eID Interoperability for PEGS

NATIONAL PROFILE SPAIN

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in Spanish eGovernment applications.

Table of Contents

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Introduction

3.1 General Status and Most Significant eIDM Systems

The most important of the existing eIDM systems in Spain is the "DNI electrónico" or "DNI-e" (electronic national identity card, hereinafter eID card) that includes technological innovations in the eID card in order to increase the document's security as well as its application field.

The eID card allows electronic authentication of the identity of a person in an irrefutable manner, and allows the bearer to eSign documents, granting them a legal validity identical to the one provided by the handwritten signature.[3]

The "Documento Nacional de Identidad", commonly known as "DNI" (Spanish Identity Card, hereinafter ID card), is the document that verifies the identity, the personal data that appears on it and the Spanish nationality of its bearer.

Most part of the data that appear in the ID card (whether electronic or not) is evidenced in the Civil Registry (at the Ministry of Justice), where the facts concerning persons civil status are inscribed.

The most important data appearing in the ID card is the personal number that is assigned by the Police General Directorate. This number is evidenced in other documents granted by the Administration such as the passport or the driving licence.

The ID card number must be presented in any request, registration or precise document for public or private actions whenever it is necessary to provide evidence of the personal identity of the interested party.

Apart from the eID card, there is also a broadly used system of PKI certificates issued by 11 commercial CSPs (both public and private), which can be used in a large number of eGovernment applications for authentication services. The interoperability between these certificates (56 types issued by the 11 CSPs) is guaranteed through the MAP multiPKI Validation Platform (called Platform @firma v.5.0.).

Both the eID card and the commercial CSP certificates will be discussed in greater detail below.

On the other hand, information concerning companies appears in the Companies Registry, where the actions relating to individual entrepreneurs and legal corporations are inscribed with the purpose of publishing them so that they may be known by the persons contracting with them. Legal entities can

[3] See www.dnielectronico.es

also authenticate themselves electronically, as certain commercial CSPs issue certificates specifically to legal entities, rather than natural persons.

3.2 Background and Traditional Identity Resources

3.2.1 eGovernment Structure[4]

Spain is today a regional state, and therefore the eGovernment structure at State level is very different to the one at the regional level, where the 17 Spanish autonomous communities (regions) have their own Government and therefore their own and different level and speed of development, implementation and extent of the eGovernment applications.

As in other countries, in every level strong efforts are made in the field of electronic information sharing, which is combined with the so called "unique counter" (*ventanilla única*), so that in the near future all citizens will be able to handle their paperwork at any official Registry (state/regional/local) and without needing to present any document that any Administrative body has already registered in its electronic databases, as all Administration bodies will share information (e.g. the case of the renewal of working authorisations, where the Social Security certifications are no more required, as civil servants working at the Immigration Directorate have direct access to the Social Security database).

eGovernment, in particular horizontal integration, is driven by the following services:

3.2.1.1 State eGovernment

EGovernment initiatives and applications are developed independently in every Ministry, and it is the Public Administrations Ministry – MAP – the one that generally coordinates all applications at state level. Full information is given at www.060.es, recently created, with all on-line services provided by the State Administration, by using or not electronic certificate.

The use of the eID card is horizontally coordinated by the Oficina Técnica del DNI electrónico (eID card Technical Office), which gives detailed information at www.dnielectronico.es.

[4] Information extracted from the report "European eGovernment Services (IDABC)" that has been confronted, updated and, in its case, adapted to the needs and requirements of this report.

3.2.1.2 Regional Government

Regional eGovernment initiatives using electronic authentication systems are lead and coordinated by the respective regional Administrations, where a specific body, department or entity is usually in charge of its coordination. In some cases the information about eGovernment is split and not available at the competent Department web page; in some others, there is a specific link on the homepage dedicated to eGovernment or to online operational transactions.

It is important to note here, in order to facilitate a proper comparison with other Member States, that management of specific matters such as education or health have been transferred to the Spanish Regions and only residual competences are kept by the State Government.

3.2.1.3 Local eGovernment

Local eGovernment initiatives are lead and coordinated by local authorities, mostly municipalities.

Most of the Spanish Regions are developing testing projects of "*Ciudades Digitales*" (Digital Cities) in order to fully transform their Local Governments so as to permit the citizens to have access to all public services by using the municipalities web pages, with different sections addressed to citizens (A2C), enterprises (A2B) and public officers (A2A) by means of their intranet.

These projects are led by the Ministry of Industry, Tourism and Commerce under the "*Programa de Ciudades Digitales*" (Digital Cities Programme) available at http://www.mityc.es/ciudades/ and co-financed by this Ministry, together with the Spanish Regions and the European Fund of Regional Development. This program addresses medium-sized Spanish cities and is focused on several areas including eGovernment. Now the city of Cuenca (in the Region of Castilla La Mancha) has been chosen to test A2C services by using eSignatures and the eID card.

Other than this, several of the larger Spanish cities have already implemented their own electronic authentication applications (e.g. Madrid, Barcelona, Valencia and Bilbao), and they are permanently working in order to extend their online transactions, which currently pertain mostly to the payment of local taxes, standing orders or obtaining certificates from the census Registry.

In general, these systems rely on authentication mechanisms offered at state level, by FNMT-CERES (Fabrica Nacional de Moneda y Timbre: the Royal Spanish Mint) or the eSignature issued by any of the regional official certification authorities in the case of Cataluña, Valencia and País Vasco.

3.2.2 National eGovernment Cooperation and Coordination[5]

In Spain, the Ministry of Public Administration (hereinafter, MAP) www.map.es is the instance in charge of general eGovernment cooperation and coordination.

In fact, for the period of 2006-2008 the MAP has approved the "*Plan de Medidas 2006-2008 para la mejora de la Administración*" (Measures Plan to improve the Administration), with different initiatives to modernise the Spanish Administration according to the citizens' needs. It contains 16 measures of different nature that will be progressively approved and implemented in the following two years. Among the legislative initiatives the draft of an Electronic Administration Law is foreseen.

The MAP also works to improve A2C services, and those A2A services that, thanks to the internal modernisation of all Government Delegations located in all Spanish Regions will permit the Administration to guarantee the accessibility of their A2C services by simplifying the processes and administrative proceedings. These actions are included in the Plan "MAP en RED" (connected MAP).

