A National Identity Management Strategy to Enhance the Brazilian Electronic Government*

José Alberto Sousa Torres[1], Glaidson Menegazzo Verzeletti[2,3], Rodrigo Távora[1], Rafael Timóteo de Sousa Júnior†[1], Emerson Ribeiro de Mello‡[2], Michelle Silva Wangham§[3]

[1]University of Brasília, DF, Brazil
alberto.torres@redes.unb.br, r_tavora@hotmail.com, desousa@unb.br

[2]Federal Institute of Santa Catarina, SC, Brazil
glaidson.verzeletti@ifsc.edu.br, mello@ifsc.edu.br

[3]University of Vale do Itajaí, SC, Brazil
wangham@univali.br

Abstract

Amongst the several problems with the Brazilian e-government services (e-Gov), many of them are related to the fact that Brazil does not have a National Strategy for Digital Identity Management (IdM). To design a national strategy, it is crucial to analyze the solutions adopted in other countries and take into account Brazilian characteristics, such as its area, population, digital inclusion index, socio-political and economic profile, the current national identity registration system and the fraud rate. In this context, this paper aims to propose a national strategy for IdM for the Brazilian e-Gov program. This strategy was built upon by a literature review of the experiences of European countries and, mainly, the peculiarities inherent to Brazil.

Keywords: e-government, Identity Management

1 Introduction

Information and Communications Technologies (ICT) are modifying various sectors of the economy and society itself. According to [1], government provides the legal, political, and economic infrastructure support and it can directly influence on the development of various sectors of the society. Therefore, electronic government (e-Gov) has the possibility to deeply modify citizens lives because it brings efficiency to interactions between government and the society (i.e. tax payments, certificate issuing, etc.).

The design and deployment of e-Gov services need to be as inclusive as possible. That is, the solution needs to be suitable for different types of devices, such as computers, smartphones, tablets, and even for low speed Internet connections. Moreover, the services need to suitable for people with different levels of knowledge (computing skills) and accessibility. Besides, e-Gov solutions should simplify the interaction between citizens and government and they should not make it more bureaucratic and complex [2] [3]. For the Organization for Economic Cooperation and Development - OECD [4], e-Gov strategies shall understand the citizens needs, and aim to build connected services instead of compartmentalized services (silos) and it should consider the return on investment.

*A shorter version of this paper was presented in the 2016 Latin American Computing Conference (CLEI), Valparaíso, Chile, October 10-14, 2016.

†Supported by the Brazilian research and innovation Agency CAPES – Coordination for the Improvement of Higher Education Personnel (Grant 23038.007604/2014-69 FORTE – Tempestive Forensics Project) and the Ministry of Planning, Development and Management (Grant 005/2016 DIPLA – Planning and Management Directorate).

‡Supported by the National Council for Scientific and Technological Development (CNPq) scholarship 200995/2015-4, Brazil.

§Supported by the Coordination for the Improvement of Higher Education Personnel (CAPES), Brazil.

Despite the benefits provided by e-Gov, several countries have found difficulties to implement a national strategy to enable e-Gov services advance to higher stages (transactional or connected web) of maturity model proposed by United Nations in its e-government survey [5]. This happens due to a complex implementation process that requires the integration of several agencies in different level of government, the standardization and sharing of data and the use of robust authentication mechanisms.

The OECD report [4] pointed out that national strategy for identity management (IdM) was a crucial factor to the success of e-Gov programs in many countries. The report also pointed that many nations had made efforts to create a national IdM strategy to support their e-Gov programs. The most of nations are looking for robust, reliable and interoperable IdM solutions.

Identity management can be understood as a set of policies, processes and technologies that can be used to ensure the quality of information associated with an identity (identifiers, credentials and attributes) [6]. Thus, IdM allows that these identities can be used for authentication and authorization mechanisms. In a real world scenario each person defines what personal data he wants to share in a transaction with another party. For the digital world, this role is played by identity management systems.

According to the United Nations (UN) study [7], Brazilian government has not set its national strategy for identity management, however it only published a framework about interoperability standards known as e-PING [8]. According to [9], this fact has impacted negatively on the country's position in the UN e-Gov ranking. In the last edition of the study [7], Brazil holds the 57^{th} position.

In this paper, we propose national strategy for identity management to boost Brazilian e-Gov, to improve services security, to provide level of assurance to identify citizens and to enable the citizen's data share between entities in different levels of government. The proposal considers the country's peculiarities such as the large territorial area, digital inclusion index and the high rate of electronic fraud.

The rest of this paper is organized as follows. Section 2 describes identity management background. Section 3 presents an analysis of national strategies identity management adopted by European top countries in the UN e-Gov ranking. Section 4 presents a diagnosis about e-GOV and identity management in the Brazilian government. Then, a national strategy for identity management to boost Brazilian e-Gov is described in Section 5. Finally, Section 6 concludes the paper and introduces some future work.

2 Identity Management (IdM) Background

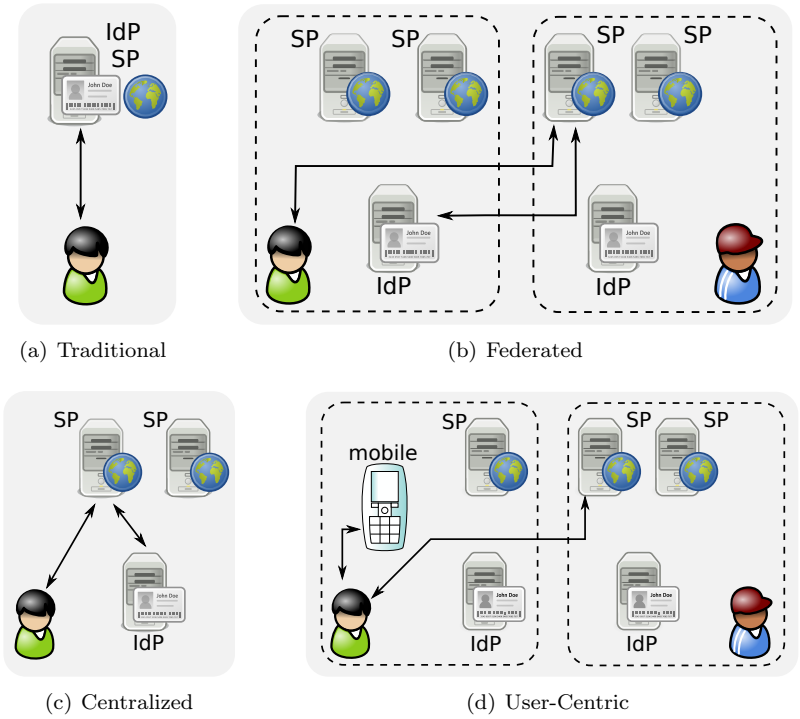
The identity of a person comprises a set of data that represents an individual within a certain context [10]. Depending on the situation and the context, the person may be represented by different identities (or partial identities). In the digital world, the number of electronic identities (eIDs) that a person can have is even greater when compared with the real-world, since the Internet allows interactions with systems that are spreaded on the network.

According [6], an eID may be comprised of:

- Identifier - a series of digits, characters and symbols or any other form of data used to uniquely identify a person (e.g., UserID and e-mail addresses);
- Credentials - an identifiable object that can be used to authenticate the claimant is what it claims to be (e.g., digital certificates, tokens and biometrics);
- Attributes - descriptive information bound to a person that specifies a characteristic of a person.

As defined in [11], an identity management system is the integration of technologies, policies, and processes, resulting in a user authentication system combined with an attribute management system. An IdM system involves three main entities, namely user, identity provider (IdP) and service provider (SP). The IdP is responsible for authentication and user information management. Authentication can be defined as the process of establishing confidence in user identities electronically presented to an information system [12]. Meanwhile, service providers (also known as relying parties -RP) are entities that provide services to users based on their attributes [11]. The arrangement of these entities in an IdM system and the way in which they interact with each other characterize the IdM models. [11, 13] classified the IdM models as traditional (isolated or silo), centralized, federated and user-centric, as illustrated in Figure 1.

In traditional model (silo), IdPs and SPs are grouped into a single entity whose role is to authenticate and control access to their users without relying on any other entity (see Figure 1.a). The user must then create a different identity for each SP in which he or she wants to interact. In this model, the providers do not have any mechanisms to share this identity information with other organizations. This makes the identity provisioning cumbersome for the end user, resulting in privacy and usability issues, since the users need to proliferate their personal data to different providers [11]. On the other hand, the main benefit of this model is that the attacks against providers to compromise user identities have a limited impact.



(a) Traditional (b) Federated

(c) Centralized (d) User-Centric

Figure 1: Identity Management Models [14]

The centralized model emerged as a possible solution to avoid the redundancies and inconsistencies in the silo model and to give the user a seamless experience. Here, a central IdP became responsible for collecting and provisioning the user's identity information in a manner that enforced the preferences of the user [11](see Figure 1.c). The centralized model allows the sharing of user identities among SPs and provides Single Sign-On (SSO) [13]. This model has several drawbacks as the IdP not only becomes a single point of failure but also may not be trusted by all users and service providers [11].

The federated identity model is based on the distribution of users authentication task by multiple IdPs which can be selected by the end users. IdPs belong to different administrative domains in a federation (see Figure 1.b). The federated identity management (FIM) is an approach to optimize information exchange related to the identity through trust relationships built in the Federation [15]. Trust agreements between IdPs and SPs ensure that identities issued in a domain can be recognized by SPs from other domains. Single Sing On session can be guaranteed even when the SPs are in different domains. Thus, this model provides conveniences for users, as it allows them to move between various service providers without having to authenticate again. For IdPs, the benefit is that they are able to manage a smaller user base and in turn this information will be more cohesive and updated. FIM allows IdPs to maintain close relationships with end users and it also allows SPs to offload the cost of managing user attributes, passwords and login credentials to trusted identity providers [16].

The negative points of the centralized and federated models focus primarily on the IdP, as it has full power over the user's data. Besides that, the user has to be dependent on an online IdP to provide the required credentials and these systems are referred to as provider centric [11]. In the federated model, while there is identities distribution by several IdPs, users can not guarantee that their information will not be disclosed to third parties without the users' consent.

