eID Interoperability for PEGS

NATIONAL PROFILE PORTUGAL

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

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

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 Portugal 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 e-IDM systems

The most significant e-IDM system in Portugal is based on the Personal Identity Card (*Cartão do Cidadão*), to be granted to Portuguese Citizens from the age of 6 and up. A second relevant e-IDM is the project of the Electronic Passport.

The Personal Identity Card has been launched in February 14, 2007. It has only been implemented in Azores and it is expected to cover all Portuguese territory by the end of 2008. However, the roll-out processing will take until 2012 to have full coverage and to replace the paper token. In the areas that are covered, the issuance of the Personal Identity Card is mandatory. The ID card costs 12 euros. This card will only be distributed by the same location where the ID hard copy document is provided: the Local Civil Registry and Citizen's Shops ("*Lojas do Cidadão*").

Detailed information is available through the official Portuguese eID website (http://www.cartaodecidadao.pt/).

The card contains 4 numbers ("personal identification number", social security number, tax number and health user number) and a chip holding two certificates: one for authentication purposes, and one for qualified signatures.

The system is closely linked to the Instituto da Tecnologia da Informação na Justiça (*ITIJ*) - *Sistema de Gestão do Ciclo de Vida de Cartão do Cidadão* - , which contains a key set of authentic attributes for citizens registered in it.

The attributes stored in the authentication certificate of the eID card are obtained directly from the *ITIJ*, being the other data collected from: (a) the Identification Services (*Serviços de Identificação Civil da Direcção-Geral do Registos e Notariado*) in relation to the "identification number"; (b) regarding the tax number, from the Tax authorities (*Direcção-Geral de Contribuições e Impostos*); (c) regarding the health number, from the Ministry of Health (*Ministério da Saúde*); (d) data referring to the Social Security, from the Social Security (*Segurança Social*).

The eID card will function as a unique card for Portuguese citizens, but it contains several numbers, due to constitutional restraints in adopting one unique number to Portuguese citizens.

As mentioned tokens include also the paper federal token in the areas where the e-Card is not implemented.

From a practical perspective, usage and uptake can be summarised as follows:

e-IDM system	Potential user base	Actual penetration	Actual use
National eID card	Population after 6 years old (and also previously granted by parents application)	Only in the islands of Azores	No public statistics are available
Federal paper token	To be eliminated in the future.	Estimated almost all population after 6 years old.	No public statistics are available

The e-Passport is another relevant e-IDM project. This project is also in a start-up phase, since it has been launched last August 28, 2006.

3.2 Background and traditional identity resources

3.2.1 e-Government structure

The implementation of e-IDM systems in the context of e-Government is coordinated centrally in Portugal. In this regard, e-Government applications are developed at a national level. E-Government projects in Portugal mainly focus on horizontal integration covering several departments and institutions. There are others that are vertically integrated, i.e., within the same area of competence, such as tax or social security.

By means of the Resolution of the Council of Ministers No. 108/2003 the Plan of Action for the E-Government was approved. This Plan is part of the said Plan of Action for the Information Society. It is aimed at placing both citizens and companies at the core of the state's modernisation process.

The Resolution listed the following main projects concerning e-Government that are to be set up: the citizen's portal; framing of the operational rules; rationalization of communication costs; electronic shopping including the launching of seven pilot projects in 2003; creation of the Public Administration's portal and of the civil servant's portal; a national social security information system; an e-card registration system and integrated systems to keep registries of deeds and of notaries public.

The Resolution of the Council of Ministers No. 109/2003 approved the National Initiative concerning broadband infrastructure. Its main purpose is to ensure the mass access to and use of this technology, thus contributing on the one hand to an increase in productivity and competitiveness rates of the Portuguese economy (significantly lower than the average European rates), and on the

other hand to a greater social cohesion. It is believed that the said rates can only rise if mass access and use of ICT is achieved.

3.2.2 National e-Government cooperation and coordination

In the Green Book for the Information Society (*Livro Verde para a Sociedade da Informação),* the Portuguese Government stresses the economic, social and cultural value of information and its role in the evolution of society. The Green Book also identified the need to implement and develop the concept of an e-Government.

After the publication of the Green Book, the Resolution of the Council of Ministers no. 94/99 (*Resolução do Conselho de Ministros n.º 94/99*) — approving the Guideline Document of the National Initiative for Electronic Commerce — provided the first legal/governmental reference to the subject. This resolution covered several areas, including among the most important ones, the legal certification and recognition of electronic commerce, to encourage the harmonisation, interoperability and security of payment methods as well as guidelines on the modification of tax systems.

The application of said principles in the Public Administration would represent an important move in the market, as the state plays an important role in companies' business. Moreover, the need to exchange information within the relevant public authority will increase the efficiency of resources. The use of electronic commerce as a vehicle to increase effectiveness in the exchange of information from one ministry to another would give rise to a re-analysis of the transfer of information mechanisms.

This Resolution included several measures to be adopted and led, on the one hand, to the implementation of rules on the use of electronic signatures by administrative entities and, on the other hand, to the use of electronic solutions by entities in their business activity.

Similarly, the government issued several resolutions to improve the implementation of e-Government platforms and to create the legal framework for the acquisition of goods and services by the Public Administration. The Resolution of Council of Ministers no. 36/2003, of March 12, pointed out the need to adopt and generalize electronic platforms within the scope of the transactions conducted by public authorities.