Regarding the support given to municipalities, reinforcing the particular actions managed from the regional Administrations, the MAP has several projects of administrative modernisation at the Local Administrations (eModel) consisting of a line of subsidies with which the MAP will co-finance (with a maximum representing a 50% of the execution) local projects aiming to modernize Local Administrations by using Information Technologies for the improvement of A2C services, proceedings simplifications and improvement of technological infrastructures and communications.

Inside the MAP it is the "*Consejo Superior de Administración Electrónica*" (Higher Council on eGovernment – hereinafter the High Council), which is the organ in charge of the preparation, elaboration, development and application of the Government politic and strategy regarding the information technologies, as well as the boost and implementation of the eGovernment within the State General Administration. In fact, this Higher Council takes care, among others, of Computer cooperation among Administrations and entities, Telecommunications use in the Administration, Security Policy and Applications for the powers execution and Improvement on quality and productivity in the information services development.

The first of these functions implies the improvement of collaboration and cooperation with the Spanish Regions and municipalities, especially for the activation of inter-administrative public services. Therefore, its plenary organ maintains relations with the emerging organs in charge of cooperation among the different administrations. It will also be responsible for the support of cooperation activities of the State Administration before E.U. international organisations, and also with Latin America in the context of information technologies and eAdministration, in collaboration with the Ministry of Foreign Affairs and Cooperation.

This Higher Council also participates in the Sector Committee of eGovernment (*Comité Sectorial de Administración Electrónica*), which is the technical organ in charge of cooperation among the three

[5] Information extracted from the Report "European eGovernment Services (IDABC)" that has been compared, updated and, in its case, adapted to the needs and requirements of this report.

levels of the Spanish Administration, state, regional and local, concerning eGovernment. Among others, this Committee seeks to harmonize the use of eSignatures, to guarantee its interoperability and to improvement the validation of certificates and eSignatures actually rendered by the MAP's validation platform, known as @firma.

The Sector Committee has also launched the Observatory on eGovernment, where all Regions participate, trying to follow the advances of all Regions towards eGovernment, to have updated information about all of them on this matter, and to launch recommendations aiming to accelerate their internal modernisation and to balance their development.

The Higher Council also participates in several international activities such as the IDABC Programme in order to guarantee interoperability of Pan European services of eGovernment, interoperability and mutual recognition of the different national digital identities and eSignatures, the i2010 Action Plan and several international groups on this matter.

3.2.3 Traditional Identity Resources

3.2.3.1 Spanish nationals: the non-electronic ID card – DNI (*documento nacional de identidad*)

Organic Law 1/1992 of February 21 on Citizen Security Protection regulates the issuance of the National Identity Card (commonly known in Spain as DNI, and also referred here as ID card).

The ID card is a personal and non-transferable document, and its bearer is obliged to its custody and conservation; it has sufficient value of its own to attest to the identity and personal data of the bearer that appears on it, as well as his Spanish nationality.

Its procurement is compulsory for Spanish persons above fourteen who are resident in Spain or who, living abroad, come to Spain for a period of more than six months. The cost charged to the citizens is either 6.70 EUR or 12.10 EUR, depending on the circumstances of issuing[6].

It remains valid for a period of five or ten years, or indefinite, depending on the age of the person who requests its issuance or renewal.

The identity card contains a number of data printed on it, specifically: photograph and signature of the bearer, name(s)[7], and surnames[8], date of birth, gender, nationality, personal number (national register

[6] E.g. a citizen pays 6.70 EUR at first issuance or for replacement of an expired card; whereas 12.10 EUR is charged when a valid card is lost or stolen.

[7] Specifically, one or two names.

number)[9] and verification character corresponding to the Identification Tax Number[10]. On the back side, it contains the place of birth, province-nation, parents' name, residence, place of residence, province, and nation in OCR-B letters for mechanical reading. Lastly, there is evidence of the expiration date and the card number.

The national register number is a unique identification number for Spanish citizens, assigned to all Spanish citizens in their national identity cards, and also appearing on the eID card and its microchip (see below). In Spain the National Police is the public body in charge of issuing such identity cards.

To request the ID card, the physical presence of the interested person is required, as well as the presentation of a literal birth certificate granted by the corresponding Civil Registry.

Birth is very important in the Spanish legal system because it determines the beginning of the personality. As proof of birth, births are registered in the Civil Registry that verifies the fact, time and place and the lineage. Once the inscription has taken place, the proof of birth can be provided through literal certificates or through extracts issued by the Judge in charge of Civil Registries[11].

The inscription takes place in the Civil Registry Office corresponding to the place where the birth took place. If requested by the parents, the inscription may be managed in the Civil Registry Office of their domicile, if it is different from the place of birth.

The Civil Registry Office is a file depending on the Ministry of Justice wherein the facts concerning the civil status of persons are inscribed. The following facts are inscribed: birth, filiation, name and surnames and any changes of these, the emancipation and adulthood age, the judicial modifications of the persons' capacity or that the latter have been declared insolvent, in bankruptcy or suspension of payments, declarations of absence or death, nationality and neighbourhood, parental rights and duties, guardianship and other legal representations, marriage and death.

---

[8] The father's first surname followed by the mother's first surname

[9] Each ID card is assigned a personal number that will serve as general *personal numerical identifier*.

[10] The Tax Administration assigns a letter to each contributor which, together with the personal number, conforms the Tax Identity Number, a number that must be consigned in all returns and communications that are presented or maintained with the Tax Administration.

[11] The Civil Registry Office is regulated in the Law of June 8, 1957, in Decree of November 14, 1958 wherein the Ruling of the Law on Civil Registries is approved, and in Royal Decree 644/1990 of May 18 on the rules regarding the Central Civil Registry Office.

3.2.3.2 Non-nationals with legal residence in Spain: NIE (número de identificación de extranjeros)

Foreigners in the situation of legal residence in Spain are identified by a resident card called "*Número de Identificación de Extranjeros*", commonly known as "NIE"[12].

The NIE card[13] is personal and non-transferable and attests to the legal residence of foreigners in Spain, their identity and that they have been granted the corresponding authorisation or the recognised right to stay in Spanish territory for more than three months.

For its issuance a prior government resolution is necessary granting the corresponding administrative authorisation or, depending on the case, recognising the foreigner's right to stay in Spanish territory. An exception is made for E.U. nationals, as no previous administrative resolution is required for them when they apply for their resident card.

