored, without demanding large investments in training.

Finally, it can be concluded that the development of this kind of tool is limited go to the government level, and that the prospects for development are not encouraging, at least until its advantages and disadvantages are much better known, from both the user's and the perspective of decision makers.

Privacy Protection

Article 19, Nº4, of the constitution establishes everyone's right to "respect and protection of private life, and to the dignity of the person and the family," and in 1995 a paragraph was added to the Chilean Penal Code that addresses the crimes against a person and his or her family's private and public life. Subsequently, in 1999, Law 19628 definitively established the protection of personal information. The first article states that the provisions of this law will be binding for "the handling of information of a personal nature in records and databases by either public organisms or private individuals," and that "anyone may process personal information, providing that it is always conducted in accordance with this law, and for purposes that are permitted by the legal framework. The full exercise of the fundamental rights of the data owners, and of the faculties granted to them by this law, must be respected in all cases."[35]

Finally, in 2008, Law 20285 (concerning access to public information) created the public agency charged with monitoring compliance with Law 19628. According to Article 33 (letter M), it is the responsibility of the Transparency Council to monitor adequate compliance by State administrative agencies with the provisions of Act 19628. Previously, the Ordinary Tribunals were responsible for exercising this control, which was conducted ex-post. Their disciplinary power was thereby restricted in practice to the occasional presentation of judicial actions on behalf of those data owners who alleged that their rights had been violated, and went no further.

Finally, a parliamentary motion was presented in 2010 aimed at modifying Act 19223, which establishes the penal categories relating to computer crime. However, to date, it

[35] *Ministerio Secretaria General de la Presidencia*, (Ministry of the Presidential General Secretariat) Act 19,628 *Sobre Protección a la vida Privada* (Protection of Private Life). Chile 1999, Article 1.

not a considered a criminal offence for a civil servant, regardless of job description within the State administration, to steal data contained within an information system under his or her responsibility after being dismissed from the position. The new draft legislation, however, indicates that the civil servant who, before being relieved of his or her respective duties for any legally justified reason, steals data from a public information system will be sentenced to short-term imprisonment, to the medium or maximum degree (from 541 days to five years).

Identity Theft

There is no criminal category in Chile's current legislation that considers identity theft to be an offence, and thus it has only been punishable after judicial interpretation of Article 214 of the Chilean Penal Code, which establishes the crime of name usurpation.[36]

According to Chile's PDI, the complaints in these cases range from men who put their ex-partner's name on a prostitution website or women who steal their ex-partner's Facebook access codes to post false messages, to much more complex questions, such as the hacking of e-mail accounts and the use of the victim's name to obtain money, or exploiting the e-mail owner's list of contacts for fraudulent purposes (so-called phishing). In 2007, the PDI received only 18 complaints of this nature, but by 2009 the number had increased to 78. The orders to investigate (cases that are forwarded from the regional public prosecutor's offices) also increased, rising from 32 in 2007 to 108 in 2009. According to the PDI one of the most effective ways of preventing this kind of crime is the development of a centrally administered national identification system that allows the rapid verification of personal data and the cancellation of the national identity card as soon as it has been reported stolen.

[36] Heading IV: *DE LOS CRIMENES Y SIMPLES DELITOS CONTRA LA FE PUBLICA, DE LAS FALSIFICACIONES, DEL FALSO TESTIMONIO Y DEL PERJURIO* (Of Crimes and Misdemeanors against the Public Faith, Forgeries, False Witness and Perjury). Paragraph 8: The illegal exercise of a profession, and the usurpation of a name or function. Article 214: He who appropriates another's name will be punished by short-term imprisonment to the minimum degree, without prejudice to the sentence that might arise as a consequence of the harm caused to either the reputation or the interests of the person whose name has been appropriated.

Mexico

Mexico occupies the 56th position among the 184 countries in the UN electronic government ranking (2010). Of the three countries analyzed, it has lowest levels of governance (World Bank, 2009). Although it does have a national electronic government strategy, this policy, in common with Chile, is not related to its legal identification policy. The main reason might be that Mexico has only recently begun to implement a national identity card (CEDI, or Cédula de Identidad), prompted more by security issues than anything else.