On November 24, 2005, the Portuguese Government approved a reference and public commitment document, entitled Technological Plan (*Plano Tecnológico*). Furthermore, the Knowledge Society Agency (Agência para a Sociedade do Conhecimento - UMIC) has been appointed as the entity that coordinates the e-Government in Portugal.

Finally, all the relevant legislation has been enacted in order to implement the State Electronic Certification System - Sistema de Certificação Electrónica do Estado ("SCEE").

- Technological Plan

The Technological Plan is aimed at the application of a growth strategy and competitiveness based on knowledge, technology and innovation.

The Technological Plan is under the direct supervision of the Prime Minister and is intended to signify a change in the Portuguese society. The aim of the Plan is to prepare Portugal for the challenges modernisation[3] poses.

The Plan provides the main measures to be taken at a high-level. The government bodies have the task of developing and implementing the Plan. The Technological Plan foresees a Coordination Network (*Rede de Coordenação*) composed of representatives of all Ministers.

- UMIC

The Knowledge Society Agency (Agência para a Sociedade do Conhecimento - UMIC[4]) was created by Decree-Law no. 16/2005, of January 15 (*Decreto-Lei nº 16/2005*), and its articles of association published on February 21, 2005. UMIC is a Portuguese public agency engaged in the planning, coordination and development of projects in the area of the Information Society, including electronic government. It was created in January 2005, as a public entity with administrative and financial autonomy which succeeded the former Unit for Innovation and Knowledge, in November 2002. UMIC is part of the Council of Ministers.

- SCEE

Decree-Law no.116-A/2006, of June 16, enacted the State Electronic Certification System - *Sistema de Certificação Electrónica do Estado* ("SCEE")[5].

The SCEE encompasses the Managing Council of the Electronic Certification System (*Conselho Gestor do Sistema de Certificação Electrónica do Estado*), the State Electronic Certification Entity (*Entidade de Certificação Electrónica do Estado*) and the State Certification Authorities (*Entidades Certificadoras do Estado*).

The SCEE is aimed at establishing a single, integrated and effective digital authentication system in electronic communications among citizens, the state and public entities.

[3] This is the wording of the official website at http://www.planotecnologico.pt/pt/planotecnologico/o-que-e-o-plano/lista.aspx.

[4] http://www.umic.pt/

[5] Please be informed that the SCEE was previously appointed by the government through Resolution of the Council of Ministers no. 171/2005, of November 3.

The SCEE has established a reliable electronic structure that guarantees the electronic security of the state and digital authentication of e-transactions between services of the Public Administration and between the state and citizens.

According to this act, the State Electronic Certification Authority (*Entidade de Certificação Electrónica do Estado)* has been defined as the highest level in the hierarchy of the state certification authorities. All other electronic certification authorities of the state will be subordinated to this entity.

This act provides the State Electronic Certification Authority with exclusivity in the issuance of certificates for all other electronic certification authorities. However, it does not issue any certificates to the public.

The SCEE operates independently from other infrastructures of a private or public nature, allowing for the interoperability with the infrastructures that satisfy the requirements necessary for authentication, through adequate technical mechanisms and of the compatibility in terms of certification policies.

This act also grants the National Security Authority (*Autoridade Nacional de Segurança*) with powers to issue accreditations and monitoring the certification authorities of the State (previously a function within the scope of the ITIJ), but not commercial certification authorities.

3.3 e-IDM framework

3.3.1 Main e-Government policies with regard to e-IDM

The eID card

The Citizen's Card is the Portuguese electronic identity card (e-ID) and its purpose is to replace the traditional ID card as well as other cards. It has been available to Portuguese citizens living in the islands of Azores since February 14, 2007 (the first paper ID card was issued on January 2, 1914, to Manuel de Arriaga, at the time the President of the Republic).

It is a smart card with the dimensions of a bank card that provides visual identity authentication with increased security and electronic identity authentication with biometrics (photo and finger print) and electronic signatures.

The development of the Citizen's Card is part of the Government's plan to simplify the administration and to modernize public services. It will replace four cards - Identification Document, Tax Payer's Card, Social Security Card, Health System Card - and will allow multichannel identity authentication, namely in person, through the Internet, or by telephone (with one-time passwords generated with the

card). It allows the citizen to identify himself/herself electronically and to use a legally valid electronic signature from a distance. It is expected to contribute to the deployment of customer-oriented advanced public services.

Please note that due to constitutional limitations, this e-card does not provide a unique ID-number for each citizen. Instead it contains all the numbers included in the mentioned existing cards.

Please note that the e-Card is to be granted to nationals but also to Brazilian citizens covered by the Treaty of Porto Seguro.

So, persons registered in the population register (i.e. Portuguese citizens and the mentioned Brazilian citizens) are issued an e-ID Card that only differs from the traditional card on the design, but not with regard to the content or the technological solution.

The identity card contains a number of data printed on it, specifically: complete name, date and place of birth, date and place of issuance of the card, validity period of the card, parents, marital status, weight, title and number of the card, picture and handwritten signature of the bearer, residence, and National Register number. The card is mandatory, and is issued to any child in the population register from the age of 6. It remains valid for a period of five years.

Please not that no e-IDM is being conceived for legal persons. Information regarding legal entities was traditionally kept on a paper basis, and the authentication of these entities is made within the following structure: (a) referring to the names of legal entities, by the National Company Registry (Registo Nacional de Pessoas Colectivas); (b) after the incorporation, all information is kept in the respective Commercial Registrar department.