The user-centric model aims to give the user full control of transactions involving his or her identity data [11]. In the user-centric model, the user identity can be stored on a Personal Authentication Device (PAD), such as, a cell phone or a smartcard (see Figure 1.d). Users have the freedom to choose the IdPs which will be used and do not need to disclose personal information to SPs to guarantee access to the SP [13]. In the user-centric, the IdPs continue acting as a trusted third party between users and SPs. However, IdPs act according to the user's preferences and not according to the interests of SPs. According to [11], the major drawback of the user-centric model it is not able to handle delegations. Several solutions that adopted this model use it combined with FIM or centralized model, however, novel solutions prefer federated model.

The IdM models guide the construction of policies and business processes for identity management systems but do not indicate which technologies should be adopted. Among the IdM technologies, Security Assertion Markup Language (SAML) standard [17] stands out in systems based on the federated identity

model and centralized model. SAML, developed by OASIS, is a platform-neutral standard that defines a common XML framework to exchange security assertions (authentication and authorization information) between IdM system entities. SAML provides interoperability between different authentication and authorization infrastructures (AAI).

The framework defined in the European project STORK (Secure Identity Across Borders Linked) uses SAML 2.0 to implement the federated identity model and ensures eID interoperability [18]. This project aims to enable European citizens to use the eID system of their country in order to access e-Gov services from other nations [19].

According to the United States Government [12], to successfully implement eGov service, Federal agencies must determine the required level of assurance[1] (LoA) in the authentication for each transaction. In this e-authentication technical guidance [12], the Government established and described four levels of identity assurance to help agencies identify and analyze the risks associated with each step of the authentication process.

In [20], the National Institute of Standards and Technology (NIST) provides guidelines for selecting technology based on this guidance. The four LoAs are [12]:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

When developing an IdM system for eGov, designers must consider particular citizen privacy needs. Any IdM system must adequately protect sensitive user information and must adhere to important elements of the privacy policy [21]. In an ideal system, users can determine which and how their identity information will be collected and stored (by IdPs and SPs).

According to [22], determining how to apply principles and guidelines for establishing and maintaining privacy to an IdM system, it is required from the designer a solid understanding of the environment in which the system operates and the risks and benefits that the system must balance.

The most widely accepted set of such principles is the Fair Information Practice Principles (FIPs), which were first developed in the 1970s. Since then, international privacy and information policies are based on the FIPs as the key element for citizens' privacy. In 1980, OECD released a document with guidelines to protect personal data privacy based on the FIPS principles. OECD guidelines have been widely adopted by the OECD member countries [23]. In 2013, the document was revised and updated due to environment changes, such as: (1) the massive data collection; (2) increase of privacy threats; (3) increase in personal data transactions; and (4) global availability of personal data [24].

In the digital world, two core informational privacy concerns are the observability, which is the possibility that others will gain information, and the linkability, which is the possibility to link sensitive data and an individual in different contexts [22].

Privacy controls should be incorporated into the IdM system during the design process (privacy by design). Controls include safeguards for the physical system components as well as policies and procedures that guide the system's implementation [22].

Protection of user identities and personal information can be achieved by using pseudonymous [21]. An IdM designer could apply this principle by preventing global unique identifiers and instead limiting the identifiers' scope to the specified domain. Using different pseudonyms in different contexts could prevent undesired context linkage and profiling by third parties [21, 22].

IdM system designers must also respect the privacy laws and regulations within their jurisdictions. In some areas of the world, such as Europe, a strong legal framework has provided fertile ground for privacy guidance and tools that go beyond the FIPs [22].

3 National Strategies for Identity Management

According to [25], the national strategy for identity management should try to limit the quantity of digital credentials and authentication mechanisms that individuals have to use across public and private sector services. In many countries, a single national electronic Identity (eID) is used for all e-Gov services. The usage of a single identity is convenient for the government because it allows different agencies to have coherent

[1] In [12], assurance is defined as the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

and cohesive information about the users, reducing redundancies within the agencies and also improving the service provisioning to end users [7]. On the other hand, the usage of multiple identities may reduce the usability [25]. The usage of a single eID can increase information vulnerability, which requires a greater effort regarding privacy issues during the planning stage of the project.

In general, solutions adopted for national eIDs normally evolve from practices and regulations already used for traditional identification methods. As shown in [4], all responding countries that launched a national eID card have migrated from their existing paper-based identity card.

Existing policies regarding offline citizen registries indicate how to establish and connect the eIDs to each citizen. The registry process usually respects national cultures; thus, in countries where the federal government is more autonomous, the registry tends to be centralized; in countries that give more autonomy to local administrations, the process is usually decentralised. Countries that have a tradition of a national population registry, or that use national identifiers, are using these systems as the foundation for their eID management strategies, adjusting only the existing infrastructure for electronic use [4].

The United Nations (UN) ranks [7] each country according to the E-Government Development Index (EGDI). The EGDI is a composite measure of three important dimensions of e-Gov, being: (1) the scope and quality of online services index (OSI); (2) a telecommunication infrastructure development index (TII); and (3) a human capital index (HCI).

Using the list of the top 25 countries ranked in the e-Gov study, according to the EGDI report from the 2014 United Nations E-Government Survey, this section will address identity management strategies adopted by 10 European countries on the list. The European continent was chosen because of the fact that 20 out of the top 25 countries in the e-Gov ranking are from Europe with 64% representation[2], and also for having the highest regional EGDI[3], with an average of 0,6936. The criteria for choosing 10 countries amongst the top 20 European countries was based on technical e-Gov documentation available in Portuguese, Spanish, and English. A complete analysis of the top 10 countries of the 2014 United Nations E-Government Survey can be found at [26].

Table 1 shows the rankings of e-Gov development of the 10 European countries mentioned above as well as Brazil, according to the UN E-Government Survey, covering the following aspects: E-Gov Development Index (EGDI), Online Service (OSI), Telecommunication Infrastructure Index (TII), Human Capital Index (HCI), and also eParticipation. The eParticipation index focuses on measuring the use of online services that facilitate the provision of information from government to citizens.

Table 1: Ranking of the countries according to their e-government development indexes

	Rank 2014	EGDI	Online Service (OSI)	Telecom Infrast. (TII)	Human Capital (HCI)	eParticipation
France	4	0,8938	1,000	0,8003	0,8812	0,9608
Netherlands	5	0,8897	0,9291	0,8175	0,9224	1,0000
United Kingdom	8	0,8695	0,8976	0,8534	0,8574	0,9216
Finland	10	0,8449	0,7717	0,8594	0,9037	0,7059
Spain	12	0,8410	0,9449	0,6629	0,9152	0,7843
Estonia	15	0,8180	0,7717	0,7934	0,8889	0,7647
Denmark	16	0,8162	0,6614	0,8740	0,9132	0,5490
Austria	20	0,7912	0,7480	0,7597	0,8660	0,6275
Germany	21	0,7864	0,6693	0,8038	0,8862	0,7059
Italy	23	0,7593	0,7480	0,6747	0,8552	0,7843
Brazil	57	0,6008	0,5984	0,4668	0,7372	0,7059

3.1 National Strategies for Identity Management using Electronic Identity Cards

With the format of an ID-1 plastic card, the electronic identity card (eID Card) has an embedded microchip that allows for storing data for identification and authentication to service providers. Most information printed on the surface of the eID card is exactly the same as the one stored on the chip, which allows for its use both for formal and electronic identification [27]. This section will present the strategies adopted by some European countries that have chosen to use the eID card: Italy, Germany, France, Finland, Spain, Estonia and Austria.

In Italy, citizens can access online services using two distinct cards: the NSC (National Service Card or CNS - Carta Nazionale dei Servizi) and the EIC (electronic identity card or CIE - carta d'identità elettronica). The NSC is not a formal ID card, it was originally conceived to allow online authentication, digital signatures

[2] Asia: 20%. Americas and Oceania: 8%.

[3] World median: 0.4712. Americas: 0.5074. Asia: 0.4951. Oceania: 0.4086. Africa: 0.2661.

and also citizen interaction with e-government services. Regarding the EIC, from January 2006, the paper-based identity card started to be gradually substituted by the eID card known as EIC[4] (electronic identity card) [28]. The EIC is pursuant to the law which was instituted on 31 March 2005, no. 43[5], and must be issued every time a citizen requires a new identity card or the renewal of a document.

In Germany, the eID card (Personalausweis) has replaced paper-based identity cards since its implementation in 2010. It is compulsory as a formal ID card for all German citizens age 16 or older, excluding the online authentication function that can be cancelled upon the citizen's request.

Data printed on the surface of the card is stored on the microchip, with the exception of height, color of eyes, and handwritten signature. According to [29], for the eID to be used as a travel document, biometric information of the holder must be collected and stored on the microchip, furthermore, cardholders may choose to include two fingerprints on the chip, as a way to increase security regarding personal identification. However, the Act on Identity Cards and Electronic Identification[6] assures the citizen the option of the government collecting the fingerprints or not.

In France, in an effort to create an eID card, the government launched an electronic ID project called INES (Secure Electronic National Identity) in 2005. Following the Development Plan for the Digital Economy by 2012, this card would also be used to allow direct participation of citizens in the public decision-making process [30].

The French government assumed that the population would start requesting the card, once it would empower citizens regarding government decisions. However, according to [31], the INES project had to be suspended due to protests, for the people believed that this proposal would impose a threat to individual freedom. Even with an uncertain future, the French government will possibly launch a new generation of eID cards with RFID chips embedded within the cards [32]. It should be be noticed that, even though more than ten years have gone by since the beginning of the INES project, France still hasn't been able to consolidate the usage of an eID card in its Identity Management strategy.

In Finland, the eID card (FINeID[7]) was first issued in 1999, making Finland the first country in the world to implement a national eID scheme [33]. The FINeID card, which is not compulsory, is issued by the Finnish Population Register Centre[8] (PRC) and can be used for civil identification, as a travel document, and also to give access to banking services, medical services, as well as e-government services [34].

The usage of FINeID grants secure access to Service Providers (SPs) and also allows citizens to sign and encrypt digital documents and emails electronically. These functionalities are available due to the existence of two pairs of digital personal certificates, issued by the PRC and stored on the card's microchip [35].