There is also a Central Registry of Foreigners that depends on the Police General Directorate, where residence permits granted to foreigners are inscribed[14].

The resident card has a period of validity identical to the one granted by the residence authorisation or the resolution recognising the right that justifies its issuance.

Foreigners staying in Spanish territory have the right and the obligation to keep the documentation that verifies their identity, issued by the competent authorities of their country of origin or the country where they come from.

At present, all foreign citizens holders of a NIE can obtain a Spanish eID card as authentication means in order to make on-line transactions with the Spanish Administration. The foreigners identity card requires prior identification before the Certification Service Provider that issues the qualified certificates (so called "*certificado reconocido*"), as the principal and safest authentication means in Spain, based on a PKI solution. Such electronic certificates have the same legal validity and technical characteristic as the ones issued to Spanish nationals by any of the Certification Service Providers authorised by the Ministry of Industry, Tourism and Commerce.

---

[12] Information obtained at www.mir.es.

[13] Organic Law 4/2000 of January 11 on the rights and liberties of foreigners in Spain and their social integration, modified by Organic Law 8/2000 of December 22 and Royal Decree 864/2001 of July 20, whereby the Ruling for the execution of Organic Law 4/2000 of January 11 is approved, on rights and liberties of foreigners in Spain and their social integration, modified by Organic Law 8/2000 of December 22.

[14] Article 60 of Royal Decree 864/2001 lists the actions that may be inscribed in the Foreign Registry Office.

The Spanish Government is now willing to provide all resident foreigners in Spain with a similar document to the electronic DNI (Spanish eID card), also based on PKI solutions, on smart cards. The introduction of this document, known as "NIE electrónico" or "NIE-e" (electronic Foreigners Identity Card) will allow its bearers to automatically obtain an electronic authentication mean with electronic signature (the same as the DNI-e for Spanish nationals).

3.2.3.3 Entrepreneurs / Corporations

In Spain, the incorporation of companies requires the granting of a public writ before a Notary, which determines the moment of its incorporation and therefore, its capacity to legally operate in trade.

After the incorporation, its inscription in the Companies Registry is mandatory after having paid the respective taxes and after obtaining the Identification Tax Number (called "*Código de Identificación Fiscal*", commonly known as "CIF", similar to the VAT no.), with identifying nature[15].

The purpose of the Companies Registry[16] is to obtain full security and transparency in mercantile business, so that it is possible to know the legal situation of entrepreneurs, without information about other circumstances that are not directly related with the entrepreneurs as operators in the mercantile business.

In this file both individual entrepreneurs[17] and organised corporations are inscribed. It is a public registrar and therefore, it may be consulted by citizens interested in any information relating to the situation of a company (its partners, managers or legal representatives, bylaws, etc.) or individual entrepreneurs.

Concerning individual entrepreneurs, basically the entrepreneur's identity and his company and the general powers granted to specific persons to act on behalf of the company are inscribed, as well as their modification, annulment and substitution. There are other details regarding transactions which can also be inscribed[18].

In the case of companies[19], its incorporation, designation and termination of administrators/managers, liquidators and auditors, general powers and delegation of faculties must be inscribed, as well as their modification, revocation and substitution.

---

[15] Royal Decree 1041/90 of Declarations on census of entrepreneurs and professionals of July 27,

[16] Royal Decree 1784/1996 of July 19, wherein the Rules for Companies Registries are approved.

[17] The inscription of natural persons in this Registry is due to their condition of businessmen or entrepreneurs.

[18] See Article 87 of the Ruling of Companies Registry

[19] Information obtained at www.dnielectronico.es.

3.3 eIDM Framework

3.3.1 Main eGovernment Policies regarding eIDM[20]

3.3.1.1 The national eID card

Although it is still too early to say, the introduction in Spain of the eID card is aimed at providing the necessary impulse to bring electronic authentication and electronic signatures into the mainstream of the eGovernment services. It is intended to be a key enabler for electronic authentication, next to the use of commercial PKI certificates, as outlined below.

The implementation of the national eID card commenced at Burgos (Castilla-Leon Region) in March, 2006.

In mid March 2007, over 370.000 eID cards had already been issued, in its gradual implementation, in 38 cities belonging to 22 Spanish provinces. Presently, the new document has been implemented gradually in over 47 issuing offices of the National Police Corps.

The implementation of the remaining provinces shall be done progressively so that, at the end of 2007, issuing of the national eID card shall have begun in all of the Spanish territory. By the end of 2008, it is estimated that about 8,000,000 eID cards shall have been issued.

The main innovation of the eID card is that it includes a small integrated circuit (chip), capable to securely save information and to process it internally.

In order to incorporate this chip, the ID card changes its traditional support (plastified cardboard) to a plastic material card that has new and better security measures. The support card of the eID is made of polycarbonate, a resistant material of high quality and durability that allows the printing of data with destructive laser, in order to make it impossible to falsify the impression.

In the electronic chip the following bearer's data are stored: filiation details, digitalized image of the photograph, digitalized image of the handwritten signature, digital fingerprint, advanced certificate of authentication and signature, electronic certificate of the issuing authority and PIN codes for each electronic certificate.

[20] Information obtained at www.dnielectronico.es

Its dimensions are identical to the traditional ID card and its size coincides with the credit cards that are commonly used.

As mentioned before, the chip of the document contains two types of certificates: the authentication certificate and the signature certificate.

The authentication certificate has the purpose of electronically guaranteeing the citizen's identity when effecting an on-line transaction. With this certificate, the bearer may prove his identity before anyone because he possesses the certificate of identity and the PIN code associated with it.

This certificate must be used solely and exclusively for authentication systems (confirmation of identity) and for safe access to information systems (by means of the establishment of private and confidential channels with the servers). Based on the authentication of this certificate, the certification service providers must not give access to personal information or request signatures on procedures or documents.

This certificate may also be used as a means of authentication recognised by private entities, without the latter being obliged to make a strong investment in the organisation and maintenance of a registration infrastructure.

The signature certificate allows the citizens to eSign procedures or documents, allowing the substitution of the handwritten signature with the electronic one based on the relationships of the citizen with third parties[21].

The activation of the eID card is not automatic as it requires the precise system to unblock the conditions of access by means of the personal code of access (PIN) and/or the impression of fingerprints (biometrics).