From an electronic perspective, the e-Card has a contact circuit containing the same information as the traditional ID-card and includes biometrical data such as photo and finger prints. It also has an electronic signature certificate.

It is an exclusive authentication document and accordingly it does not contain any information of the services of Public Administration that may access the card. As an electronic document, the e-Card allows electronic authentication through IT means and the authentication of electronic documents through the electronic signature.

The Citizen's Card project is coordinated by the Coordination Unit for the Administration Modernization (UCMA)[6] which works in strong partnership with the UMIC for operational matters.

From a physical perspective the citizen's card will have a "smart card" format and will replace the current identity card, taxpayer card, Social Security card and National Health Service user's card.

[6] http://www.ucma.gov.pt/

The front of the card will display the holder's photograph and basic personal details whereas the back will list the numbers under which the holder is registered with the different bodies whose cards the citizen's card combines and replaces. The back will also contain an optical reader and the chip.

From an electronic point of view the card will have a contact chip, with digital certificates (for electronic authentication and signature purposes). The chip may also hold the same information as the physical card itself, together with other data such as the holder's address.

The citizen's card will allow citizens to use a multichannel system in their interactions with public and private services, as follows:

- Internet Channel / Site: the site will provide card-based access to electronic services, in order to give people a privileged channel for dematerialised interaction with public and private services. New online services will be made available, particularly in relation to real estate purchases and changes of address, which will only be possible using strong authentication.

  The site will also use the "single sign-on" concept as part of citizens' relationships with the Public Administration.

- Telephone Channel / Contact Centre: this channel will enable people to obtain services by telephone, using a one-time password (which they will get via the Citizen's Card and its reader system) to identify themselves and authenticate the transaction.

- Personal Contact Channel / Others: the Citizen's Card will interact with other services, particularly those that involve personal contact, thereby implementing the vision of the integration of back-offices and personal reception channels which underlies the "single contact point" concept.

Other systems

Some specific systems need to be mentioned further, since they form the backbone of a substantial number of e-government applications: Online incorporation of companies; Tax - Declarações Electrónicas (E-Declarations); Customs; Social security; Justice; and notary deeds and copies.

Tax - Declarações Electrónicas (E-Declarations)

E-Declarations platform is a web platform that enables the communication of citizens and companies with the Portuguese Tax Department (*Direcção-Geral dos Impostos*).

All electronic forms for tax purposes can be obtained on a specific website set up by the Ministry of Finance (www.dgci.gov.pt) in Declarações Electrónicas.

Tax declarations can be carried out online via the special applications set up for this purpose. Please note that these applications are largely harmonised and similar in appearance and operation.

Also bear in mind that the technical project implemented by Tax Department (*Direcção-Geral dos Impostos*) is similar in all applications and taxes covered by this platform.

E-Declarations can be accessed within the scope of the following taxes and obligations: CIT (Corporate Income Tax); Personal Income Tax; VAT; Annual declarations; Accessory obligations; Collection of tax; Municipalities; Notaries.

The services provided within the referred e-platform are as follows:

The password is granted by the DGITA (*Direcção-Geral dos Serviços de Informática e Apoio aos serviços Tributários e Aduaneiros*) based on the following steps:

- the user accesses the site www.dgci.gov.pt and applies for a password, based on personal data such as the tax number and fiscal domicile;
- the password is issued by the referred entity, printed and sent to the user at the fiscal domicile.

Passwords are stored in a DGITA database using a "one way password" scheme. Communications use the SSL protocol. Electronic Declarations also have an authentication function in the internal system, called Transit NSI - *Trânsito NSI*, and in the external system (*Administração Portuária*).

Customs

Portugal customs adhered to the NCTS-network (New Computerised Transit System), which permits the exchange of electronic data between connected offices. By virtue of Legislative Order no. 42/2003, of October 9 (*Despacho Normativo n.º 42/2003, de 9 de Outubro*), the system whereby all declarations are sent electronically using EDI-based messages (by EDI-FACT or XML), by accessing the website[7] and uploading the communication has been implemented. Please note that the website system does not use advanced electronic signatures, the user is merely provided with a log in identification and a password.

This platform follows the same technical structure of Tax - Declarações Electrónicas (E-Declarations).

Social Security

The Direct Social Security (*Segurança Social Directa*[8]) is a web page through which citizens and companies can communicate with the Social Security.

[7] See http://www.e-financas.gov.pt/de/jsp-dgaiec/main.jsp.

[8] http://www.seg-social.pt/

Companies can access the Direct Social Security through the service of Declaration of Remunerations (with a Single Person Identification Number and key word) that uses the DRI or the DR-Online.

For citizens, adherence to the Direct Social Security is carried out through this site and subsequently the Social Security confirms the access to the address of the citizen, by sending a letter containing a password (the user must change this password when accessing the program for the first time).

The site uses Safe Transactions SSL 128 Bits, with a web-server certificate.

The online social security site includes a high grade (RC4 128 bit, SA 1024 bit) Verisign SSL Web server certificate.

Online incorporation of companies

Decree-Law no. 125/2006, of June 29, establishes a means of incorporating companies through the Internet. This act has been regulated by the Council Order no. 657-C/2006, of June 26.

The adopted regime for incorporating commercial companies or private companies having a commercial form through the Internet may be used by any interested party, be they natural persons or legal entities, represented by the relevant persons in charge, with sufficient powers in the company.