In Spain, the eID card (Documento Nacional de Identidad electrónico – DNIe) was launched in 2006, replacing offline identity documents [36]. Three pairs of digital certificates are stored on the card's microchip [37]:

- **Component certificate:** The purpose of the certificate is the authentication of the ID card through a mutual authentication protocol. With this authentication, an encrypted communication channel between the card and the driver is established.
- **Digital signature certificate:** This certificate aims to prove the citizen's identity and also establish confidential communication channels between citizens and service providers.
- **Content commitment certificate:** Used to sign documents, having the same value as a manual signature.

In Estonia, the first eID cards (ID-kaart) were issued in 2002. The card is mandatory for all Estonian citizens over 15 years of age and is currently issued by the Police and Border Guard. Through a public-private partnership, the eID cards are issued using digital certificates valid for 5 years, granting security for online transactions [38]. The usage of the eID card is varied, serving as a national eID card, a travel document, verifying banking transactions, and enabling citizens to vote electronically (I-voting). It also allows for the viewing of medical history and for giving access to service providers [39].

Estonia was the first country in the world to institute electronic voting for national elections in 2005[9]. One of the features that enabled Internet voting was the usage of personal digital certificates, stored on the microchip of the eID card [39]. According to statistics presented by [40], in the European Parliament elections in 2014, 103.151 voters (31.3% of all participating voters) voted online.

[4] CIE - in Italian "carta d'identità elettronica".
[5] Available at http://www.camera.it/parlam/leggi/05043l.htm
[6] Section 5, paragraph 9 of the Act on Identity Cards and Electronic Identification, available at http://goo.gl/NWrE9A.
[7] Available at http://www.fineid.fi.
[8] Available at http://www.vaestorekisterikeskus.fi/default.aspx?site=4.
[9] Availeble at https://www.valimised.ee/eng/.

In Austria, the first eID cards (citizen card – eCard) were issued in 2002. In 2005, all Austrian citizens received an eID card issued by Health Plan Operators. In 2008, the privately-owned company, A-Trust[10], was allowed to become a card issuer as well, increasing the types of eID cards accepted. Nowadays, any card with an embedded microchip that fulfills the functionalities required by the government can be used for SPs authentication; to do so, the citizens only need to activate their eID cards through one of the following options: online activation on the A-Trust website[11], on the government website[12]; activation in person at a registration site; or activation via registered letter [41].

For [42], the eID cards can be issued with two pairs of digital certificates in Austria. One of them is mandatory, used for citizens to access online e-government systems, the other is optional, it brings extra security functions, and is used for qualified signatures and encryption.

3.2 National Strategies for Identity Management with alternative eID technologies

According to [43], the adoption of new alternative eID technologies is stimulated due to the necessity of offering an universal form of identification in some cases. In other cases, they are stimulated as a way to complement the national programs that use an eID card. In the search of new eID technologies, governments may choose to use open standards and develop their own solutions; create public-private partnerships, purchase ready-made solutions; or develop a solution where the private sector can be responsible for only part of the process.

In this context, the usage of a mobile device (mobile eID) or an eID applet in EMV smart cards, comes as an alternative to the eID card. Mobile devices can be used as proof of possession in the electronic authentication process, enabling the storage of the user's attributes as well. In [44], it is shown that private-owned companies have increased their interest in developing mobile eID solutions for governments.

Using access credentials that only require username and password from a single or multiple IdPs, has also become an alternative to the eID card usage in some countries. Based on this approach, the identity provider stores the citizens attributes. According to [11], using a single IdP has the advantage of mitigating the possibilities of sharing the user's' credentials. On the other hand, using multiple IdPs gives the user the power of which identity provider to choose. In this perspective, using an OTP (One-Time Passwords) token offers an additional security layer for the traditional username and password usage.

In the following subsections we will present the strategies adopted by Estonia, Finland and Austria that use mobile eID in their identity management strategies. We will also present the strategies used by Spain, Denmark, United Kingdom and Netherlands that have adopted to use access credentials with a single username and password for their citizens.

3.2.1 National Strategies for Identity Management using Mobile ID

In Estonia, the mobile ID service (Wireless PKI) was launched in May 2007 as an alternative to the existing eID card [45]. The service is provided by a mobile carriers such as EMT[13], Elisa[14], Tele2[15] e Lithuanian[16] in cooperation with several banks and the Estonian Certification Center[17] (AS Sertifitseerimiskeskus). Just as the eID card, the mobile ID enables authentication to e-government services, as well as digital signing of documents. This is possible because the users' certificates are stored on the SIM card of the mobile device, where the private key is accessed by entering a personal identification number (PIN) [39].

In Finland, an alternative to the eID card is also offered through mobile ID. The telecom carriers of the country, like Sonera[18] and Elisa[19], offer citizens the option to use a SIM card that has encryption support, allowing users to securely access banking applications, e-commerce and electronic government services [33].

In Austria, apart from the eID card, the government has offered citizens a mobile ID solution (Mobile Phone Signature) since 2009. This solution was developed in the EU pilot project on interoperability called STORK [46] with the EU Commission support. The mobile eID solution is offered in the country through a server based architecture, where an HSM (hardware security module) stores the citizens' private keys in a safe manner [44]. The authentication for accessing the keys is made with a possession factor, the SIM card, a knowledge factor and a password. The activation of the mobile ID in Austria is similar to the eID card

[10] Available at http://www.a-trust.at.
[11] Available at https://www.a-trust.at/e-card/selfdata.aspx.
[12] Available at https://finanzonline.bmf.gv.at.
[13] Available at https://www.emt.ee/en/liitu.
[14] Available at https://www.elisa.ee/.
[15] Available at http://www.tele2.ee/.
[16] Available at http://www.omnitel.lt/klientu_aptarnavimas_telefonu.
[17] Available at https://www.sk.ee/en.
[18] Available at http://www.sonera.fi/.
[19] Available at https://elisa.fi/.

activation. Another noticeable characteristic of the identity management strategy is related to the quantity of eIDs a citizen can have [41], which allows a person to have as many eIDs, as desired.

3.2.2 National Strategies for Identity Management using Username and Password

In Spain, besides having the eID card (DNIe), the government launched a new framework in 2014. This framework allows citizens to identify to an SP by means of shared keys (user and password), avoiding the need of lots of different keys for accessing SPs [47]. Known as Cl@ve[20], this framework allows user online registration and also improves security for accessing the SP using an OTP token, which is sent to the user through an SMS message. Thus, this solution can be used as an alternative to the country's eID card.

In Denmark, the government, in collaboration with the private contractor DanID[21], has developed the NemID as the eID solution for citizens to have access to public and private services on the web such as banking services as well as e-government services [48]. In order to create a NemID, the citizen needs to provide his/her Central Person Register (CPR) number along with the number of the Social Security Card. Thus, these numbers are associated with all NemIDs that the citizen might create. In addition, to each NemID created, a card with a one-time password (OTP) is generated, and an access credential (username and password) chosen by the citizen is created as well.

In the United Kingdom, the government chose to contract private providers to offer eIDs, which give citizens' freedom enabling them to choose whatever Identity Provider (IdP) they prefer. Currently, the following IdPs are accredited by the government: Digidentity, Experian, the Post Office, Verizon, Barclays, PayPal, GB Group, Morpho and Royal Mail [49]. Since there isn't a National ID in the UK, the IdPs end up being responsible for proving a person's identity to Service Providers by crossing data with others information sources.

In the Netherlands, just like in the UK, there are several valid identity documents which can be used to prove one's identity. For the digital world though, DigiD[22] identity provider, developed by the Dutch government, is the only IdP that is accredited to operate. This way, although not mandatory, only one eID per person is allowed , and this eID can be obtained by registering a pseudonym as a login. When registering the eID on the DigiD login page, the citizen must provide his/her Social Security Number (BSN[23]) as a prerequisite to get his/her credential.

3.3 National eID Management Systems and Privacy

As described in the Sections 3.1 and 3.2, the national IDM strategies adopted by governments present a strong presence of the private sector in many countries . This presence can be observed in the following services: issuing eID cards (e.g. Germany); acting as service providers (e.g. Denmark); acting as identity providers (e.g. the United Kingdom); issuing personal digital certificates (e.g. Austria); and also offering mobile ID solutions (e.g. Finland).

Table 2 shows that about 70% of the countries offer more than one eID option to their citizens. This fact confirms the concerns to increase availability of access options for a broader coverage of the population and also democratization of services. Table 2 also presents information regarding the eIDM model adopted by each country. The United Kingdom, Spain, Germany and Italy have opted for Federated Identity models, while other countries have opted for Centralized models.

Although at least half of the countries presented on this paper still use Idm Systems that make use of credentials based on shared secrets (e.g. user and password), it can be observed that many countries have increasingly started adopting mobile ID solutions. This trend shows the concerns of some nations for using emerging technologies. It can also be noted that the choice for standards widely known like SAML is becoming more common. Adopting latter standard allows faster adaptability to systems, assuring the development interoperable e-Gov services [50].

Regarding interoperability, there are currently more than 15 projects being developed around the world. Two of these projects stand out as the most relevant in Europe: the FutureID project and the Stork2 project [51]. FutureID started in 2012 and its main goal is to build a wide, adaptable, ubiquitous, privacy-aware infrastructure able to integrate technologies already available. The Stork Project (Secure idenTity acrOss boRders linKed), on the other hand, aims to assure a convergence of public and private solutions for a safe and user-friendly access to services providers. These SPs can be spread across the European continent [17].

[20] Available at http://clave.gob.es/.
[21] Available at http://www.danid.dk/.
[22] Available at https://www.digid.nl/en/.
[23] Unique identifying number given to every Dutch citizen born from October 1st 1994.