Only Spanish citizens can obtain the eID card (DNI-e). The Royal Decree 1553/2005 of December 23rd, regarding the issuing of the national identity card, its certificates of authenticity and eSignature (http://www.dnielectronico.es/marco_legal/RD_1553_2005.html) confirms that the Police General Directorate is the department (belonging to the Interior Ministry) to exercise all competences of management, direction, organisation, development or administration of all matters concerned to the issuance or performance of ID cards, including the electronic ones. In practice, the role of VA has been delegated to the MAP (Ministry of Public Administration) and the FNMT (the Mint).

As stated in section C.3., the issuance of electronic resident cards (NIE-e) is also planned for resident foreigners in Spain.

[21] Articles 3, 4 and 15.2 of eSignature Law.

3.3.1.2 Commercial PKI certificates

Apart from the eID card certificates, other PKI certificates continue to be used in parallel with the eID card. Certificates recognised for this purpose are eCertificates provided by a certification service provider that has satisfied special legal requirements (similar to the ones established by Directive 1999/93/EC). Regarding the financial resources to bear the risk of liability for damages, in Spain certification service providers (CSP) are obliged to subscribe a civil liability insurance of at least 3.000.000,00 Euros.

It is important to mention that under the eSignature Law, CSPs that provide certification services do not need an administrative authorisation (in compliance with the eSignature Directive guidelines). Therefore, any new CSP willing to provide certification services is only obliged to notify it to the Ministry of Industry, Tourism and Commerce by giving identification data; and then the Ministry will verify compliance with the eSignature Law. After the checking is concluded succesfully, the CSP is included in the list published at its website: http://www.mityc.es/DGDSI/Servicios/FirmaElectronica/Prestadores/.

CAs are obliged to publish their Declaration of Certification Practices and any of the documents recorded in article 19 of the eSignature Law:

> Declaration in which they will detail the obligations that they commit to comply.

> The declaration of certification practices will be at public disposal, easily accessible, at least by electronic means, and for free.

> The declaration of certification practices will be considered as a security document.

In those documents the CAs give a series of technical and legal guarantees about the management and conservation of their certificates and the corresponding authentication services.

3.3.1.3 MAP multiPKI Validation Platform

The launch of the electronic national identity card has been complemented by the creation of a multiPKI Validation Platform[22] supported by the MAP that provides freely eSignature and eCertificate validation services to eGovernment services (currently there are about 180 available services using the platform). It is this platform which binds the authentication services of the national eID card and commercial PKI certificates together, and which allows application owners to use both identification solutions.

[22] More detailed information at: http://www.dnielectronico.es/seccion_aapp/platform.html

The MAP multiPKI Validation Platform (called Platform @firma v.5.0.) validates electronic certificates and eSignatures issued by the main Certification Authorities of the country, including the eID Card Certification Authority, and also provides time-stamping services and an eSignature program that allows citizens to eSign documents in various eSignature standards locally before being submitted over the Internet. The service is offered to eGovernment applications of all public administrations (state, regional and local). The platform has been built up on open source and open standards.

Currently this Platform supports 11 certification services providers[23] and 56 types of eCertificates.

a) Public Providers of Certification Services

- DGP (Dirección General de la Policía – Police General Directorate): http://www.dnielectronico.es/

D. FNMT-CERES (Fábrica Nacional de Moneda y Timbre – Royal Mint): http://www.cert.fnmt.es/

DI. CATCert (Agència Catalana de Certificació – Catalonian CA): http://www.catcert.net/web/cat/inici/home.jsp

DII. ACCV (Autoritat de Certificació de la Comunitat Valenciana – Valencian CA): http://www.accv.es/default_default.htm

DIII. IZENPE (Basque CA): http://www.izenpe.com/s15-5218/es/

b) Private Providers of Certification Services

- AC Camerfirma (Commerce Chamber): http://www.camerfirma.com/
- ANF AC (Asociación Nacional de Fabricantes - Autoridad de Certificación): http://www.tradise.com/tradise/
- ANCERT (Agencia Notarial de Certificación-Notaries): http://www.ancert.com/
- Firma Profesional: http://www.firmaprofesional.com/bienvenida.htm
- ACA (Autoridad de Certificación de la Abogacía-Lawyers): http://www.cgae.es/especial/acaredabogacia/acaredabogacia.htm
- Banesto (Banco Nacional Español de Crédito - Bank): http://ca.banesto.es/

The Platform also provides an eSignature client for its use by citizens in the Administrations Portals[24]. This way, through standard interoperable interface of callings to services (web services technologies), the public entities immediately incorporate the most recognised certificates of the country (the eID card among them) to their services of eGovernment and offer eSignature to citizens in various formats or international standards which are validated by the Platform.

---

[23] The list of authorities is available at http://www.dnielectronico.es/seccion_aapp/rel_autoridades.html

[24] Additional information about the role of the Platform has been provided by Miguel Álvarez Rodríguez (MAP). See footnote 21.

Despite this, it remains the responsibility of the application owner to permit more or less rigid authentication methods (user code or security token, SW recognised electronic certificates, HW, or in the strictest case only the eID card itself). In some cases, sector regulation related to the service using the eGovernment application requires the use of recognised eSignatures for online transactions when this is required for making petitions or for presenting letters to the Public Administration in person. There is an increasing tendency within the Spanish Administration to require identification by eCertificates in their online transactions. However, it is required by law that the new eID card be admitted by all eGovernment services for authentication and eSignature purposes, so that all Spanish citizens are entitled to use those certificates in their transactions with all the existing eGovernment services. Thus, the eID card is likely to become a standard solution for electronic authentication.

Full information is contained in the document "*Declaración de certificados de @firma*" (Declaration on @firma certificates), issued on September 2006: http://www.dnielectronico.es/PDFs/dec_cer_6.pdf, where 3 groups of certificates, widely used by citizens/enterprises within their relation with public Administrations, are classified, according to their nature: certificates related to natural persons, corporate persons or components.

- Natural Persons (NP) Certificates, directed to citizens or individuals as a way of eIdentification on the Internet, which allow the creation of recognised eSignatures.
- Corporate Persons or entities (CP) certificates, usually issued to the company's legal representative (or person empowered to Law on behalf of the company), recognised in many eGovernment applications for the signature of administrative procedures.
- SW Certificates or components for coded SSL, for machines or automated processes where online petitions or answers have to be eSigned; for the creation of safe channels for the data exchanging between the server and citizen (e.g. applications of online Registry). This type of certificate is not recognised yet (SW based certificates are free for citizens in most cases).