In addition, also lawyers, solicitors and notaries may promote their constitution, certifying the identity, capacity, representation powers and the will of interested parties, using a means of electronic validation of their identity.

Within the scope of this project the following e-IDM regime has been implemented:

The incorporation of companies through this e-Government platform is done by lawyers, solicitors and notaries, after electronic authentication through the use of a digital certificate that proves the professional quality of the user. These certificates may only be used for professional purposes, as evidenced by electronic lists of certificates made available, respectively, by the *Ordem dos Advogados* (Lawyers Bar Association,) the *Câmara dos Solicitadores* (Solicitors Association) and the *Ordem dos Notários* (Notaries Order).

During the online setting up of companies, each applicant must use its qualified electronic signature on the statutes or instrument of constitution of the company, except where the applicant uses hand-written signatures, validated by a lawyer, solicitor or notary.

Justice

In the year 2000, Portugal began the process of introducing an e-justice project, enabling attorneys to file their briefs by electronic means.

Lawyers use an advanced electronic signature in general issued by Multicert-Serviços de Certificação Electrónica, S.A..

As the message is sent by lawyers, the Order in Council no. 337-A/2004 requires that the certificate associated to the electronic signature certifies the professional capacity of the signatory (lawyer or solicitor).

In order to provide lawyers with an appropriate certificate, the Portuguese Bar Association[9] entered into two Protocols in 2003 with Multicert - Serviços de Certificação Electrónica, S.A.[10]: the first for the provision of digital signatures and the second for the provision of MDDE, a solution that combines the issuance of digital signatures and time stamping.

Notarial deeds and copies thereof

Decree-Law no. 66/2005, of 15 of March, set forth a new regime for the transmission and reception of e-documents: in this case, documents have the same value as they would if certificated by the Registry and Notaries. This act has been set out within the scope of the Service Direct Public (Resolution of the Council of Ministers no. 156/2000, of 16 of November, and Decree-Law no. 12/2001, of 25 of January). Furthermore, this act also aims to widen the scope of the request for the issuance of said certificates to other entities, such as lawyers and solicitors.

In relation to the e-IDM system, the necessary procedures for the implementation of the mentioned act must be defined by the general director of the Registry and Notary (*Director-Geral do Registo e Notariado*), by protocol between the DGRN (*Direcção-Geral dos Registos e Notariado*) and the Notaries' Bar Association and by protocol between the DGRN, Notaries' Bar Association and the Lawyer's Bar Association and the Chamber of the Solicitors.

Citizen's Portal (Portal do Cidadão)

The Citizen's Portal (http://www.portaldocidadao.pt) is a web platform developed by UMIC that mainly centralises information to be provided to citizens about all matter of Public Administration.

All Internet users may access publicly available information.

[9] http://www.oa.pt/

[10] http://www.multicert.pt/

The provision of other services requires the registration of the user, through the following steps. On the site http://www.portaldocidadao.pt, the user access to *Novo Registo* area and then has to follow the three steps rule: Inscription of personal data; Subscription of Services; Confirmation of the Registration.

Strictly speaking, for registration purposes the Citizen's Portal does not ask for any information which would only be accessible to Portuguese nationals; the registration is open-free. However, foreign citizens can only use the Citizen's portal (outside the scope of the provision of general information) in a limited number of situations, such as the case of a foreign citizen requiring the certification of a real estate property. The use of this portal to provide specific services to foreign citizens is not the key objective.

Please note that after having inscribed the respective data, the system send the user by an email containing a link that the user must access in order to get the registration. Logging on to the system thereafter uses a username/password system.

3.3.2 Legal framework

The legal framework to be considered is the following:

eID Card

The Resolution of the Council of Ministers no. 77/2001, of July 5, proposed the e-Card. This act has also created a working group in charge of providing the plan of action of the implementation of the e-Card. This act must be regulated by a regulation, which should be introduced early next year.

e-Passport

The Resolution of the Council of Ministers no. 154/2005, of September 30, sets out the guidelines for the implementation of the Portuguese e-Passport. These guidelines have been fulfilled by the Decree-Law no. 138/2006, of July 26, and the Decree-Law no. 139/2006, of July 26, and the Resolution of the Council of Ministers no. 1245/2006, of August 21.

Justice

The Decree-Law no. 183/2000, of August 10, amended article 150 of the Code of Civil Procedure. This provision allows the possibility of presentation in court of acts of the parties in digital support or by sending them by e-mail. Order In Council no. 1178-E/2000, of December 15, sets out that in those cases, digital signatures issued by a accredited certification authority meeting the requirements enacted by the Decree no. 290-D/99 must be used.

Through Decree-Law no. 324/2003, of December 27, that amended article 150 of the Code of Civil Procedure, that came into force on January 1, 2004, the Portuguese legal framework accepted that all acts to be performed by the parties[11] within legal proceedings may be sent to court by "e-mail with an advanced electronic signature". It has also been stated that the date of the act is the one of the emission, when duly certified[12].

Although some discussions within the scope of the implementation of this e-IDM system, the use of advanced electronic signatures has never been challenged, which is one of the requirements to be met when the parties wish to use e-mail. A second requirement is the use of time stamps as evidence of the time when the communication was sent.

Please note that this time stamp is not, however, a requirement of validity or effectiveness of the act, but only evidence of the date of the issuance of the act.

This chronological validation requirement is equally applicable in the cases of notices between lawyers of the parties.