Table 2: Comparative Analysis of Identity Management Systems

	eIDM Models	IdP	IdP Choice	Unique eID Solution	eID Solution	Use of the pseudonym	Privacy Law Enforcement
France	-	-	Yes	No	eID Card	-	-
Netherlands	Centralized	Government	No	Yes	User/Password	Yes	-
United Kingdom	Federated	Private	Yes	No	User/Password	Yes	Yes
Finland	Centralized	Government	No	No	eID Card; Mobile eID	No	Yes
Spain	Federated and user centric	Gov. and Private	Yes	No	eID Card; User/Password	No	Yes
Estonia	Centralized	Government	No	No	eID Card; Mobile eID	No	-
Denmark	Centralized	Private	No	Yes	User/Password	Yes	Yes
Austria	Centralized	Government	No	No	eID Card; Mobile eID	Yes	Yes
Germany	Federated and user centric	Private	Yes	Yes	eID Card	Yes	Yes
Italy	Federated and user centric	Gov. and Private	Yes	No	eID Card	Yes	Yes

Another important aspect related to the e-Gov policy chosen by a specific country is the freedom of choice that citizens have when choosing Identity Providers for authentication. If, in one hand, the United Kingdom chose to contract private IdPs to offer eIDs [49], on the other hand, the Italian government tries to promote the government IdP as the main solution, even though a private-owned IdP is also available in the country [28]. In Denmark, due to the partnership with only one private company, the citizens can only choose between using or not the IdP accredited by the government.

The existence of more than one eID solution is a reality in some countries like Austria, Spain, Estonia and Finland. Apart from the eID card, these countries have also adopted a second eID solution. Some have provided this second option through the usage of shared secrets (e.g. user and password), others by partnerships with telecom operators providing SIM cards with PKI features.

Offering secure and interoperable solutions that preserve, simultaneously, the privacy rights of the citizens is a huge challenge. All ten countries analyzed on Table 2 have specific information privacy and data protection laws. However, law enforcement mechanisms are not always clear in the adopted identity management models. France, for example, for lack of a consistent e-Gov policy, is still trying to consolidate the usage of electronic identity through an eID card [32]. For this reason, it is difficult to measure how privacy laws are being implemented on the eIDM context of that country.

In 1995, the European Union (EU) developed harmonized data-protection legislation to be applied across all 27 EU member states. The European Data Protection Directive [24] forms an overarching privacy regulation that all data controllers within the EU must adhere to. In EU countries, the FIPs (Fair Information Practice Principles) apply in the legal context of Europe, in particular the paradigms of transparency, individual participation, and legitimate purpose. EU data-protection law also stresses the commonly accepted principle of data minimization, limiting them collection and processing of personal data to the extent necessary for the given purpose [22].

In addition to the usage of basic privacy mechanisms, such as the use of an identifier based on hashing of the eID biographic data, the strategies adopted by Austria and Germany stand out for the use of advanced privacy protection mechanisms.

The German system makes use of various resources in order to guarantee privacy. One of the resources for user authentication is the EAC (Extended Activation Control) protocol, a group of cards uses only one key pair, which guarantees the anonymity within the group. This protocol preserves privacy, but weakens the security because it allows personification fraud among people of the same group. Another resource is the storage of both biographic data and identification key only in the ID card chip, protecting privacy but, at same time, making the eID revocation process too complex.

In Austria, on the other hand, a single identification number (CRR-number) is given to each citizen registered at the Central Register of Residents (*Zentrales Melderegister ZMR*). Based on this CRR-number (*ZMR-Zahl*), another unique identifier (called sourcePIN) is calculated and stored in the citizen card. The sourcePIN identifier is created by a reliable state-owned company and is used as the electronic identifier for accessing online applications. What distinguishes the Austrian model from the models found in the other

[24] Available at http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

countries is that the sourcePIN can't be stored anywhere except in the citizen card, due to data privacy legislation [52]

Finally, it can be observed that each analyzed country in this paper implements e-government policies according to local necessities. However, creating privacy laws and improving investments on e-government services is a common goal present in all European countries.

4 Electronic government and identity management in Brazil

Electronic government and identity management are interrelated topics. Several clues associate the definition of national IdM strategies to efforts aimed at attaining higher levels of maturity in e-Gov services [9]. For instance, the UN established a model with four stages of online service development [7]: 1-Emerging information services, 2-Enhanced, 3-Transactional, and 4-Connected services. For a country to be considered in the two most advanced stages (3 and 4), some form of electronic authentication of the citizen's identity is required to be operational in the concerned e-Gov services.

As mentioned, the Brazilian federal government has not yet defined its national strategy for IdM. This fact has led several federal agencies to adopt a silo identity management model [9]. Indeed, each of these agencies is allowed to build its own user base to provide transactional e-Gov services to citizens. This common practice greatly burdens the citizen, who has to create a username-password pair for each accessed service. Also, it creates difficulties and impediments to integrate government services.

These reasons lead us to argue in this paper that the definition of a national eID strategy is a key factor for the advancement of Brazilian e-government. Before specifically describing our proposed strategy in section 5, we discuss in this section some interesting aspects of the current state of e-Gov services and IdM provisioning in Brazil.

4.1 Evaluation of electronic government in Brazil

In the UN ranking of 2014 [7], Brazil obtained a score 0.6008 for its e-government development index (EGDI), which put the country in the 57th position in the world ranking and 8th position in the Americas. In the UN prior report of 2012 [53], Brazil was in the 59th position and had 0.6167 EGDI value.

The EGDI calculation is structured in three dimensions, one of which being related to human capital, thus considering the country's social advancement such as the illiteracy rate or the amount of enrollment in higher education. The other two dimensions are related to the technological infrastructure and the provision of online services. Based on the UN report [7], the study in [9] points out that the social and infrastructure aspects are primarily responsible for Brazil's poor ranking. If we consider only the Human Capital Index (HCI), Brazil occupies the 78th position of the raking. When considering only the Infrastructure Index (ITT), the country occupies the 61st position. If we consider the online services index (OSI), Brazil occupies the 49th position. However, this is the only index that is deteriorating significantly [9].

It seems that a considerable part of this deterioration in the OSI index is a consequence of the difficulty of the Brazilian e-Gov services to reach higher levels of maturity. According to [7], although 100% of Brazilian e-Gov services have already reached the Emerging stage, only 26% of these services reached the last stage (Connected). While in the intermediary stages, 68% are classified as Improved and 28% as Transactional. It is worth to note that in this classification a service can fall into more than one stage simultaneously.

For a service to be classified as Transactional or Connected, it must include strong authentication mechanisms because it is essential to have mechanisms to ensure a person's identity in online transactions with the government, in order to prevent identity fraud. Consequently, it can be inferred that the lack of a national strategy for IdM in Brazil hinders the advancement of e-Gov services to higher levels of maturity.

As a result, the lack of an integrated, unified and robust online citizen identification policy is considered one of the main causes for 40% of e-Gov services that still require the citizen presence [54]. While the in person identification is considered as the highest level of identity assurance, it is possible to consider that there are other means of reliable authentication, which approach that same high level of security for online scenarios.

Thus, the use of authentication methods with higher levels of assurance – LoA, as described in Section 2, is an important requirement so that e-Gov services can reach the Transactional and Connected levels.

4.2 Identity Management in Brazil

The experience of the countries analyzed in Section 3 indicate that eID implementation strategies usually rely on the civil identity registrations. Brazil is among the countries that traditionally requires a civil identification document as a prerequisite for its citizens to interact with public and private entities. On the other hand, National eID is not widely used on eGov services transactions.

However, besides being necessary for the development of advanced e-Gov services, the definition of an IdM strategy is motivated by public security reasons, in particular due to the risk of electronic fraud. In Brazil, identity frauds account for public resources embezzlement, as well as for blows to the private sector. Frauds in public concessions were estimated to be more than 12 billion Reais per month in 2013 [55], in part due to failures in identifying the corresponding beneficiary. In the private sector over 154,000 fraud attempts were recorded and characterized as identity theft, in January 2016, which corresponds to a rate of one fraud attempt every 17.8 seconds [56].

In Brazil, the inertia to define a national identity management strategy may be related to the absence of a national civil identity database, given that the registration of the population and the issue of ID cards have been conducted mostly in a decentralized manner by the Brazilian Federation States which, under the current Brazilian constitution, are autonomous in these matters in relation to the Union.

There was an expectation that this situation would change with the enactment of Federal Law No. 9454 in 1997, which determined the creation of a single national identification number for each Brazilian citizen – the so called Civil Identity Registry (or RIC, for its acronym in Portuguese). This Law also attributed to the Federal Executive branch the authority to create the central registry system. In this context, the States and the Federal District would be responsible for collecting and storing a civilian identity base for the whole country. In this strategy, the central body of RIC would play the role of IdP in a centralized identity management model.

However, after almost twenty years since the enactment of Law 9454, the RIC project is still in the analysis process by the Ministry of Justice (MJ). There are signs that the RIC is unlikely to be put into practice, one of them is the fact that the project was not included among Federal Government strategic projects [54]. Another evidence is the Legislative Bill No. 1775/2015, which deals with the creation of the National Civil Registry (or RCN, for its acronym in Portuguese), a system that is similar to RIC but overseen by the Superior Electoral Court. This Bill is going through many difficulties to move forward in Congress, as it is experiencing a number of extensions requested by the commission which is analyzing the text [57].

The lack of prioritization of the IdM strategy is a fact in Brazil, and as well as in the other countries that are members of Red GEALC (e-government network responsible for establishing goals and e-Gov guidelines for the countries of Latin America and the Caribbean). In 2012, the Declaration of San Jose [58] signed by member countries of Red GEALC did not include the digital identity management strategies on the list of recommendations to be followed by member countries in the following years.

Thus, given the uncertainties surrounding the RIC project, there were some isolated initiatives from Brazilian states to implement their own IdM solutions. The three states of the South, along with São Paulo, Espírito Santo and the Federal District, began to act as IdPs, following the federated IdM model. In 2014, it was reported a regional partnership between the states of Rio Grande do Sul, Santa Catarina, Paraná and Mato Grosso do Sul in order to integrate their civil registration databases [59]. In practice, this initiative aims to establish trust relationships for transactions between these states so that they can share their citizens' biographical information and eventually, as well as their biometric data.

In the Federal District, one of the few states in the country in which all civil identification data are stored in a digital database, there is a pilot program aimed to provide a citizen identification service for notaries, where pricing would be based on the amount of consultations validating customer identities. On the other hand, the State of São Paulo, in partnership with the private sector, is considering a civil identification service that aims to promote the expansion of e-Gov services through the inclusion of digital certificates in the identity card chips [60]. These digital certificates are expected to be issued by ICP-Brazil, the Brazilian Public Key Infrastructure. Much like the Federal District, São Paulo expects to raise revenues by acting as an IdP.