3.3.1.4 Virtual Office

During the last years the Tax Agency[25] has developed a Virtual Office that allows, among other services, to present declarations, to access their consultation, or to see taxing information. To accede to this type of services, a certificate (electronic signature) is required that fully assures the identity of the user, and with it, that the declarations sent via web may only be originate from the person who sent them.

The Tax Agency recognises certificates issued by different certification authorities. Each one of them may have different procedures to obtain them. In all cases, the physical presence of whoever shall be the bearer of the certificate (or the user, in the case of certificates issued to legal persons) before the Registry Authority is required, in order to demonstrate his identity and to supply the documents that are needed.

[25] Information obtained from www.aeat.es

These services may be used by natural or legal persons. For natural persons foreigners who are legal residents in Spain may use these services.

Social Security has also developed a Virtual Office or attention counter for Internet users through which citizens, corporations and collaborators of Social Security who had previously effected consultations and procedures personally, may now do them in any of their offices.

In order to use these services is it necessary to have an electronic certificate, although in other cases, the person may make the request without the electronic certificate, but then the report is sent to the address that appears in the data base of Social Security.

3.3.1.5 Authentication Policies

There is no defined policy in Spain concerning authentication that establishes different hierarchies in the existing authentication systems. However, in practice there is a certain hierarchy among them, fundamentally based on the sensitivity of the information which is accessed and in the security measures that each one of the authentication systems implies.

In the following chart this hierarchy is specified, with certain examples:

Level	Citizen's Identity	**Citizen's Authentication**	Applications
0	None	None	Specific public services such as the downloading of forms for tax declarations
1	Online, introducing an identity number, fundamentally the ID card number (DNI) or tax identification number (NIF)	Authentication takes place inserting a user name and a password	Specific public or private services of relative importance such as e-mail services or specific requests, like the draft of the tax declaration
2	Includes level 1 and delivery of an e-mail with a URL activation or the delivery of a letter to the users address containing the data necessary to activate the service	Includes level 1 and the introduction of an random and changing combination of letters or numbers	Services of much importance that require a greater security degree such as, for example, banking services
3	Physical and in presence identity is required to obtain the user's certificate	Authentication based on the user's certificate	Highly confidential and very personal services such as access to personal information stored by the Administration: work resume, medical history

3.3.2 Legal Framework

The applicable legal framework is established by the following rules:

- Directive 1999/93/CE of the European Parliament and the Council, of 13 December 1999 on a Community framework for electronic signatures
- Law 59/2003 of December 19, on Electronic Signature (hereinafter, eSignature Law)
- Organic Law 15/1999, of December 13, on the Personal Data Protection
- Royal Decree 1553/2005, of December 23, ruling the national identity card and its eSignature certificates.

The eSignature Law was enacted to incorporate certain innovations regarding Royal Decree-law 14/1999 of September 17 that already regulated eSignature, such as the "recognised" eSignature (Spanish equivalent to the qualified signature), and to determine the basic ruling framework of the eID card, expressing its two most characteristic aspects (verifying the identity of its bearer in any administrative procedure and allowing the eSignature of documents), remitting itself to the specific ruling concerning the peculiarities of its legal system[26].

On the other hand, Organic Law 15/1999, of December 13, on Personal Data Protection, which aims "to guarantee and protect, in everything that concerns the handling of personal data, the public liberties and fundamental rights of natural persons, and especially their honour and personal and family intimacy", and is also applicable to all those agents that intervene in the creation of the eSignature or other electronic identity documents and need to deal with personal data.

Lastly, Royal Decree 1553/2005 of December 23, whereby the national identity document and its certificates of eSignatures is regulated, specifies the basic rules on the issuance of normal and electronic identity documents as well as the regulation of rules on issuance and validity of electronic certificates.

The main electronic identity system is the eID card which is compulsory for persons over 14 years. As indicated previously, the issuance of the eID card began in 2006, and therefore a certain period of time will elapse before all Spanish citizens have the eID card.

There are other electronic means of identity that allow citizens and corporations to access to different electronic administration services, most notably the commercial CSP certificates discussed above. These however are of course voluntary means.

[26] Preliminary recitals of eSignature Law.

The eID card distinguishes between signature and identity functionality because it serves to electronically and undoubtedly verify the identity of the person, as well as to eSign documents with a legal value equal to the one provided by the handwritten signature.

Citizens are informed of the advantages of the eID card by means of general information campaigns, by means of the information provided at the moment of issuing the electronic ID card and through information that is available on the web page specifically created to provide information about this instrument.

Concerning the security of the data, the eSignature Law refers to the general rules. However, article 17 of eSignature Law indicates a series of obligations for providers of certification services such as "they may only gather personal data directly from the signers or with their prior consent", and that "the data required shall exclusively be the data necessary for the issuance and maintenance of the electronic certificate and the rendering of other services related to eSignatures, and not being able to be considered with different purposes without the express consent of the signer."

Although at present the electronic identity systems are only being used by public organisations, they have been designed so that they may also be used by private parties. Many online services that are currently provided by private groups shall substitute their authentication systems for the eID card.

E-Signatures may be used by legal persons. Article 7 of the eSignature Law indicates that "electronic certificates of legal persons, their administrators, legal and voluntary representatives with sufficient faculties for these effects may be requested."

This same article prescribes that "electronic certificates of legal persons shall not affect the system of organic or voluntary representation that is regulated by civil or commercial legislation applicable to each legal person".

It also indicates that "the custody of data on the creation of signatures associated to each eCertificate of legal persons shall be the responsibility of the requesting physical person, whose identity shall be included in the eCertificate."

Lastly, it prescribes that "actions or contracts shall be understood as having been effected by legal persons" if they have been eSigned within the limits foreseen in the rule.

3.3.3 Technical Aspects

Today in Spain, two types of authentication mechanisms are being used.

One of them, whose main example is the national eID card, is based on a PKI infrastructure with a cryptographic card containing an intelligent chip (http://www.dnielectronico.es/Guia_Basica/descripfisica.html). Apart from the national eID card, this system can also be used by the aforementioned commercial CSPs if they choose to issue smart cards containing their certificates.

The other system is authentication by means of electronic certificate based only on software elements such as the one offered, for example, by the Fábrica Nacional de Moneda y Timbre (the Spanish Royal Mint, hereinafter, FNMT) (http://www.cert.fnmt.es/content/pages_std/html/aplications/ayudam.htm).

