IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE GREECE

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 Greek 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

Despite political commitment to eGovernment, eGovernment is still in its infancy stage in Greece. Thus, no large-scale electronic identity scheme has been developed yet, with the exception of the PKI infrastructure for public servants, which is being developed in the framework of the Syzefxis project, and other specific e-government applications, such as Taxisnet, KEP etc., in which electronic identities play a role.

More particularly, the most prominent system is the one implemented by the project Syzefxis, which will introduce PKI based identities to civil servants (http://www.syzefxis.gov.gr). Syzefxis is a project establishing a network infrastructure which would be used for eGovernment and eSignatures in the public sector.

The main goals of the project are the improvement of public services' functions and the provision of the appropriate public key infrastructure for the public sector and, also the provision of an eLearning platform accessible by civil servants. In the framework of the project, 50,000 smart cards and 10,000 card readers will be distributed and SSL certificates will be provided to certify government servers. Smart cards encompass two digital certificates, one for electronic signing and the second for cryptography.

Other e-government applications include:

i) the TAXISnet which provides electronic services to citizens (http://www.taxisnet.gr), such as the electronic submission of tax declaration, of annual use;

ii) the Social Insurance Institution which provides for the declaration of social contributions for employees (http://www.ika.gr);

iii) the Citizens' Bureaus offering a variety of electronic services to citizens (http://www.kep.gov.gr); and

iv) the Courts of Athens, Piraeus and Thessaloniki (http://www.protodikeio-ath.gr http://www.protodikeio-pir.gr http://www.protodikeio-thes.gr), providing online services to lawyers and citizens also.

It is notable that the above applications do not rely on electronic signatures, and authentication takes place strictly based on username and password after registration of a user.

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

eIDM system	Potential user base	Actual penetration	Actual use
PKI system	50,000 public servants	Still in development	No public statistics are available
TAXISnet	The taxpayers	At least 10% of the taxpayers	No public statistics are available
Social Insurance Institution (IKA)	The employees	-//-	No public statistics are available
KEP	A great number of Citizens	-//-	No public statistics are available
Courts of Athens, Piraeus, Thessaloniki	30,000 lawyers and many citizens	Under construction	No public statistics are available

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

As a rule, the incentives for eGovernment projects in Greece come from national eGovernment bodies, which undertake the coordination of activities that are implemented by various administration bodies of all levels. Regional and local administration authorities seem, however, to be also interested in developing eGovernment projects for their citizens.

In particular, state administration in Greece is exercised by central and local government. On the basis of the principle of decentralization, there are 13 administrative regions established, which are governed by the Region Secretary and the Region Council as the main organs of regions[3]. Regarding local administration, it should be mentioned that it is organized in two levels, i.e. the prefectures (54) and the local municipalities[4].

Main actors that define eGovernment priorities and actions are the Information Technology Committee and the Ministry of Interior, Public Administration with its specific department for

[3] See S. Lytras, in: Gerontas/Lytras/Pavlopoulos/Siouti/Flogaitis, *Administrative Law*, Athens 2004 (in Greek), p. 169 et seq.

[4] See S. Flogaitis, in Gerontas/Lytras/Pavlopoulos/Siouti/Flogaitis, *Administrative Law*, op. cit., p. 175 et seq.

eGovernment, which has been recently established; whereas sector specific eGovernment projects are implemented by individual government bodies.

The Information Technology Committee was established 2004[5] and is operating as a common platform for planning and development of Information Technology[6]. Its task is to coordinate and monitor the initiatives of public institutions aiming to promote the use of new technologies and eGovernment. In particular, the Committee is responsible for developing Greece's Digital Strategy for the period 2006-2013, as well as for the coordination of the public institutions' actions and interventions concerning the use of new technologies and e-governance[7].

The Ministry of the Interior, Public Administration and Decentralization is formally assigned with the responsibility for the development of eGovernment in Greece. Within the Ministry, the General Secretariat for Public Administration and eGovernment was established (by the amendment of the existing Secretariat for Public Administration) by Article 24 (1) of Law 3200/2003, with main responsibility to tackle eGovernment issues[8]. The role of this body is central for the development of eGovernment in Greece.

Recently, a consultative body for eGovernment has been established by the Ministry of the Interior, Public Administration and Decentralization, i.e. the eGovernment Forum[9]. The creation of this institution was an initiative of the General Secretariat for Public Administration and eGovernment and it will be operated by the Information Society S.A. in the framework of the Project "Information Society".

The eGovernment Forum has as its tasks:

i) to activate the business community in order to produce relevant know-how and submit proposals for the use of ICT in their transactions with public administration;

ii) to exploit the know-how of Greek and foreign academic institutions; and

iii) to promote and utilize international experience and practice with the participation of experts in eGovernment issues.