3.3.3 Technical aspects

The most relevant public eID Token in Portugal are the e-Card and the e-Passport. When also considering solutions with a limited scope of practice, the project carried out within the scope of e-Justice is the oldest and most tested project. We therefore consider that we should make a detailed report of these projects below.

Electronic card (e-Card)

From an electronic perspective, the e-Card has a contact circuit containing the same information as the traditional ID-card and includes biometrical data such as photo and finger prints. It also has a qualified electronic signature certificate, an authentication certificate and the EMV 4.1/MasterCard Chip Authentication Program (CAP) that generates one-time passwords and message digests.

The identity card itself is a Gemalto Cryptoflex JavaCard 64K, equipped with a 16 bit microcontroller (Infineon SLE66CX322P) and an additional crypto processor (for RSA and DES computations). The

[11] The Order In Council no. 337-A/2004 also establishes an information duty for the judicial secretariat, when the file is sent by e-mail, to quote the defended indicating the e-mail of the lawyers of the claimant.

[12] Accordingly the Order in Council of the Ministry of Justice would regulate this article. This act has been regulated by Order in Council no 337-A/2004, of 31 March. However, the wording of this regulation raised some doubts and in April 1, 2004, new rules concerning the delivery of procedural acts and notices were set forth in Order In Council no. 337-A/2004, of 31 of March.

card has ROM, EEPROM and RAM. A Java Applet implements the Chip Authentication Program (CAP). The chip contains two PKI key pairs and certificates (for authentication and signature respectively, no encryption key), one PKI key pair for the card itself (without certificate) and a CVC root public key (to authenticate who can access the private data on the chip – for instance, the police).

With regard to specific hardware, the card will be read by a wide range of card readers.

A specific middleware to be used together with the card will be developed for the Portuguese government by Zetes. This middleware is a low-level API that bridges between the application itself (or high-level API) and the device actually performing the cryptographic operations (the e-ID card, in conjunction with the compatible card readers).

High-level APIs will be developed by Multicert and will constitute the application level interface for e-Government applications that use cryptographic operations from the smartcard (qualified digital signature and authentication) and PKI related services (timestamping, LDAP validation, OCSP validation).

An e-ID application development kit will be available online. **Development cards that are functionally equivalent to actual e-ID cards will also be available.**

The compliance of the e-ID with the requirements of Annex III of the European Directive 1999/93/EC has not yet been officially assessed. It is therefore not entirely certain whether it can be considered a "SSCD" in accordance with the Directive. Nevertheless very few people in Portugal will have any doubt that the e-ID enables them to create "qualified" electronic signatures.

The "qualified" certificates on the e-ID are issued by INCM (Portuguese Mint). The certificates follow the X509v3 model.

The description of the fields of the signature certificate is contained in the table below:

e-ID citizen Signature Certificate					
Base Certificate	OID	Include	Critical	Value	
Certificate					
SignatureAlgorithm					
Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	X509v3
SerialNumber		X		Sequential and unique, provided by the CA	
Signature		X		Sha-1WithRSAEncryption	
Validity					

NotBefore		X		Key Generation Process Date/Time	
NotAfter		X		Key Generation Process Date/Time + 5 years	
SubjectPublicKeyInfo		X		RSA 1024	
Issuer					
DistinguishedName		X		CN = Cartão de Cidadão – CA AssinaturaQ «CA number», OU = Assinatura Digital Qualificada do Cidadão, OU = Cidadãos, O = Cartão de Cidadão, C = PT	
Subject			Required		
countryName	{ id-at-6 }		YES	provided by Identification Registry	Dynamic
commonName	{ id-at-3 }		YES	Concatenation of surname, givenName and the purpose of the certificate “(Signature)”	Dynamic
Surname	{ id-at-4 }		YES	provided by IR	Dynamic
GivenName	{ id-at-42 }		YES	provided by IR	Dynamic
serialNumber	{ id-at-5 }		YES	provided by IR (Subject’s Identity card number)	Dynamic
Standard Extensions	OID	Include	Critical	Value	
CertificatePolicies	{id-ce 32}	X	FALSE	N/a	
policyIdentifier		X		tbd	Fixed
policyQualifierrs				N/a	
policyQualifierId	{ id-qt-1 }	X		CPS	Fixed
Qualifier		X		http://www.cartaodocidadao.pt/public/pol/cc_ca_assq_cps_001.html	Fixed
Qualified Certificate Statement					
qcStatement	{ id-etsi-qcs 1 }	X			
KeyUsage	{id-ce 15}	X	TRUE	N/a	
nonRepudiation				Set	Fixed
Digital Signature				Set	Fixed
authorityKeyIdentifier	{id-ce 35}	X	FALSE		
KeyIdentifier		X		SHA-1 Hash	
cRLDistributionPoints	{id-ce 31}	X	FALSE		
distributionPoint					
FullName		X		http://www.cartaodocidadao.pt/public/crl/cc_ca_assq_crl_xxxxxxxx.crl	Fixed
NetscapeCertType		X	FALSE		
	2.16.840.1.113730.1.1			sMime	Fixed
Private Extensions	OID	Include	Critical	Value	
AuthorityInfoAccess	{id-pe 1}	X	FALSE		
accessMethod	{ id-ad-2 }	X			

accessLocation		X		http://www.cartaodocidadao.pt/public/cert/cc_ca_assq_xxxx.crt	Issuing CA certificate
accessMethod	{ id-ad-1 }	X			
accessLocation		X		http://www.cartaodocidadao.pt/public/serv/ocsp	
Subject Directory Attributes		X	FALSE		
				Subject's date of birth	
Freshest CRL		X	FALSE		
				http://www.cartaodocidadao.pt/public/crl/cc_ca_assq_crl_00000010_delta.crl	Delta CRL URL

The e-ID Citizen CA belongs to a broader domain of CAs of the Portuguese State. The Portuguese State has set up a CA hierarchy with the Portuguese Root CA (ECEE) at the top. The ECEE certifies the private keys of the CAs in the government domain including the e-ID Citizen CA.