At present there is no difference between the on-line services offered for both types of authentication systems, although it is true that as an official identity method before authorities, only the ID card is valid.

Both the physical card used by the national eID card as well as other smart cards used for other certificates (for example, like the one issued by the Royal Mint) use format ID-1 (credit card type)

(http://www.dnielectronico.es/seccion_integradores/Tarjeta:Soporte.html).

The main information concerning the Spanish national eID card is contained at a Basic Reference Guide, issued on June 2006 by the Technical Commission to support the implementation of the eID card is available at http://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1.0.pdf. The eID card uses contact ICs, with ISO 7816-3 compatible access and with an EEPROM size of 34 Kb for data

(http://www.enielectronico.es/PDFst19w134.pdfP).

The electronic certificate on the card used by the eID card and by other smart cards incorporates cryptographic capacities

(http://www.dnielectronico.es/seccion_integradores/espec_uno.html,

(http://www.cert.fnmt.es/index.php?cha=cit&sec=tech_support&page=85).

The cards used for the national eID card and the Royal Mint use the standard PKCS#15

(http://www.dnielectronico.es/oficina_prensa/imagenes/060315/dossier_maquetado_final.pdf

(Http://www.cert.fnmt.es/index.php?cha=cit&sec=tech_support&page=85).

The cards used for the national eID card also follows other standards: ETSI TS 102 042,ETSI TS 101 456, ETSI TS 101 862, CWA 14167, CWA 14172, CWA 14.890 (http://www.dnielectronico.es/seccion_integradores/estandares.html).

The cards used for the national eID card and the Royal Mint follow the standards PKCS#11, CSP and API PC/SC

(http://www.dnielectronico.es/como_utilizar_el_dnie/ and

(http://www.cert.fnmt.es/index.php?cha=cit&sec=tech_support&page=85).

The hierarchy concerning the PKI of the national eID card consists of a two-layered model:

- A first level where the Root CA ("AC Raiz") is located, representing a confidence key point for all the system. This way, all natural, corporate, public or private persons will recognize the effectiveness of the eID card for vouching the identity. This AC only issues certificates for itself and its AC Subordinates. It will only be operating during the realisation of operations for which it is established and the dependant Police General Directorate exercises these functions.
- A second level constituted by the CA subordinated to the Root CA ("AC Subordinada") that will issue the identification and signing certificates included in the eID card.

http://www.dnielectronico.es/seccion_integradores/certs.html.

The following entities take part in the management of the eID card:

- The Police General Directorate, as competent organ to issue and manage the eID card;
- The Authority approving the policies, as a PKI Executive Committee responsible for the elaboration and updating of the *Declaration Draft about Certification and Practice Policies*, as abovementioned; and the organ that will study the possibility of an external CA inter-acting with the PKI of the eID card or the provision of validation services by third parties.
- Certification Authorities (CA), as outlined below:
    - a Root CA that only issues certificates for itself and its subordinated CAs. Certifications of Root CA : http://www.dnielectronico.es/certs/Acraiz.crt
    - 3 subordinated CAs that issue certificates for eID card holders. Certifications of subordinated CAs: http://www.dnielectronico.es/certs/AXXX.crt[27]
- Registry Authorities: constituted by all offices that issue the national ID card, that will assist the CA in all proceedings related to citizens concerning their identification, registry or authentication, guaranteeing the correct assignment of keys to the applicant.
- Validation Authorities (VA): that will check the certificates' current status by using the OSCP: http://ocsp.dnielectronico.es, which shows to any third party its present status to an Accepting Party, without asking them to access the published CRLs. Initially only the MAP (Ministry of Public Administration) and the FNMT (the Mint) will act as VA on behalf of the Police Department.
- Accepting Party: any person or entity, different to the holder, that accepts and trust on the certificates contained in the eID card.

Not all Public Administrations offering online transactions have already adapted them from a technical point of view so as to also accept the new eID card[28]. Some organisms such as the Tax Agency have leaded the launch of new services of easy management by citizens (e.g. tax

[27] XXX is the 3 digits numeric identifier of the subordinated CA

[28] Full list available at: http://www.dnielectronico.es/servicios_disponibles/

declarations by natural persons), initially based on eSignatures, which are also now compatible with eID cards.

The standard for the publication of certificates is Online Certificate Status Protocol (OCSP), according to which, an OCSP customer sends a request on the status of the certificate to the Validation Authority who, after consulting its database, offers – via http – an answer on the certificate status

(http://www.dnielectronico.es/Autoridades_de_Validacion/).

As a method for revocation, certificate revocation lists (CRL) are used

(http://www.dnielectronico.es/Autoriddes_de_Validacion/).

The electronic identity system in Spain is based on a centralised registry in the Police General Directorate (Ministry of Internal Affairs), and it is in its office for issuing the eID card where the certificates of Spanish citizens are registered

(http://www.dnielectronico.es/obtencion_del_dnie/doc_acep_080506.pdf).

The eID card system is not based on Liberty alliance, WS Star, or SAML.

Presently in Spain, all Public Administrations offer e-Administration services that rely on users' certificates. The connection between a citizen and an entity (public or private) is established as follows:

- The citizen makes a request for an authenticated security connection.
- The Public Organism (or Private Entity) creates an authenticated message and sends it to the citizen.
- The citizen verifies the validity of the service certificate offered.
- The code for the session and its cipher is generated with the public code of the Public Organism (or Private Entity).
- The message for the exchange of codes is constructed.
- The citizen introduces the eID card in the reader and, with the electronic authentication certificate, validates the codes exchange message.
- The private channel is established.
- The Public Organism (or Private Entity) verifies the message to open the session.

- The Public Organism (or Private Entity) verifies in the Validation Authority the validation status of the Citizen's Authentication Certificate.

- A secure channel is established and the SSL tunnel is closed.

As is reflected in the previous outline, the authentication process between both parts to establish a secure channel requires the use of two certificates. On one hand, a Certificate from the Public Organism (or Private Entity): this certificate, associated to the Organism or Entity's server, guarantees that the citizen is connecting with the mentioned organism and not to another. The certificate used by the Organism or Entity is in no case issued by the DGP or the Ministry of Internal Affairs. The veracity of this certificate must be guaranteed by a Certification Authority other than the Police General Directorate, and subject to eSignature Law in the framework of obligations applicable to the providers of certification services.