The State of Espírito Santo started the experimental phase of the so-called "Citizen Card", which aims to facilitate access to public services. The available card has a contact chip, which stores a digital certificate, and a contactless chip, which serves to identify the citizen in applications such as turnstiles at public buildings, hospitals, schools and bus [61].

The government of Rio Grande do Sul leads another initiative called "Citizen Login"[25] which aims to integrate services and systems, enabling collaboration in government and private networks. The model brings innovations such as the possibility of a user to associate data to her/his account, as for example the voter registration or the tax revenue individual registration (or CPF, for its acronym in Portuguese). However, the lack of a physical user device, as well as the fragility of the registration process, are barries to using this eID in a series of e-Gov services that require greater user identity assurance.

Despite these initiatives, the lack of financial and human resources hampers the progress of States in structuring their eID systems. This can be confirmed by the diagnosis made by the Ministry of Justice in 2014, which aimed to map the structure of civil identification in the Brazilian states on issues related to

[25] http://logincidadao.org.br/

infrastructure, procedures, human and material resources [62]. This study found that the vast majority of states do not even have an information security policy, nor an adequate infrastructure, such as safe rooms and physically protected datacenters, to host the necessary services.

One of the major concerns presented in [62] was the finding that only Distrito Federal and Mato Grosso have the completely digital civil registry databases, while ten states have never begun the digitizing process of their records. Another significant finding is that 48% of the Brazilian population had not been called for fingerprint data collection. Finally, the mentioned study found that 16 of the 27 surveyed states complained about the limited availability of financial and human resources to ensure the functioning of their Civil Identification agencies.

This section showed us that there is a lack of national identity management strategy and that the current eGov services need to be improved. The following section describes our national IdM strategy proposal that could offer a more efficient, secure and robust solution.

5 Brazilian National Strategy for Identity Management Proposal

The proposal of Brazilian National Strategy for Electronic Identity Management was based on analysis of successful eID strategies adopted by top ranked countries in United Nations e-Gov ranking and on Brazil's singularities, such as the current digital development index of e-government, the digital inclusion rate, the current national identity registration system and the high rate of electronic frauds.

The analysis of IdM strategies of several European countries well-positioned in the UN e-Gov ranking was presented in the section 3. Some important features were observed either in the analysis of the strategies of some countries or in the diagnosis of Brazilian reality. The first perception is that most of the initiatives have been linked to existing national civil identification programs and it was considered a positive way to make the conception of the eID stronger.

The strong influence of federal government in the development of IDM strategies is another important aspect to be observed. In countries where citizen databases are decentralized and owned by the municipalities, such as in the Netherlands, federal government often acts as an integrator of these identities bases and presents them as a single centralized database. In other countries there is a close relationship between government and private companies and because of that, the national strategies were designed to boost both e-government and e-commerce. In some specific cases, such as in the UK, private companies can assume the role of service providers and at the same time act as identity providers of the system.

The study about identity management models showed that most countries adopted centralized and user-centric models and they have developed strategies to enhance user privacy, which is already protected by strict personal data protection laws. The most common authentication factors adopted by countries are eID cards with two digital certificates embedded and One Time Password via SMS messages. Regarding the management structures, it was observed that they are often composed by a central body and an advisory board, as it happens in the Netherlands.

In short, Brazil is a continental country with a decentralized and non-hierarchical political structure composed by municipalities, states and the federal government. It is also a country with a high degree of poverty and it often has budgetary difficulties to implement public policies and to maintain public services, despite being among the ten biggest economies of the world. There is also a high level of corruption and one of the highest rates of identity frauds in the world. Although there is no official data that specifically address the number of electronic identity frauds. But there are researches that refer to the cost of not having a secure identification (both civil and electronic identities). In this respect, studies conducted by the University of Brasilia in cooperation with the Ministry of Justice showed that the Monetary Value of Avoidable costs with the implementation of a secure identification would be between 2,684 billion and 5,315 billion of dollars [63, 64]. In regards to the private sector, only in January of 2016 more than 154,000 fraud attempts known as identity theft were recorded, which means one fraud attempt in every 17.8 seconds in Brazil [56].

This proposal was divided into four main parts, the first one is related to the definition of the management structure, the second talks about the proposal of an identity management system, the third defines the authentication factors, and the last one refers to a identity document model.

5.1 Management Structure

The Management structure refers to the definition of the hierarchy of authority and the specification of roles and responsibilities in IDM strategy. The model proposed here is similar to the currently being adopted in the Brazilian National Id Program, where there is a central government agency, which is responsible for the system coordination, developing standards, policies and for all business processes needed do maintain the system up and working. This agency must be linked to an advisory council, composed of members indicated

by public and private clients of the system, such as ministries, courts, public agencies, banks, and a number of other potential customers (see Figure 2). Studies point to several potential applications of an national eID system both in the public [65] sector as well as in the private sector [66]. The main difference between the proposed model and the existing structure in the Brazilian National eID (RIC) Program is over the role played by the Council. In the RIC program, the Council act as the main decision authority of the system, while the Council in our proposal, acts as an advisory and supervisory board. In the proposed management structure, it is up to the Chief of Staff Presidency to have the leadership role in the proposal. The Chief of Staff was chosen because he or she has a higher authority over the other ministries involved with the system.

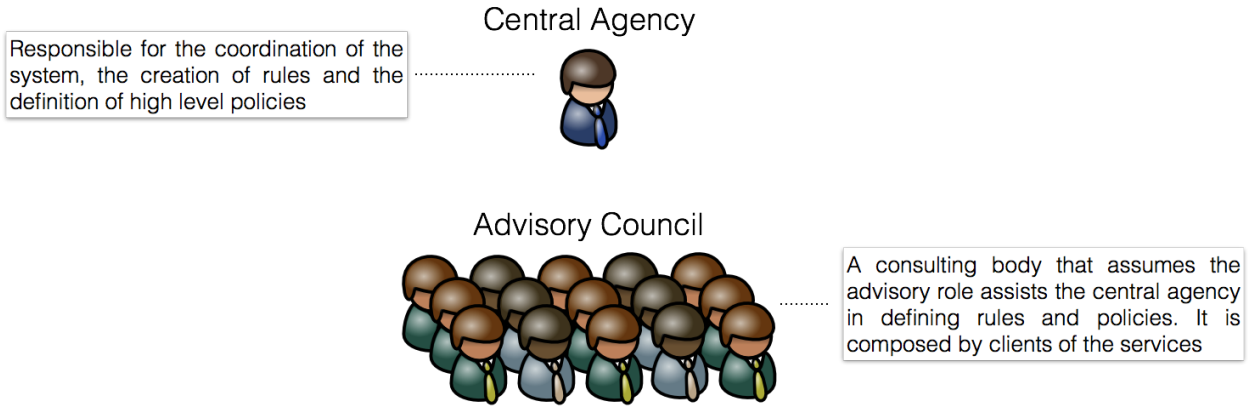


Figure 2: Proposal of Management Structure.

In practice, the lack of power from the Ministry of Justice (the committee leader), in making decisions in the RIC project was reflected in frequent schedule delays and consequently in low efficiency. In two years, the project team responsible for the execution of activities and studies accumulated dozens of reports that could not be carried on because the of huge time necessary to get an approval from the committee.

Similar to this proposal, the strategies adopted in other countries reveled that the IDM structure is often part of the government structure, which is led by a coordinating ministry or agency directly linked to the presidency who heads the system. Although these agencies have a leading role in the strategies management models (Section 3), it is important to highlight that they are assisted by an advisory committee, it is proposed in this paper.

5.2 Brazilian Identity Management System

The federated identity management model presented itself could be the best alternative to the Brazilian IDM system because the States are legally responsible for the citizen enrollment process and for the issuing civil identities. Each State would have identity records related to a part of the population and could act as an Identity Provider in the federation. However, as shown in Section 4.2, the Brazilian states are experiencing budget constraints that prevent them from taking on new financial commitments to develop the needed infrastructure and to hire qualified personal to implement the entire IdM system by themselves. This scenario was confirmed by a diagnosis commissioned by the Ministry of Justice that exposed several structural problems faced by the states to meet the daily demands and to maintain the current infrastructure [62]. The comparison between the costs to create and keep decentralized infrastructures in all 27 States and the costs to provide the same service in a centralized manner indicates that the second option requires less investment.

The analysis of these aspects led us to adopt a centralized identity management model (see Section 2) where the Brazilian Federal Government is the single Identity Provider (IdP). The idea is to take advantage of the current decentralized state registration structure to gather citizen records for the centralized civil database (RIC) as shown in the Figure 3). This database is connected with the electronic identity database (eID) to ensure that each citizen could have just one eID. To remotely authenticate the citizens, the IdP only need few personal data stored in eId database, such as eId number, password, and mobile phone number. Other personal citzen data will be stored in the centralized civil database (RIC). The access to the personal data stored in the civil database (RIC) from eID database would only be allowed with the express permission of the citizen.

It is important to highlight in the proposed strategy that the link between the two database records – eID and RIC – must ensure that each user exist just once in both databases and, because of that, it should have just one civil and electronic identity. The use of an automatic biometric deduplication system (ABIS) is recommended as the main way to ensure that each individual will be enrolled just once. This happens

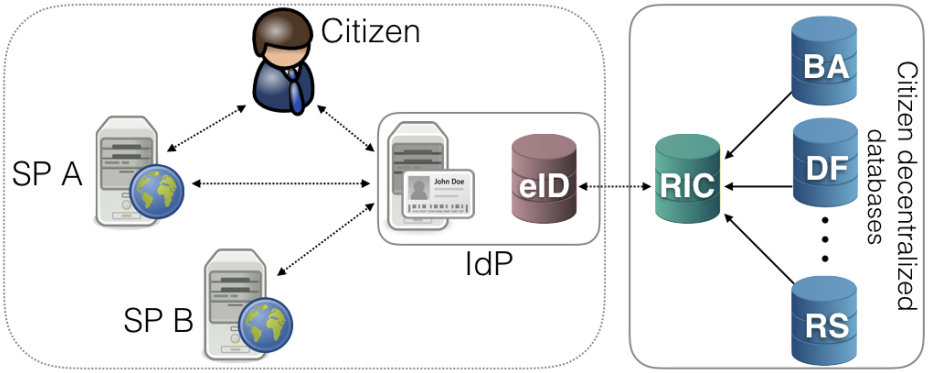


Figure 3: Proposal of a National Identity Management Strategy.

because this kind of systems uses biometric features, that are unique to each person, to check if the user was already registered. Several countries are already using ABIS solutions in the registration of theirs citizens, such as India, Indonesia and Mexico.