Identification Policy

The Political Constitution of Mexican United States establishes the obligation of every Mexican citizen to be inscribed in the national citizen registry (*Registro Nacional de Ciudadanos*). For this purpose, the General Population Act (*Ley General de Población*) states that the Government Secretariat is in charge of the registration and irrefutable authentication of the identity of all people settled in the country, and of the Mexican citizens living abroad, and should draft the rules, methods and technical procedures needed to establish the national population registry (RENAPO, or *Registro Nacional de Población*).[37]

RENAPO is therefore responsible to register all persons, using data that will enable them to certify and irrefutably accredit their identity, thereby endowing them with the legal certainty needed for the full exercise of their rights.[38] This service emits the Unique Population Registration Key (CURP, or *Clave Única de Registro de Población*), which, according to the Government Secretariat, constitutes an instrument that serves to individually register all inhabitants, both foreigners and locals, as well as those Mexican citizens living abroad.[39] Although this key is linked to the birth certificate and is recorded in the passport, it contains no biometric information about the bearer.

In 2009, the government issued the CEDI. The Government Secretariat, via the Directorate General of RENAPO, is responsible for setting in motion the National Personal Identification Service *(Servicio Nacional de Identificación Personal*), which is directly responsible for providing a unique identity system supported by a national database, to be

[37] Modernización Integral del Registro Civil: Conceptos y Estructura. Programa de Modernización Integral del Registro Civil. Mexico 2001.

[38] Registro Nacional de Población (National Population Register) http://www.renapo.gob.mx/RENAPOPortal/

[39] Secretaría de Gobernación Mexicana (Mexican Government Secretariat) http://www.gobernacion.gob.mx/Portal/PtMain.php?pagina=faq

comprised of the legal identity of each and every resident of the country with their corresponding biographic and biometric details. The CURP will be employed for this purpose, alongside the biometric information. The expected final result is that every person will have a unique registration and identity card, thereby guaranteeing their identity.

According to government announcements in Mexico, a database has already been built containing 84 million birth affidavits certified by civil registries in every state in the country, representing authentic copies of the contents of the corresponding original documents.[40] The biometric information obtained by the measurement of fingerprints, face, and iris will be integrated with this information, thereby guaranteeing that each individual has a unique valid birth registration alongside the corresponding biometrics. Furthermore, this new smart card will contain a chip to facilitate commercial electronic traffic and the development of the electronic government strategy.

Electronic Government

In 2000, the government launched the National e-Mexico System (*Sistema Nacional e-México*), a policy aimed at articulating interests both between and within distinct levels of government, telecommunications companies, ICT enterprises, and diverse educational institutions, with the principal objective of extending the coverage of basic services such as education, health care, economy, governance, science, technology, and industry, among others.[41] It also aims to contribute to reducing the digital divide.

During 2001, the Digital Government Strategy (*Estrategia de Gobierno Digital*) was established, coordinated by the Public Function Secretariat *(Secretaría de la Función Pública*), which was aimed at promoting the use of ICTs to improve governmental management efficiency, bring more transparency to the public function in all spheres of government, and combat corruption within the federal public administration. This strategy, also termed e-Government, was constituted as a component of the National e-Mexico System.[42]

In 2002, the Presidential Agenda for Good Governance was established to ensure the following within the government: honesty and transparency, professional behavior, high standards, digital development, well-regulated activities, and reduced operating costs. The digital government guideline is intended to "establish a government that optimizes the

[40] Federal Government of Mexico. http://www.presidencia.gob.mx/buscador/index.php?contenido=46891

[41] Executive summary of the National e-Mexico System. *Coordinación General del Sistema Nacional e-México*, September 2002