On the other hand, the citizen uses his own authentication certificate, in order to be identified before the organism (or Private Entity). In this manner, the Organism (or Private Entity) may determine the identity of the citizen to offer a personalised service. The veracity of this certificate shall be determined by the Police General Directorate in the case of the eID card

(http://www.dnielectronico.es/Guia_Basica/uso_dnie.html).

The description of the fields of the signature certificate is contained in the table below. Please not that in the Spanish case there is a difference between the Citizen Signature Certificate (CSC) and the Citizen Authentication Certificate (CAC). As their technical description is almost the same, differences will be directly highlighted along the table[29].

e-ID citizen Signature Certificate (CSC) / Authentication Certificate (CAC)					
Base Certificate	**OID**	**Include**	**Critical**	**Value**	
Certificate					
SignatureAlgorithm					
Algorithm		X		SHA256 with RSA Encryption SHA1 with RSA Encryption	Fixed
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		Standard X.509 v3	
SerialNumber		X		Not sequencial	Dynamic
Signature		X		SHA1 with RSA Encryption[30]	
Validity					
NotBefore		X		Key Genenration Process Date/Time	
NotAfter		X		Key Genenration Process Date/Time + 30 months	
SubjectPublicKeyInfo		X		RSA Encryption – Key length: 2048 bits	
Issuer					
CountryName	{ id-at-6 }	X		ES	Fixed

29 Information extracted from the report "European eGovernment Services (IDABC)".

30 SHA256 with RSA Encryption is foreseen for citizen certificates by 2009.

CommonName	{ id-at-3 }	X		CA DNIE XXX[31]	Fixed
Organization		X		Dirección General de la Policía	Fixed
Organizational Unit		X		DNIE	Fixed
Subject			Required		
countryName	{ id-at-6 }	X	YES	ES	Fixed
CommonName	{ id-at-3 }		YES	**CSC:** 1st Surname 2nd Surname, GivenName (signature) **CAC:** 1st Surname 2nd Surname, GivenName (autentication)	Dynamic
Surname	{ id-at-4 }	X	YES	provided by RRN	Dynamic
GivenName	{ id-at-42 }	X	YES	provided by RRN	Dynamic
SerialNumber	{ id-at-5 }	X	YES	Citizen ID number, including letter[32]	Dynamic
Standard Extensions	**OID**	**Include**	**Critical**	**Value**	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		**CSC:** 2.16.724.1.2.2.2.3 **CAC:** 2.16.724.1.2.2.2.4.	Fixed
policyQualifierrs					
policyQualifierId	{ id-qt-1 }				
Qualifier		X		http://www.dnielectronico.es/dpc	Fixed
Qualified Certificate Statement					
qcStatement	{ id-etsi-qcs 1 }	X		id-etsi-qcs-QcCompliance id-etsi-qcs-QcSSCD	
KeyUsage	{id-ce 15}	X	TRUE	N/a	
Digital Signature		X	TRUE	**CSC** : 0 **CAC** : 1	
NonRepudiation (Content Commitment)		X	TRUE	**CSC :** 1 **CAC:** 0	
Key Encipherment		X	TRUE	0	
Data Encipherment		X	TRUE	0	
Key Agreement		X	TRUE	0	
Key Certificate Signature		X	TRUE	0	
CRL Signature		X	TRUE	0	
KeyIdentifiers	{id-ce 35}	X	FALSE		
AuthorityKeyIdentifier		X	FALSE	Application of SHA-1 Hash on CA PKI	
Subject Key Identifier		X	FALSE	Application of SHA-1 Hash on Subject PKI	
CRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint			FALSE	It will not be used	
FullName					
NetscapeCertType					
Subject info		X			
Biometric info		X	FALSE	Hash of biometric data SHA256/SHA1	
Personal data info	2.16.724.1.2.2.3.1.	X		Hash of biographic data (printed data on eID card) SHA256/SHA1	
Subject Directory attributes		X		Date of Birth	

31 XXX= number that identifies the issuer CA

32 The letter is a control digit used in Spain so as to avoid transcription errors.

Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }				
accessLocation		X		OCSP http://ocsp.dnie.es Root CA http://www.dnie.es/certs/Acraiz.crt	
accessMethod	{ id-ad-1 }				
accessLocation					

All the entities implied (the Origin Certification Authority, the Subordinate Certification Authorities and the accepting Third Parties) share information by means of Certificate Revocation Lists (CRL)

(http://www.dnieledtonico.es/PDFs/politicas_de_certificacion.pdf).

The national eID card allows the biometric verification of the identity of its bearer although this function will only be available at controlled points of access. The system uses the fingerprint of the user for his identity, and to do so, it uses the Match on Card algorithm

(http://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_y1.0.pdf).

3.3.4 Organisational Aspects

In Spain, the procedure for citizens to obtain their national eID card is summarised in four steps.

The citizen who requests his eID card for the first time and thereby, the associated electronic certificates, must appear before an Office for the Issuance of the electronic ID card.

To request the issuance of the eID card, the physical presence of the person to whom it will be granted and the presentation of the required documents will be indispensable.

The delivery of the ID card and of the associated certificates will be done personally to its bearer on the same day on which he requests its issuance.

After having completed the phase for the documentary presentation and the physical personalisation of the card, the logical phase of personalisation begins with the charging of data on the chip of the support card. The generation of codes shall be effected on the card and in the presence of the bearer, after the qualification of a random PIN that is delivered in a closed envelope. Afterwards, the citizen may change his PIN number for added security.

After having obtained the eID card, the citizen may use the services of the State Administration already available with the electronic certificate, and likewise he may use the ever more numerous services of other administrations (regional and local) that allow the use of these certificates. In this line, the efforts of the Spanish Administration are being oriented towards solving the problems of compatibility of services, both public as well as private, and the solutions that are being found are satisfactory.

The eID card will allow the Certificate Authorities of a second level to issue certificates without requiring the physical presence of the petitioner, which will sensibly reduce their needs for infrastructures, as well as facilitating the procedures for citizens[33].

Concerning the authorisation and delegation processes, at present in Spain there is no specific generalised policy or infrastructure yet. However, there are certain cases where this delegation exists, such as the one developed and used for the presentation and on-line payment of taxes. Indeed, the Tax Agency recognises certain persons called "collaborators", who may belong to other public administrations or private entities, institutions or organisations that represent specific sectors or social, labours, entrepreneurs or professional interests.