At the top the e-ID hierarchy consists of a combination of a three-layered model:

- ECEE (root CA of the Portuguese State)
- e-ID Citizen CA ("root" CA for the Portuguese Citizen e-ID)
- Signature CA Authentication CA

(only issues qualified signature certificates) (only issues authentication certificates).

For the validation of electronic signatures created by means of the e-ID both Certificate Revocation Lists (CRLs) or the Online Certificate Status Protocol (OCSP) can be used.

e-Passport

E-Passports contain the following:

- Golden print of the Portuguese Coat-of-arms and the information concerning the type of passport.
- The passport will feature a logo indicating that this is an electronic passport (chip), in the lower left side.
- Invisible ink imprint, visible under an ultraviolet light, of scattered elements representing the Portuguese Republic, the European Union and that this is an electronic document.
- Security paper coated with polymeric material.
- Personal data are laser engraved, and some fields have a touch-sensitive embossing.
- Kinegram ® - Element presenting motives that change colour.
- Microperforated photograph: Laser-microperforated photograph of passport holder.

The Portuguese e-passport complies with ICAO's "PKI for Machine Readable Travel Documents offering ICC Read-Only Access".

In order to develop interoperable implementations of X.509 v3 systems for ICAO use, it is necessary to specify a profile for use of the X.509 v3 extensions tailored for ICAO purposes.

Those States conforming to the ICAO specification must issue certificates that conform to the two following profiles. All security objects must be produced in Distinguished Encoding Rule DER format to preserve the integrity of the signatures within them.

The profiles use the following terminology for each of the fields in the X.509 certificate:

m – mandatory (the field MUST be present)

o – optional (the field MAY be present)

c – critical (the extension is marked critical, receiving applications MUST be able to process this extension).

ECN PEP CA Certificate Profile **Cerificate Component**		**Section in RFC 3280**	**Value**	**Field Type**	**Comments**
tbsCertificate	**Version**	4.1.2.1	v3	m	
	Serial Number	4.1.2.2	<assigned by the CA to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.5	m	value MUST match the OID in signatureAlgorithm (below)
	Issuer	4.1.2.4		m	see document [4] for last approved CSCA DN
	Country (C)		"PT"		example - see document [4] for last approved DN
	Organization (O)		"Republica Portuguesa – ECN PEP Raiz"		example - see document [4] for last approved DN
	Organization Unit (OU)		"ICAO MRTD PKI – Portuguese Republic CSCA"		example - see document [4] for last approved DN
	Common Name (CN)		"Republica Portuguesa – ECN PEP Raiz"		example - see document [4] for last approved DN
	Validity	4.1.2.5		m	Implementations MUST specify using UTC time until 2049, from then on using GeneralisedTime
	Not Before		<issuing date>		
	Not After		<issuing date + 3.100 days>		As in [6]
	Subject	4.1.2.6	<same as Issuer Field>	m	When the subject is a CA, the subject field MUST be populated with a non-empty DN matching the contents of the Issuer field.
	Subject Public Key Info	4.1.2.7		m	used to carry the public key and identify the algorithm with wich the key is used (e.g., RSA, DSA or Diffie-Hellman)

algorithm		1.2.840.113549.1.1.1		The OID rsaEncryption identifies RSA public keys. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} The rsaEncryption OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have ASN.1 type NULL for this algorithm identifier. [5]
subjectPublicKey		<Subject Public Key with modulus *n* of 4096 bits>		
X.509v3 Extensions	4.1.2.9		m	
Authority Key Identifier	4.2.1.1		o	The optional "Authority Key Identifier" extension was choosed to use.
keyIdentifier		<The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	m	
authorityCertIssuer		<not used>	o	
authorityCertSerialNumber		<not used>	o	
Subject Key Identifier	4.2.1.2	<The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	m	
Key Usage	4.2.1.3		mc	This extension is marked CRITICAL
Digital Signature		"0" selected		

Non Repudiation		“0” selected		
Key Encipherment		“0” selected		
Data Encipherment		“0” selected		
Key Agreement		“0” selected		
Key Certificate Signature		“1” Selected		
CRL Signature		“1” Selected		
Encipher Only		“0” selected		
Decipher Only		“0” selected		
Private Key Usage Period	4.2.1.4	<not used>	o	
Certificate Policies	4.2.1.5		o	The optional "Certificate Policies" extension was choosed to use.
policyIdentifier		2.16.620.1.1.1.3.1	m	MAI Certificate Policy Identifier
policyQualifiers		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://www.pep.pt/cps/	o	OID value: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) OID description: "The CPS Pointer qualifier contains a pointer to a Certification Practice Statement (CPS) published by the CA. The pointer is in the form of a URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)

	Basic Constraints	4.2.1.10		mc	This extension is marked CRITICAL
	CA		TRUE		
	PathLenConstraint		0		New CSCA certificate.
	CRLDistributionPoints	4.2.1.14	<not used>	o	Choose not to use.
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.5	m	MUST contain the same OID algorithm identifier as the signature field in the sequence tbsCertificate. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } [5]
	Signature Value	4.1.1.3	<contains digital signature issued by the CA>	m	By generating this signature, a CA certifies the binding between the public key material and the subject of the certificate.