[42] *Estrategia de Gobierno Digital de México* http://www.gobierno-digital.gob.mx

potential of information and telecommunications technology, not only as a way of combating corruption and enhancing transparency in the public function, but also to promote the efficiency and quality of the services and products offered to the citizenry."[43]

The Inter-Secretarial Commission for Digital Government Development (CIDGE, or *Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico*) was set up in 2005. In its Article Nº 9, the founding agreement states that the commission "is a strategic agency whose primary objective will be to support, guide, and harmonize actions aimed at developing electronic government, as well as to use and take advantage of ICTs throughout the federal public administration."[44] The same article sets out the commission's functions, including the following:

- To identify the administration's ICT needs and recommend the actions required for their development;
- To support agreements that seek the economic resources needed for project development, with both national and international organizations, dependencies, and entities, whether public or private;
- Promote the establishment of mechanisms to coordinate and collaborate among federal powers, the Procurator General of the Republic, the governments of the federal entities and the municipalities, and the public and private institutions, both national and international, in order to propitiate the exchange of experiences and information, analyze common problems, and carry out joint ventures in the field of electronic government and ICTs;
- Propose the establishment of a technological architecture within the federal public administration, with a vision oriented to define and align government processes, via operating models that enable opportunities to replicate or reuse resources, enhance effectiveness, and obtain savings in costs by improving the services offered to the citizens.[45]

Finally, in 2009 the Public Function Secretariat drafted the Digital Government Agenda, aimed at increasing government efficiency through the digitalization of

[43] Fox, Vicente. *Agenda Presidencial para un Buen Gobierno*. II Forum of *Innovación y Calidad en la Administración Pública*. Mexico 2002.
[44] Agreement designed to create in permanent form the Inter-Secretarial Commission for Digital Government. *Secretaria de la Función Pública de México* (Public Function Secretariat). DOF 2005.
[45] Ibid.

administrative procedures and the employment of information and communications technology. Through this agency, the federal public administration will establish digital government development strategies aimed at providing better services, facilitating access to information, enhancing accountability and transparency, and strengthening citizen participation. The Model for Digital Government, a citizen-centric strategy, was also presented alongside the agenda. The model contains various elements organized on different levels, which range from the creation of procedures and services, to customer care and attention. The aforesaid model covers three main areas: a) internal governmental operation, b) customer care desk and, c) the users. The final objective is to reduce the digital divide that currently exists within and among some federal administration institutions.[46] However, some of the government's immediate challenges in the field of ICTs are the use of the advanced electronic signature; the standardization of the management monitoring system; the issuing of the new identity card; the implementation of Government Resource Planning (GRP); the integration of a rapid business start-up system; and the creation of electronic clinical records.[47]

Data Protection

Article 16 of the Mexico's constitution establishes the legal framework for privacy protection. The first paragraph of this article enshrines one of the most important individual guarantees, by establishing that no one should be interfered with personally and in terms of their family, home, documents, or possessions, except by virtue of express written authorization by a competent authority that substantiates and justifies the legal motive for the procedure. The second paragraph establishes the right to the protection of personal data, and to the access, rectification, and cancellation of the same, as well as the right to demonstrate opposition within the terms of the law. The aforesaid law will establish the cases that are exempt from the principles of data handling, either for reasons of national security, public order dispositions, public health and safety, or to protect the rights of third parties.

In 2010, as a result of the constitutional reform of 2009, which modified Article 73 and endowed the Mexican Congress with the powers to legislate on the issue protecting data held by private parties, the Federal Act on the Protection of Personal Data held by Private Parties *(Ley Federal de Protección de Datos Personales en Posesión de los Particulares*)

[46] Press Release No. 01/2009. Public Function Secretariat of Mexico. Mexico 2009.