A deep study of the main strategies adopted by European countries (user-centric and the centralized models) was essential to base the choice for the model used in our proposal. Two main issues are linked to these models: one related to privacy and the other to fraud prevention. Despite the user-centric strategy appearing as a solution to enhance personal data protection, it is not effective to prevent fraud since it makes it more difficult to link users across different databases. On the other hand, the centralized model is an efficient solution to combat identity fraud since the user data is centrally stored and can be easily linked as it takes the control of the data from the user to the identity provider. Several European countries have adopted an hybrid model in which only the basic personal data is stored centrally and most of the biographic and biometric data are stored in the user's support tool, such as a smart card or a smartphone, for example. As mentioned before, in our proposed strategy, we adopt the centralized model, however, our IdM system has some features to preserve the citizen privacy such as it limits to the collection of personal data, personal data will be not disclosed to SPs without the consent of the individual, and personal data will be protected by security controls against such risks as loss.

A research conducted by the University of Brasilia points out that there are no specific personal data protection laws in Brazil. This subject is treated sparsely in different parts in the Brazilian legislation and court decisions and is rarely treated as a fundamental right [67]. Despite Personal Data Protection being currently discussed within the Ministry of Justice, a draft of a new Law has not been proposed yet [68], probably because a strong movement for personal data protection is not yet present in the Brazilian society, in contrast to what happens in Europe.

As noted in the report [67], in some cases, Privacy-Enhancing Technologies could limit the security. In the German National Identity, for instance, the personal attributes are not stored in the IdPs, which increases the complexity of the revocation process of eIDs. Indeed, the use of a group identification key for on-line authentication, instead of a personal identification key to preserve privacy, weakens security enabling impersonation attacks among each group. Therefore, we propose the adoption of Privacy-Enhancing Technologies that are not Sum-Zero with Security such as the user consent or approval of data disclosure to the SP, the data minimization when checking address or age and the use of restricted identification protocols based on pseudonyms (without personal data disclosure) used in countries such as Italy and Germany. An interesting solution that assures no traceability of user transactions between different SPs is the use of identification numbers which are derived from the combination of the user identification number and the SP identification number.

The choice of the user authentication protocol depends on the security and privacy analysis (logical attacks), such as in the semantic challenge attack reported in the ICAO Active Authentication Protocol (AA). Therefore, the IdM system must use a mutual authentication protocol, where the SP authentication must be performed previously to the user identification, as implemented in the Extended Authentication Protocol (EAC) in order to prevent spoofing attacks.

In regards to interoperability, to allow authentication and authorization assertions exchange between different entities, particularly between IdPs and SPs, the proposed IdM System uses the Security Assertion Markup Language (SAML). This technology has already been included in the Brazilian e-Gov interoperability standards [8] and is adopted as the central element in important eID interoperability programs in Europe, such as STORK (I and II) and FutureID.

Some of the SAML native features are the "persistent identifiers", that are constructed using values that

have no discernible correspondence with the subject's actual identity [69]. Through an attribute combination, it's possible to deliver an exclusive identifier to each service provider avoiding the traceability of the user (such as a pseudonym). In the model adopted by Austria, the SAML standard is used during the identification and authentication processes, assembling the retrieved identity information into a certain format and transferring these data to the corresponding online application [70]. The proposed IdM System will be able to use pseudonyms as specified in SAML V2 standard.

5.3 Authentication Factors and Level of Assurance

The third part of our strategy proposes the adoption of different alternative authentication factors, which may be a possession factor (a Personal Authentication Device-PAD) based on a smart card or a mobile device, with a knowledge factor based on a password.

We propose the use of multiple alternative authentication factors, instead of an expensive all-in-one eID identity card. A Mobile eID, based on smartphones or an EMV chip card[26] running an eID applet can be used to authenticate when a high level of assurance is required. When a low level of assurance suffices, some low-cost authentication factors may be adopted, such as the memorized secret (password[27]) or a one-time-password stored on OTP scratchcards. We decided for the use of OTP scratchcards (Look-up Secret) because, although the benchmarking showed that several countries adopted the use of one time password via SMS messages, a recent draft published by NIST discouraged the Out-of-band authentication using the PSTN (SMS or voice), method that is being considered for removal in future editions of NIST Digital Authentication Guideline.

The levels of assurance of each authentication factor, categorized by the NIST [72] model, are listed on Table 3.

Table 3: Levels of Assurance(LoA) of alternatives low-cost authentication factors.

LoA	**Authentication factors**
2	Username/Password
3	Username/Password + One-Time password
3	Mobile eID with digital certificates
4	EMV chip card with digital certificates

In the proposed strategy, the use of high-end multiple application smartcards in EMV chip cards enables the inclusion of an eID applet, as implemented in countries such as Austria, Estonia and Finland, as an alternative to the issuance of eID identity cards. In Austria, the use of a unique eID applet specified by the Government and compatible with EMV chip cards, health cards, or association cards, improves the availability of the eID, which is crucial to improve the user adoption rate. It is important to highlight that the EMV chip card alternative will be able to provide the multi-factor authentication (PIN and digital certificates).

Apart from memory and processing power requirements, the chip installed in the EMV card must be robust against physical and logical attacks to be used as an eID token. The security may be improved by the use of Memory Management Unit (MMU), which is a true hardware firewall that enhances the security of multi-application smart card operating system and prevents other applets from accessing important chip resources, such as the private key used in the eID authentication protocol. Therefore, some minimal security requirements to the chip must be placed in order to include an eID applet [28].

Recent surveys [43, 73] revealed that the Mobile eID solution has been adopted in many countries, such as Estonia, Finland, United Arab Emirates and Denmark. In this solution, a client application is used in the smartphone and the private key is securely stored in the SIM card. Additionally, a great effort has been coordinated by the Global Platform to standardize the Trusted Execution Environment (TEE), which addresses the security of smartphones operational systems and applications to protect sensitive material, like passwords and cryptographic keys.

Due to high security and ease of implementation, it's observed that the adoption of a secure element (eg SIM card) is common in the Mobile eID solution adopted by other countries [44]. Usually, these Mobile eID solutions require users to acquire enhanced SIM cards that are capable to store safely eID data. On

[26] Defined by EMVCo, EMV Contact is a specification for chip-based contact payment cards and terminals (https://www.emvco.com).

[27] As specified in [71], the password must be a user generated string consisting of 8 or more characters chosen from an alphabet of 90 or more characters. Moreover, the IdP implements dictionary or composition rule to constrain user-generated secrets.

[28] As specified by the NIST [71], the Cryptographic module shall be FIPS 140-2 validated, Level 2 or higher; with physical security at FIPS 140-2 Level 3 or higher.

the other hand, using a secure element, users can rely on features such as create electronic signatures. In addition to the Mobile eID, eID applet and EMV cards may be used to digitally sign documents and store digital certificates.

Currently, the Brazilian public key infrastructure (ICP BRASIL) is described in the Brazilian Legislation through the MP 2200 [74] and regulates high level policies and requirements for a qualified signature. The digital signature and authentication functions are performed trough the same certificate and its associated private key is protected with a PIN code.

However, the use of a single certificate for both features seems to be insecure, since a user can accidentally use the signature function while trying to authenticate a system. This may be the major reason why most of the countries analysed, such as Austria [75, 76], Germany [77, 78], Belgium [79] and Estonia [38], generate two different certificates and their associated private keys, wherein one of the certificates is used to provide authentication and the other, called qualified certificate, provides handwritten equivalent signature. Therefore, we propose the use of distinct certificates and PINs for each function in order to mitigate the risk of misuse of the certificates.

The proposed strategy mimics the model adopted in most analyzed countries, where the authentication certificate is issued by the government authority for all eID tokens without any fee to the user, while the signature certificate is issued by the Certificate Authorities through the Public Key Infrastructure (ICP Brasil) and is optional to the citizen who is willing to pay the issuance fee.

The use eID based on EMV cards and Mobile eIDs allows the enrollment of a great part of the Brazilian citizens, who either owns a smartcard – about 154 million people according to a recent survey [80], or is a bank account holder – about 64% of the citizens according to [81]. Nevertheless, taking into account the equity principle, all citizens must be able to access e-Gov services, therefore the strategy must be designed to include 100% of citizens. Therefore, additional authentication options are proposed: the use of a pair user/password authentication by a centralized Idp and the use of OTPs scratch cards, which combines a possession factor with a knowledge factor.

Since 75% of the current e-Gov services do not require high level of assurance authentication, the use of a pair user-password or OTP should be implemented prior to the other authentication methods to readily enable the access to the services. The adoption of additional authentication methods based on Mobile eID and EMV cards, with higher level of assurance, enables access to 40% of e-Gov services, which today are only offered by off-line/in-person identification, and in turn, will allow the achievement of higher stages of maturity (transactional or connected web) [54].

By the proposed IdM strategy, Brazilian e-Gov services may be categorized according to the required level of assurance, which will define the possible authentication methods. For instance, to request a non-critical information, a simple remote authentication performed over the network with the use of a pair user/password and assured by a secure protocol (that allows an authentication that is resistant to guessing, replay, session hijacking and eavesdropping attacks and at least flimsy resistant to man-in-the middle attacks) is enough. In contrast, to access income tax declaration services, a higher level of assurance authentication factor must be used, such as a joint of two authentication factors, like password and OTP, a Mobile eID or an eID applet running in an EMV card, which may also be used to access lower level services.

Finally, it is important to highlight that the LOA scheme for categorizing the variety of authentication methods that can be used in the proposed IdM system (identity assurance information) can be expressed in SAML assertions as defined by the OASIS in the SAML Identity Assurance Profiles [82].