ECD Certificate Profile **Cerificate Component**		**Section in RFC 3280**	**Value**	**Field Type**	**Comments**
tbsCertificate	**Version**	4.1.2.1	v3	m	
	Serial Number	4.1.2.2	<assigned by the CA to each certificate>	m	
	Signature	4.1.2.3	1.2.840.113549.1.1.5	m	value MUST match the OID in signatureAlgorithm (below)
	Issuer	4.1.2.4		m	see document [4] for last approved CSCA DN
	Country (C)		“PT”		example - see document [4] for last approved DN
	Organization (O)		“Republica Portuguesa – ECN PEP Raiz”		example - see document [4] for last approved DN
	Organization Unit (OU)		"ICAO MRTD PKI – Portuguese Republic CSCA"		example - see document [4] for last approved DN
	Common Name (CN)		“Republica Portuguesa – ECN PEP Raiz”		example - see document [4] for last approved DN
	Validity	4.1.2.5		m	Implementations MUST specify using UTC time until 2049, from then on using GeneralisedTime
	Not Before		<issuing date>		
	Not After		<issuing date + 1.900 days>		As in [6]
	Subject	4.1.2.6		m	see document [4] for last approved Document Signer DN
	Country (C)		“PT”		example - see document [4] for last approved DN

Organization (O)		“Republica Portuguesa”		example - see document [4] for last approved DN
Organization Unit (OU)		"ICAO MRTD – Portuguese Republic DS certificate"		example - see document [4] for last approved DN
Common Name (CN)		“ICAO MRTD ECD <nnnnnnnnn>”		example - see document [4] for last approved DN
Subject Public Key Info	4.1.2.7		m	used to carry the public key and identify the algorithm with wich the key is used (e.g., RSA, DSA or Diffie-Hellman)
algorithm		1.2.840.113549.1.1.1		The OID rsaEncryption identifies RSA public keys. pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 } rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1} The rsaEncryption OID is intended to be used in the algorithm field of a value of type AlgorithmIdentifier. The parameters field MUST have ASN.1 type NULL for this algorithm identifier. [5]
subjectPublicKey		<Subject Public Key with modulus *n* of 2048 bits>		
X.509v3 Extensions	4.1.2.9		m	
Authority Key Identifier	4.2.1.1		m	
keyIdentifier		<The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjec key identifier in the issuer's certificate (excluding the tag, length, and number of unused bits)>	m	
authorityCertIssuer		<not used>	o	

authorityCertSerialNumber		<not used>	o	
Subject Key Identifier	4.2.1.2	<The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits)>	o	The optional "Subject Key Identifier" extension was choosed to use.
Key Usage	4.2.1.3		mc	This extension is marked CRITICAL
Digital Signature		"1" selected		
Non Repudiation		"0" selected		
Key Encipherment		"0" selected		
Data Encipherment		"0" selected		
Key Agreement		"0" selected		
Key Certificate Signature		"0" selected		
CRL Signature		"0" selected		
Encipher Only		"0" selected		
Decipher Only		"0" selected		
Private Key Usage Period	4.2.1.4	<not used>	o	
Certificate Policies	4.2.1.5		o	The optional "Certificate Policies" extension was choosed to use.
policyIdentif		2.16.620.1.1.1.3.1		MAI Certificate Policy Identifier

	ier			m	
	policyQualifier		policyQualifierID: 1.3.6.1.5.5.7.2.1 cPSuri: http://www.pep.pt/cps/	o	OID value: 1.3.6.1.5.5.7.2.1 (id-qt-cps PKIX CPS Pointer Qualifier) OID description: "The CPS Pointer qualifier contains a pointer to a Certification Practice Statement (CPS) published by the CA. The pointer is in the form of a URI." (http://www.alvestrand.no/objectid/submissions/1.3.6.1.5.5.7.2.1.html)
	CRLDistributionPoints	4.2.1.14	<not used>	o	Choose not to use, since ICAO mandates that all CRLDistributionPoints fields SHOULD NOT be populated [1]
	Signature Algorithm	4.1.1.2	1.2.840.113549.1.1.5	m	MUST contain the same OID algorithm identifier as the signature field in the sequence tbsCertificate. sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 } [5]
	Signature Value	4.1.1.3	<contains digital signature issued by the CA>	m	By generating this signature, a CA certifies the binding between the public key material and the subject of the certificate.

ECD certificates are used by the Portuguese Government to sign Document Security Objects of Machine Readable Travel Documents (e-Passport). These certificates are also used by ICAO and receiving States for validating the authenticity of digitally stored MRTD data.

Justice

The Portuguese Bar Association is the Registration Authority (RA) for all the digital certificates that are issued to certify the professional quality of the signatory. Once identified by the RA, the lawyer generates the key pairs and the RA sends a Certificate Request message to the CA (Multicert) containing the subject's DN:

CN = «name of the lawyer» - Ordem dos Advogados

OU = Personal ID

OU = Nome profissional de Advogado - «number ID of the lawyer»

OU = «name of the lawyer company (optional)» or "Advogado"

OU = Corporate

OU = Ordem dos Advogados - RA

O = MULTICERT-CA

C = PT

The lawyers' digital certificates are always issued for one year.