[47] Patiño Calderón, Carlos. 2009. *Agenda de Gobierno Digital: proximos pasos. CIAPEM*. Chetumal, Mexico.

was approved and published in the Official Federal Bulletin (*Diario Oficial de la Federación*) by the Government Secretariat on 5 July 2010.[48]

Identity Theft

The Federal Act on the Protection of Personal Data held by Private Parties contains a specific chapter dealing with crimes deriving from the unlawful use of personal data. Article 67 establishes prison sentences of three months to three years for those who, for personal financial gain, take advantage of their authorization to handle personal data to provoke a security breach in the databases under their custody. Article 68 envisages custodial sentences of six months to five years for those who, for undue personal financial gain, handle personal data with deception, thus taking advantage of errors incurred by either the owner or the person authorized to transmit the data. Finally, Article 69 establishes that if sensitive personal information is involved, then the sanctions described in this chapter could be doubled.[49]

Prior to the enactment of this law, there was an initiative put in place by the Federal District Legislature, which created Chapter III (Heading XII) of the Federal District's Penal Code.[50] This aimed at categorizing the crime of identity or personality usurpation, stipulating that all those that supplant, alter, falsify, or reproduce official documents deserve a punishment ranging from two to six years in prison, and a fine equivalent to between 400 to 600 days minimum salary for those condemned for this crime.[51] The DF Penal Code, however, already considers these practices to be crimes, and the Cyber Crime Special Combat Unit is responsible for their investigation.[52]

[48] Decree that enacts the *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (Federal Act for the Protection of Personal Data held by Private Parties) and reforms Articles 3 (Sections II and VII) and 33, as well as the designation of Chapter II (Heading II) of the *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. (Federal Transparency and Access to Public Governmental Information Act) Government Secretariat, Mexico 2010 http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

[49] Federal Act on the Protection of Personal Data held by Private Parties. Chapter XI: *De los Delitos en Materia del Tratamiento Indebido de Datos Personales* (Crimes concerning Unlawful Use of Personal Data), Articles 67, 68 and 69. Government Secretariat, Mexico 2010.

[50] *Estados Unidos Mexicanos, H. Congreso de la Unión Boletín N°. 1842*. Chamber of Deputies.

[51] Bulletin UNAM-DGCS-457, *Ciudad Universitaria*, 2010.

[52] Ibid.

Table 2. Comparative Indices

Indices	**BELGIUM**	**CHILE**	**MEXICO**
Governance level 2010 (World Bank)	Very high	High	Medium
Revenue level 2010 (World Bank)	High	Medium-high	Medium-high
e-Government ranking 2010 (UN)	16/184	34/184	56/184
Human Development Index UNPD (2009)	17/182	44/182	53/182
Administrative dependence of civil registry and identification	Municipality	Ministry of Justice	Government Secretariat
Obligatory identity document	Yes, from the age of 12 onwards	Yes, from the age of 18 onwards	N/D
Use of biometrics	Yes	Yes	Yes (implementation stage)
C2G confidence level 2008 (*Latinbarómetro*)	N/D	High: 2.6% Some/little: 79.3% None: 18.1%	High: 2.8% Some/little: 67.3% None: 29.8%
Well-defined e-Government policy	Yes	Yes	Yes
Identity protection laws	Yes	Yes	No
Explicit technical standards	No	No	No
Identity administration policy	Yes	Yes	Yes
Level of open source software Use	High	Medium	N/D

Source: Author's elaboration.
N/D No available data.

APPENDIX 2: GLOSSARY

APF: acronym for *Administración Pública Federal de México* (Federal Public Administration of Mexico)

Biometrics: the automated use of physiological or behavioral characteristics in order to establish or verify an individual's identity.

C2G: Citizen to Government

C2B: Citizen to Business

CEDI: in Spanish, acronym for *Cédula de Identidad de México* (Mexican Identity Card)

CIAPEM: acronym for *Comité de Informática de la Administración Pública Estatal de México* (State Public Administration Computing Committee).

Civil Registration: the continuous, permanent, obligatory, and universal recording of the occurrence and characteristics of vital events (births, adoptions, marriages, divorces and deaths) and other civil status events pertaining to the population by decree, law or regulation, in accordance with each country's legal requirements.