5.4 A Low-cost and Robust Identity Document Model

As observed on Section 3, national eIDs are usually created under the same rules of previous national identity documents. In Brazil, we also have to consider the cultural use of a national identity document as a proof for in-person identification.

Therefore, the IdM Strategy for a new Brazilian identity document model, combining as many authentication factors as possible, must be designed to be a robust national identity document to avoid frauds, since it is still used as a possession factor for in-person identification for enrollment or renewal of social benefits.

Although almost all European national identity eID cards are based on multi-application smartcards with eID applets, a very low adoption rate of eID functions to access e-Gov services has been observed in countries such as Germany and Spain [83]. Some European countries charge fees to issue eID cards from their citizens. In Brazil, the issuance of the very first identity document is free of charge by law, thus the high cost of high-end eID cards may be improbable and the benefits are still questionable if we consider the expected adoption rate. For instance, in 2010 a contactless multi-application eID card had a unit cost of 40 R$, under a pilot project. The issuance of this eID card for all Brazilian citizens would cost more than 8 billion reais.

Recently, the cost of eID cards seems to be slightly lowering due to the expansion of smartcard resources. Thus, we expect that in future, eID cards will be adopted all around the world. Nevertheless, in order to optimize the cost/benefit ratio and if we consider the current adoption rates, we propose the initial issuance of a low cost chipless identity document which would still be robust against counterfeit and also enable a strong in-person authentication.

An alternative lowcost and robust identity document model is proposed on [83], and depicted in Figure 4. The chipless model was chosen to limit the estimated cost under one real. The use of a binary robust hashing of printed face image is proposed to avoid a typical impersonation fraud made by face image substitution. A 2D-barcode stores a compact digital signature of biographical data printed on Machine Readable Data (MRZ) and on robust hashing. The 2D-barcode read (BCR) must be designed to be compatible with typical smartphone cameras, so that a public application can be used to verify the signature. This feature avoids the use of expensive security elements, such as holograms. A biometric authentication factor is proposed with the use of a protected biometric template stored in a 2D-barcode. The use of an invisible ink is proposed solely because ICAO standard forbids the use of visible barcodes on front page. The biometric verification is performed on the reader. Therefore, to avoid the theft of the biometric template, this would be used only in public sector services with certified readers. More details are given in [83].

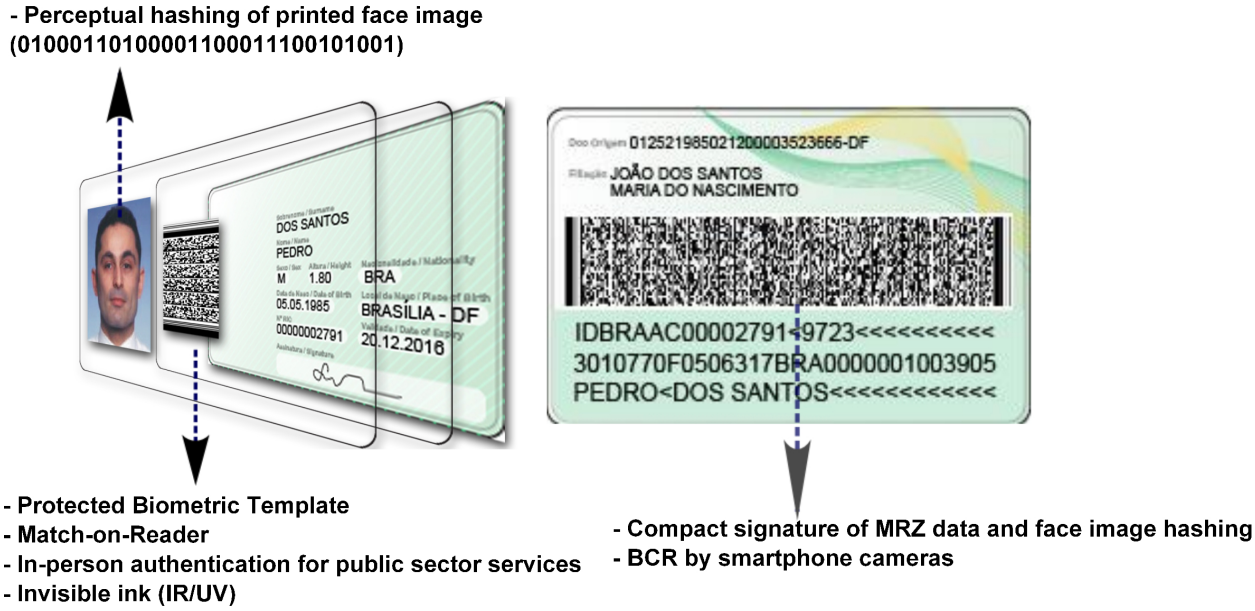


Figure 4: An alternative robust and lowcost identity document model

5.5 Final Remarks

The benchmarking of countries strategies showed that most of these countries use smartcards as a support tool for electronic identity. However, it has been observed that the high cost associated with the production of these cards does not always bring the benefits expected by governments. A study conducted by [83] shows that in several of the major European countries, such as Germany and Spain, the use of the electronic identity as authentication method in transactions with government are very low and sometimes, less than 10% of the cards issued are used with this purpose.

The impact of the high cost to issue these cards does not seem to be a problem for many European governments since the cost of production is passed on to the citizens through an issuance fee. However, the Brazilian Law explicitly prohibits the government to charge its citizens to issue the identification card. Considering the budget proposed by the Brazilian Ministry of Justice in 2010, the total cost to issue cards to all Brazilians would exceed 3,6 billion of dollars. This high issuance cost for smart cards by the government and the high risk of poor adherence by its population were two of the main reasons in our proposal to choose an alternative and low cost authentication method to replace the use of eIDS as the official smart card.

6 Conclusion

Brazilian e-Gov program holds the 57^{th} position in the UN ranking [7] and this situation is due to the low maturity levels of e-Gov services in the country. The absence of a national strategy for e-Gov identity

management is one of the main obstacles to achieve the high levels of the model proposed by the UN.

This paper described a proposal for a national strategy for identity management to boost Brazilian e-Gov services to higher levels on the UN's maturity model, that is, transactional and connected web. To design this proposal, a study was conducted on national strategies adopted in European countries who excelled at e-Gov services and on two major projects for electronic identity interoperability, Stork2 and FutureID. In their initiatives for the introduction of electronic identities in public services and the corresponding identity management systems, many European countries confronted the central problem regarding globalization, since the systems of electronic identity and identity management in each country are not compatible with each other, i.e., they are not prepared to interoperate. In our proposed strategy, we seek to leave Brazil prepared locally but also for the immediate future and its integration with the rest of Latin America and the world, whether in treaties such as the MERCOSUR or the Pacific Alliance. This was the motivation to consider Stork2 and FutureID in our survey.

We also carried out a diagnosis on the Brazilian reality, in order to overcome deficiencies and to explore opportunities so that the proposed strategy really meets Brazil's specific requirements. Therefore, the proposed strategy combines solutions adopted by other countries and makes use of a low-cost identity document, which is a novel contribution. Factors such as the total cost of ownership, the current information technology infrastructure of Brazilian States, the need to combat identity fraud, the adoption of electronic identity by 100% of the population, the design privacy and interoperability between identity management systems. were considered.

The national strategy described in this paper presents a management framework for the Brazilian eID system, a centralized IdM model and an eID solution that does not rely on smart card. Nevertheless, it provides support for different types of electronic authentication. As future work, we recommend the definition of a technological architecture for the development as well as the deployment of a concept proof of this proposed strategy.

References

[1] W. J. McIver Jr and A. K. Elmagarmid, *Advances in digital government: Technology, human factors, and policy*. Springer Science & Business Media, 2002, vol. 26.

[2] Z. Fang, "E-government in digital era: concept, practice, and development," *International journal of the Computer, the Internet and management*, vol. 10, no. 2, pp. 1–22, 2002.

[3] L. Carter and F. Bélanger, "The utilization of e-government services: citizen trust, innovation and acceptance factors," *Information systems journal*, vol. 15, no. 1, pp. 5–25, 2005.

[4] OECD, "National strategies and policies for digital identity management in OECD countries," *OECD Digital Economy Papers*, no. 177, 2011.

[5] "e-Government Survey 2010: Levering e-government at a time of financial and economic crisis," Economy & Social Affairs, United Nations, 2010.

[6] "NGN identity management framework," Recommendation Y.2720, ITU, 2009.

[7] "e-Government Survey: E-Government for the Future We Want," Economy & Social Affairs, United Nations, 2014.

[8] BRASIL, "e-PING Padrões de Interoperabilidade de Governo Eletrônico," Comitê Executivo de Governo Eletrônico, Tech. Rep., 2014, http://goo.gl/PsV0UT.

[9] J. A. S. Torres, H. P. Peixoto, F. E. G. de Deus, and R. T. de Sousa Júnior, "An Analysis of the Brazilian Challenges to Advance in e-Government," *The 15th European Conference on eGovernment*, 2015.

[10] S. Claußand M. Köhntopp, "Identity Management and Its Support of Multilateral Security," *Comput. Netw.*, vol. 37, no. 2, pp. 205–219, Aug. 2001, http://dx.doi.org/10.1016/S1389-1286(01)00217-1.

[11] A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer, "User centricity: a taxonomy and open issues," *Journal of Computer Security*, vol. 15, no. 5, pp. 493–527, 2007.

[12] " E-Authentication Guidance for Federal agencies," OMB Memorandum M-04-04, United States, Dec 2003, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

[13] A. Jøsang and S. Pope, "User Centric Identity Management," in *AusCERT Asia Pacific Information Technology Security Conference 2005*, Maio 2005.

[14] M. S. Wangham, E. R. de Mello, D. da Silva Böger, M. Gueiros, and J. da Silva Fraga, *Minicursos X Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*. Sociedade Brasileira de Computação, 2010, ch. Gerenciamento de Identidades Federadas, pp. 1–52.

[15] J. Camenisch and B. Pfitzmann, "Federated identity management," in *Security, Privacy, and Trust in Modern Data Management*. Springer, 2007, pp. 213–238.