On 15 September 2003 the MDDE (*Marca do Dia Electrónica*) Electronic Postmark (EPM) service was launched– the first EPM paid service worldwide to be used on a daily basis by Portuguese lawyers –, protecting the integrity of electronic mail (or data), through the use of auditable time stamps, digital signatures and hash codes. These postmarks enable the relevant parties to verify the authenticity of the contents of the e-mail messages and provide evidence to support the non-repudiation of electronic transactions.

The initial version of the MDDE electronic postmark, is targeted at lawyers, members of the Portuguese Lawyers Association, who usually send documents to the courts by secure e-mail, and have started to use the MDDE service in order to add non-repudiation evidence of the date and time when the email was sent. The MDDE EPM service:

- digitally signs and adds an electronic stamp on electronic transactions such as e-mail messages,
- adds non-repudiation evidence of the time and date when the email was sent (following IETF/PKIX RFC 3161 [ACPZ01] and the European Electronic Signature Standardization Initiative (EESSI) "Time Stamping profile" [ETSI02]) – the MDDE EPM employs a secure time stamping clock, synchronized to the Observatório Astronómico de Lisboa (OAL), the official Portuguese source of time.

- assures the relevant parties of the reliability of the contents,
- provides irrefutable evidence that the message was actually sent (since the MDDE postmark is attached to the original e-mail message at CTT's SMTP gateway, only once the e-mail message has effectively been sent from the sender's computer – this is an unique feature of CTT's electronic postmark), and
- works with every e-mail client software.

The electronic postmark (EPM) service was launched (marketing and selling it as the electronic counterpart of the physical registered letter service) on the 15th September 2003, and by the end of October 2006, 10.337 lawyers were using the service and over 450.000 postmarked e-mail messages have been sent. Around 1.000 messages a day are postmarked (each postmark costs 0.25 €), and 8 to 10 new users are signing up daily for the service (25 € yearly service fee).

The security services provider Multicert, a joint venture of the Portuguese Postal services along with Portugal Telecom, Portugal Mint and SIBS, developed the MDDE EPM and is operating the Portuguese Postal service. This is backed by a PKI infrastructure (that supports PKCS#7 digital signatures, timestamps and OCSP – Online Certificate Status Protocol – validation) that assures authentication, integrity and non-repudiation for all the parties involved.

3.3.4 Organisational aspects

E-Cards and e-Passport project are just starting in Portugal. In the future the solutions provided in the said cards (as well as in lawyers document) will enable users to authenticate themselves in a variety of electronic environments. However, no effective solutions have been yet implemented with the use of said cards (and namely as we previously mentioned, other e-Government platforms rely in log-in and password systems).

Accordingly, we are not able to provide any information regarding the effective use of such devices, but obviously that the verification of data and the use of the e-Card electronic signature in order to bind the user to a certain declaration or the execution of agreement is to be expected.

3.4 Interoperability

As stated in the introduction above, the Portuguese eID card and e-Passport are only available and issued to a limited number of permanent residents (in the case of e-Card, only in Azores).

In the future, it is expected that these e-IDM system may interoperate in many platforms and different systems of information.

Please note that according to public authorities the public platform of interoperability is "being implemented", and that no information is being provided in relation to assuring interoperability with

foreign cards, due to the fact that e-IDM and other e-Government platforms are set out to start more effectively in the near future.

3.5 e-IDM Applications

Please see detailed explanation above.

3.6 Future trends/expectations

It should be noted as a global remark that Portugal has no specific regulations with regard to the process of authentication in general. Portugal has a long tradition on the digital/ electronic signatures, as Portugal has enacted a legal framework in August 1999 (Decree-Law no. 290-D/99).

Although the lack of regulation of the Decree-Law no. 290-D/99 lead to some constraints on the uptake of the use of e-signatures, these e-devices are now being seen as the technical solutions that e-government and related e-platforms should require to identify the users.

The Decree-Law no. 290-D/99 has been amended by the Decree-Law n° 62/2003 that faithfully transposes the provisions of the e-Signatures Directive, but does not apply to authentication as such. Additionally, there are many projects that do not rely on secure authentication schemes.

While all major e-IDM public projects using secure authentication devices are in a start-up phase, and while there are several other projects relying on username/password solutions already on a stable and long roll-out phase, in all formal contacts that we had with Portuguese public authorities it has been referred to us that future trends go in the direction of adopting authentication schemes relying on the eID card and to create secure technical solutions in order to allow a wide interoperability of such devices in many networks.

3.7 Assessment

The Portuguese approach has a number of advantages and disadvantages, which can be briefly summarised as follows.

3.7.1 Advantages:

- Major e-IDM processes are in a start-up phase. However, Portugal government has providing a strong focus in publicising technological solutions (in a wider scope, by the launch of the Technological Plan) and all these projects might be seen as integrating an environment sustained by macro-political strategies.

3.7.2 Disadvantages:

- All of the e-projects that touch or focus the economical system (tax, customs) do not rely on secure e-IDMs. Furthermore, these solutions are those that have a more consistent and long use and we may preview some difficulties in the swap of the e-IDM system.

- The most relevant e-IDM Portuguese system is largely built for Portuguese nationals (although it also applies to Brazilian citizens covered by the Treaty of Porto Seguro) and no cross-border interoperability solutions are being considered.

- There is a lack of applications and the relative rarity of card readers results in a limited use of the cards electronic features in practice.