This collaboration fundamentally refers to the following aspects: simplification in the fulfilment of taxing obligations, assistance and verification of tax returns' correct declaration. The collaboration also includes, after authorisation by the obliged persons to electronically present to the Tax Administration tax returns, declarations, communications or any other document with taxing transcendence, correction of errors, information on the status of the procedures for returns and reimbursements, and requests and obtainment of tax certificates.

In order to act on behalf of third parties with their own certificate, a collaborator requires a specific authorisation from the citizen, who may grant it by personally appearing at the Tax Agency offices, or by means of a public or private document[34].

3.4 Interoperability

As mentioned in section C.3., NIE-e will provide its bearers (foreigners with legal residence in Spain) an electronic authentication tool that will allow them to use electronic signatures, the same as the DNI-e.

Otherwise, there are no operational mechanisms in Spain to accept eIDM from other countries. The main interoperability initiative in Spain has been the creation of the Validation Platform, known as "@firma", which is mostly focused on creation national interoperability between the existing and future CSPs.

[33] http://www.dnielectronico.es/obtener.html

[34] http://www3.aeat.es/ADUA/internet/apodern.htm

Nevertheless, the European Commission Action's Plan i2010, and, in particular, the Manchester's Ministerial Declaration signed on November 2005, wishes to establish by 2010, an Interoperable EU eIDM Framework that will imply the possibility of accepting electronic identifiers from other countries, so that any E.U. citizen can make administrative transactions with their national identifiers, without needing to obtain a Spanish one, as mentioned before.

These measures will probably need to be accompanied with legislative changes at European and national level to enable the incorporation of non-national eIDM systems to the electronic administrative transactions of each country.

Within the i2010 plans, the European Commission proposes, in the Competitiveness and Innovation Program (CIP), the execution of several experiments at a large scale or "real" tests of interoperability, between several member states, on certain Pan-European e-Administration services that give the citizens and companies the possibility of mobility inside the EU (health care, taxation…)".

These experiments will prove the suitability of the common specifications defined in order to allow foreign citizens the use of their eIDM when they accede to e-Administration services provided by their residence country. The Spanish government is collaborating in this project through the Ministry of Public Administrations (MAP) with the Validation Platform.

3.5 eIDM Applictions

3.5.1 Public sector applications

At present most relevant eIDM applications are developed by the public Administration. From September 2006 onwards, private citizens can use more than 250 eServices that require the use of eSignature. All services accessible with the eID card are available and listed at: http://www.dnielectronico.es/servicios_disponibles/.

This web site includes services within the

- State General Administration. See complete list at http://www.dnielectronico.es/servicios_disponibles/serv_disp_age.html
- Regional Administrations (Andalusia, Castilla y León, Asturias, Navarra, Galicia and Cantabria). Operational services offered by each Region, available at http://www.dnielectronico.es/servicios_disponibles/serv_disp_ccaa.html

- Local Administration . At present, only Albacete (in Castilla-La Mancha Region) is offering e-services using the eID card. See http://www.dnielectronico.es/servicios_disponibles/serv_disp_adm_loc.html

Some organisms such as the Tax Agency (AEAT)35 have led the introduction of these services based on eSignature and therefore the most significant efforts have been focused so as to guarantee the interoperability of the existent services with the eID card, including applications (payment of taxes, requests of information, notifications,…)

There are many applications in the public sector, mostly related to data access in different public registries and to realize certain on-line transactions in the same way and with the same legal effects than the off line proceedings.

3.5.2 Private sector applications

Although in an early stage, private sector has seen in the eID card new business opportunities and is now developing new electronic services based on this eIDM system.

> In this sense, some banking organizations allow their clients to identify themselves and to make consultations with their DNI-e when they are providing financial services by Internet:

- In the mid term, the DNI-e will also be used to sign banking operations as well to contract on line products or financial services (www.bancosabadell.com).

- Another banking institution (Caja Madrid) already allows its clients to be identified by their DNI-e when they require financial services on line. This entity is also adapting now its cash machines in order to let its clients to use their DNI-e instead of the traditional banking cards. (https://oi.cajamadrid.es/CajaMadrid/oi/pt_oi/Login/login).

> Finally, Cisco Company has developed a system that will allow the users to be identified in Virtual Private Networks with their DNI-e. This system allows the users to connect on-line with their companies or organizations using the DNI-e.

[35] Complete list of e-services already using the eID card offered by the Tax Agency is available at http://www.dnielectronico.es/servicios_disponibles/age_trib.html

3.6 Future Trends / Expectations

The Spanish Administration is presently focused on the issuance of the DNI-e, the eID card that will become the main eIDM system in Spain.

This system is compatible with the eSignature certificates that many citizens and corporations already use. The public Administration is encouraging the electronic services that need electronic authentication. At the State Administration there are many ministerial departments that are now making a significant effort to generalise electronic communications, and in some cases to establsh them as the only communication channel with the citizens.

On the other hand, the State Administration is obliged to employ, as much as possible, systems that guarantee the compatibility of the instruments of eSignatures included in the eID card with different equipment and products of eSignature that are generally accepted in Spain.

3.7 Assessment

3.7.1 Advantages

- With the eID card citizens will have a very useful means of identification that will allow them to consult personal data, to fulfil procedures or negotiations, or to access different public and private electronic services, providing the highest degree of confidentiality and security on the Internet, and identifies the parties in their on-line transactions.

- All Spanish citizens will have an eID card (DNI-E) because its issuance is compulsory. The obtainment of the document will imply the obtainment of information regarding the electronic means of identification and their possibilities.

- Today there are many citizens that are not using any other means of electronic identification, and are not using any on-line electronic services because of their ignorance regarding the operation of these systems.

- Corporations should develop different services based on the identification and eSignature, so that they may enliven the commercial relationship with their customers. These services will be offered with maximum security. From the corporative and commercial point of view, the eID card becomes a fundamental tool in relationships with the private sector.

3.7.2 Disadvantages

- Although it is already planned, the Spanish Administration has not developed yet, in general, eIDM systems for foreigners, although foreigners holding a resident card (NIE) may obtain electronic certificates in order to interact with the Administration.

- There is much social ignorance regarding the possibilities offered by the electronic identification means.