[16] D. W. Chadwick, *Federated Identity Management*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 96–120, http://dx.doi.org/10.1007/978-3-642-03829-7_3.

[17] OASIS, *Security Assertion Markup Language (SAML) 2.0 Technical Overview*, june 2005.

[18] STORK, "Final Version of Technical Specifications for the cross-border interface," 2015, https://goo.gl/K4jocq.

[19] ——, "Stork - What is it?" 2015, https://goo.gl/sPZPZc.

[20] NIST, "Electronic authentication guideline," *NIST Special Publication 800-63-2*, 2013, http://dx.doi.org/10.6028/NIST.SP.800-63-2.

[21] G.-J. Ahn and J. Lam, "Managing privacy preferences for federated identity management," in *Proceedings of the 2005 workshop on Digital identity management*. ACM, 2005, pp. 28–36.

[22] M. Hansen, A. Schwartz, and A. Cooper, "Privacy and Identity Management," *Security Privacy, IEEE*, vol. 6, no. 2, pp. 38 –45, mar. 2008.

[23] R. Gelman, "Fair Information Practices: A Basic History. Version 2.12," 2014, http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[24] "The OECD Privacy Framework," OECD Publishing, OECD, 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[25] "Digital Identity Management: Enabling Innovation and Trust in the Internet Economy," OECD, 2011.

[26] G. M. Verzeletti, M. S. Wangham, E. R. de Mello, and J. A. S. Torres, "Um Estudo Comparativo de Estratégias Nacionais de Gestão de Identidades para Governo Eletrônico," in *IV WGID - Workshop de Gestão de Identidades – XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg*, 2014.

[27] I. Naumann and G. Hogben, "Privacy features of European eID card specifications," *Network Security*, vol. 2008, no. 8, pp. 9–13, 2008.

[28] "eID Interoperability for PEGS: Update of Country Profiles study - Italian country profile," IDABC European eGovernment Services, European Communities, ago 2009.

[29] "eGovernment in Germany," eGovernment Factsheets, European Comission, Jan 2015.

[30] "eGovernment in France," eGovernment Factsheets, European Comission, mai 2014.

[31] F. Piliu, "Les faux documents sont des Sésames qui ouvrent beaucoup de portes," 2016, http://goo.gl/c20Ury.

[32] D. Batido, "Progrès des ID Cards," 2015, http://goo.gl/ntcLse.

[33] "When eID becomes Mobile for a whole nation," Gemalto, 2015, http://www.gemalto.com/brochures/download/gov_cs_finland_valimo.pdf.

[34] T. Rissanen, "Electronic identity in Finland: ID cards vs. bank IDs," *Identity in the Information Society*, vol. 3, no. 1, pp. 175–194, 2010.

[35] "eGovernment in Finland," eGovernment Factsheets, European Comission, jan 2015.

[36] "eGovernment in the Spain," eGovernment Factsheets, European Comission, Fev 2014.

[37] A. Heichlinger and P. Gallego, "A new e-ID card and online authentication in Spain," *Identity in the Information Society*, vol. 3, no. 1, pp. 43–64, 2010.

[38] "The Estonian ID Card and Digital Signature Concept - Principles and Solutions," ESTONIA, 2003, http://goo.gl/1VWesM.

[39] "eGovernment in the Estonia," eGovernment Factsheets, European Comission, Apr 2014.

[40] V. Valimiskomisjon, "Statistics about Internet Voting in Estonia," 2015, http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics.

[41] "The Austrian Citizen Card System," Bürgerkarte, 2015, https://www.buergerkarte.at.

[42] E. Communities, "eID Interoperability for PEGS: Update of Country Profiles study - Austrian country profile," IDABC European eGovernment Services, jul 2009.

[43] "National Mobile ID schemes - Learning from today's best practices," Gemalto, 2014, http://goo.gl/RvIWfK.

[44] T. Zefferer and P. Teufl, "Leveraging the Adoption of Mobile eID and e-Signature Solutions in Europe," in *Electronic Government and the Information Systems Perspective*. Springer, 2015, pp. 86–100.

[45] "eID Interoperability for PEGS: Update of Country Profiles study - Estonian country profile," IDABC European eGovernment Services, European Communities, jul 2009.

[46] "eGovernment in the Austrian," eGovernment Factsheets, European Comission, Apr 2014.

[47] "Orden PRE/1838/2014," Ministerio de la Presidencia, 2014, http://www.boe.es/boe/dias/2014/10/09/pdfs/BOE-A-2014-10264.pdf.

[48] "eGovernment in the Denmark," eGovernment Factsheets, European Comission, Jun 2014.

[49] N. Merrett, "Verizon joins GOV.UK Verify accredited suppliers list," 2015, http://goo.gl/zvucZy.

[50] OASIS, *Electronic Identity Credential Trust Elevation Framework Version 1.0*, maio 2014.

[51] J. A. S. Torres, "Um estudo sobre projetos de interoperabilidade para identidades eletrônicas," Monografia de Pós Graduação em Governança de TI. Universidade Católica de Brasília, Brasília, 2014.

[52] B. Zwattendorfer and D. Slamanig, "On privacy-preserving ways to porting the Austrian eID system to the public cloud," in *Security and Privacy Protection in Information Processing Systems*. Springer, 2013, pp. 300–314.

[53] "e-Government Survey 2012: E-Government for the People," Economy & Social Affairs, United Nations, 2012.

[54] J. A. S. Torres, F. E. G. de Deus, and R. T. de Sousa Júnior, "Diagnóstico do governo eletrônico brasileiro – Uma análise com base no modelo de gerenciamento de identidades e no novo guia de serviços," in *IV WGID - Workshop de Gestão de Identidades – XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg*, 2014.

[55] D. Amora, "TCU aponta risco de fraude bilionária no INSS," 2014, http://auditar.org.br/web/?h_pg=noticias&bin=read&id=1519.

[56] "Janeiro registra mais de 150 mil tentativas de fraude, aponta Serasa," Serasa, 2016, http://goo.gl/wNtDN5.

[57] "PL 1775 - Dispõe sobre o Registro Civil Nacional - RCN e dá outras providências," Congresso Nacional, 2015, http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1301476.

[58] "Comunicado de la II Reunion de Ministros y IV de Autoridades de Gobierno Eletónico de América Latina Y el CAribe," Red Gealc, Nov 2012.

[59] "Na falta de Registro Nacional, quatro estados criam sistema de RG integrado," Deutsche Welle Brasil, 2014, http://goo.gl/pK5MYk.

[60] "Ata da 62ª Reunião Ordinária do Conselho Gestor do Programa Estadual de Parcerias Público-Privadas, instituído por força da Lei Estadual nº 11.688, de 19-05-2004," Diário Oficial do Poder Executivo de São Paulo., São Paulo, Jan 2014.

[61] "Cartão para facilitar serviços no ES entra em fase experimental," G1 ES, 2014, http://goo.gl/RF2PXh.

[62] "RT RIC – Diagnóstico da Identificação Civil no Brasil," Ministério da Justiça, 2014.

[63] "RT RIC – Custos econômicos e sociais de falhas nos sistemas de identificação individual," Ministério da Justiça, 2014.

[64] "RT RIC – Impactos sociais das falhas de identificação," Ministério da Justiça, 2015.

[65] "RT RIC – Levantamento de potenciais aplicações governamentais para o RIC," Ministério da Justiça, 2015.

[66] "RT RIC – Levantamento de potenciais aplicações privadas para o RIC," Ministério da Justiça, 2015.

[67] "RT RIC – Levantamento da legislacao aplicada ao acesso a dados pessoais," Ministério da Justiça, 2015.

[68] "Anteprojeto de Lei para a Proteção de Dados Pessoais," Ministério da Justiça, 2015, http://goo.gl/NyCDAl.

[69] OASIS, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 – Errata Composite*, september 2015.

[70] B. Zwattendorfer, A. Tauber, and T. Zefferer, "A privacy-preserving eID based Single Sign-On solution," in *Network and System Security (NSS), 2011 5th International Conference on.* IEEE, 2011, pp. 295–299.

[71] NIST, "Digital Authentication Guideline," *DRAFT NIST Special Publication 800-63*, 2016, https://pages.nist.gov/800-63-3/sp800-63b.html.

[72] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "Electronic Authentication Guideline, NIST Special Publication 800-63-2," 2013, http://goo.gl/QdBV5d.

[73] "Estonia's Mobile-ID: Driving Today's e-Services Economy," GSMA, 2013, http://goo.gl/UIT7cN.

[74] BRASIL, "Medida Provisória nº 2.200-2, de 24 de agostos de 2001," 2001, https://goo.gl/eQgZEX.

[75] B. Zwattendorfer, A. Tauber, and T. Zefferer, "A privacy-preserving eID based Single Sign-On solution," in *NSS'11*, 2011, pp. 295–299.

[76] H. Leitold, A. Hollosi, and R. Posch, "Security architecture of the Austrian citizen card concept," in *Computer Security Applications Conference, 2002. Proceedings. 18th Annual.* IEEE, 2002, pp. 391–400.

[77] Ö. Dagdelen, "The Cryptographic Security of the German Electronic Identity Card," 2013.

[78] M. Horsch and M. Stopczynski, "The German eCard-Strategy," Technical Report: TI-11/01, TU Darmstadt, http://www. cdc. informatik. tudarmstadt. de/reports/reports/the_german_ecard-strategy. pdf, Tech. Rep., 2011.

[79] D. De Cock, C. Wolf, and B. Preneel, "The Belgian Electronic Identity Card (Overview)," in *Sicherheit*, vol. 77, 2006, pp. 298–301.

[80] "Número de smartphones supera o de computadores no Brasil," Revista Exame, 2015, http://goo.gl/AZywWy.

[81] "População brasileira com conta bancária soma 86,3 milhões de pessoas," Agência Brasil, 2015, http://goo.gl/pWwgYN.

[82] OASIS, *SAML V2.0 Identity Assurance Profiles Version 1.0*, November 2010.

[83] R. G. F. Távora, J. A. S. Torres, and D. F. R. Fustinoni, "Proposta de um modelo de documento de identidade robusto a fraudes e de baixo custo," in *V WGID - Workshop de Gestão de Identidades – XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg*, 2015.