Constitution: the fundamental law of a State that establishes the concept, character, and organization of its government, the scope of its executive power and the way in which that power is exercised.

CURP: acronym for *Clave Única de Registro de Población de México* (Unique Population Registration Key).

e-Participation: the use of ICTs by democratic actors within the political and administrative process, at both local and international levels.

eID: acronym for electronic identity card. A document representing an individual's identity, which serves the purposes of identification, verification, and electronic signature. It is generally a smart card, with an embedded contact or contactless microchip. In Europe, eID represents the incipient identification management trend.

Electronic Government (e-government): the use of information technology by governmental agencies, which have the ability to transform and optimize relations between governments and citizens, businesses, and other government sectors.

Facebook: virtual community created in 2004 in which the user can find friends and join different kinds of organization.

Fedict: acronym for the Service Public Fédéral Technologie de l'Information et de la Communication , or Federal Government Information and Communication Technology Service of Belgium.

FLOSS: Free Libre Open Source Software

G2B: Government to Business

Habeas Data: the right of every person to request access to the public or private records that contain their personal information, or that of their relatives, in order to establish their accuracy and to demand the rectification and/or deletion of inexact or obsolete data, or data that might cause discrimination.

Human Right: universally accepted liberties and benefits that all humans should be able to claim by right in the societies in which they live.

ICAO: International Civil Aviation Organization.

ICT: Information and Communications Technology.

Identity Card: official document containing an individual’s name, profession, and address, and to which further details pertaining to the bearer can be consigned.

Identity 2.0: refers to open source software initiatives aimed at identifying the persons involved in an Internet transaction.

Interoperability: the capacity of information systems and of the procedures that they support to share and modify data, thereby facilitating information and knowledge exchange between them.

Interconnection: the possibility of communicating between two or more points, with the aim of creating a link between them, either temporarily for a single transaction, or fixed online to allow permanent communication between two machines.

Kids-ID card: Belgian identity card for children under the age of 12.

Law: the declaration of the will prescribed in the constitution, which orders, prohibits, or permits.

MRTD: Machine Readable Travel Documents

OECD: Organization for Economic Cooperation and Development

Open source software: software that can be acquired free of charge. Its source code (which contains the instructions needed by the computer to execute the software) can be legally studied, modified, and subsequently distributed to other users, also free of charge.

Passport: official document that identifies the bearer as a national of the issuing State.

Phishing: an attempt by an individual or group, to obtain personal data through deceptive computerized means (so-called social engineering techniques).

Pharming: identity theft method that consists in redirecting users from a genuine website to a fraudulent one that replicates the original.

Public Key Infrastructure (PKI): infrastructure that provides the improved levels of confidence required for information transactions conducted over the Internet.

Regulation: legal rule enacted by the executive branch according to the powers bestowed on it by the constitution and the law.

***RENAPO*:** acronym for the *Registro Nacional de Población de México* (National Population Registry of Mexico)

***SRCeI*:** acronym for *Servicio de Registro Civil e Identificación de Chile* (Civil Registry and Identification Service of Chile)

***SII*:** acronym for the *Servicio de Impuestos Internos de Chile* (Inland Revenue Service of Chile).

Smishing: method of identity theft in which the user receives an SMS text message in which a certain company confirms that a service has been contracted, and that the payment will be collected unless the order is cancelled on the company's website. This website is, however, set up to steal the affected user's personal data.

Social Networks: a designated grouping of actors, either individuals or groups, linked to one another through a combination of social relationships.

Twitter: real-time information network, fed by people all over the world, which allows the user to instantly share and discover whatever is happening.

Visa: authorization to enter, leave, remain, or transit through a country, issued by the consular authorities of the country to be visited.

Vishing: an identity theft technique that occurs when the trickster invites another person to call a certain telephone number. The user is then connected to an automated answering service, which solicits personal data before proceeding.

Web 2.0: social phenomenon in which the Web is perceived as a user-centric platform design that extends throughout all the apparatuses connected to it, thereby facilitating information sharing and system interoperability.