Furthermore, the strategic planning for ICT is an issue of responsibility of the Special Secretariat of Digital Planning[10] (renamed from the former Special Secretariat for the Information Society), which was formed on December 2000[11], operating under the Ministry of Economy and Finance. Its task is to plan and supervise the operational programme of the Information Society (OPIS)[12], including actions and proposals for issues related to the individual strategy of the country and for the promotion of information technology and digital technologies.

[5] Ministerial Act Nr. 14 of 28.6.2004, Government Gazette A/116, 29.6.2004.

[6] See http://www.infosoc.gr/infosoc/en-UK/sthnellada/committee/default.htm

[7] See op. cit.

[8] See http://www.gspa.gr

[9] See Government Gazette B/1517/16.10.2006.

[10] See http://www.infosoc.gr/infosoc/en-UK/sthnellada/operators/Special_secretariat/default.htm

[11] See Official Gazette 1502 of 8.12.2000.

[12] See http://www.infosoc.gr/infosoc/en-UK/epktp/

The implementation mechanisms of OPIS are the Special Management Service of the Operational Programme for the Information Society[13], the Observatory for the Information Society, which is an independent Private Law Body Corporate[14] and the Information Society S.A.[15], which is a state-owned company, providing support to projects of OPIS.

3.2.2 National eGovernment cooperation and coordination

Cooperation between central, regional and local authorities is attained mainly by horizontal projects such as Syzefxis, which is a project of the Ministry of the Interior, Public Administration and Decentralization and is implemented by the General Secretariat for Public Administration and eGovernment. The latter plays an important role in the coordination of eGovernment activities undertaken by public institutions.

It seems, however, that a cooperation mechanism between the General Secretariat and other bodies, such as the Information Technology Committee, is needed. Although the creation of the eGovernment Forum will contribute to the development of new ideas, it does not have a coordinating role as its task, so that the lack of coordination is still evident.

Information concerning eGovernment projects is provided by the websites of the General Secretariat for Public Administration and eGovernment, the Information Technology Committee and the Information Society S.A. Specific projects, such as the Syzefxis project, provide also information in their websites. Also, a private website, created by the e-Government Laboratory of the University of Athens (http://www.e-gov.gr/), provides specific information and is used as a forum for the exchange of views.

3.2.3 Traditional identity resources

Identification towards Greek eGovernment services traditionally relied on the mandatory paper based identity card in conjunction with the information contained in population registers held by municipalities. There are currently no concrete plans for an eID card. It is notable that in Greece there exists no central national register like in other EU Member States, but municipalities and communes keep (electronic) registers of inhabitants, which contain information on the personal and family status.

[13] See http://www.infosoc.gr/infosoc/en-UK/sthnellada/operators/eyd/

[14] The Observatory for the Information Society was founded by Law 3059/2002 (Government Gazette • 241/11.10.2002) and is supervised by the Ministers of National Economy and Finance, of Internal Affairs, Public Administration and Decentralization. See http://www.infosoc.gr/infosoc/en-UK/sthnellada/operators/observation/

[15] See http://www.infosoc.gr/infosoc/en-UK/sthnellada/operators/KtP_SA/

These issue certificates of birth (and of family status) for every registered citizen, which are then used for the issuance of identity cards.

It is an obligation for every Greek citizen over 12 years of age, living permanently or temporarily in Greece, to have an identity card issued by a police station in the area of their domicile. Non-nationals are provided with a permit of stay from the administrative region of their domicile.

The identity card contains a number of data printed on it, specifically: surname, first name, father's surname and mother's name (in Greek and in Latin characters), date of birth and place of birth, height, nationality, municipality of registration, municipal roll serial number and blood type (optional)[16]. The card is mandatory. It remains valid until changes in the marital status occur.

Information regarding legal entities was traditionally kept in paper based trade registers, which were maintained in Court Registers and the Departments of the Ministry of Commerce, whereas in case of public limited and limited liability companies the relevant acts were also published in the Government Gazette. In 6th December 2005, Law 3419[17] was published, which provided for an electronic General Register for legal persons, including most companies' forms, and for natural persons, which are merchants. However, this electronic Register did not start its functioning yet.

Thus, the traditional identity infrastructure can be said to consist of locally kept paper registers for natural persons, and of a centrally maintained electronic register for legal persons which will replace the existing paper based trade registers.

[16] It is notable that the previous regulation on IDs provided that religion and husband's name for women were also included in the IDs' data, but the Data Protection Authority held that the processing of such data in not compatible with the law on data protection (Decision No 510/200). The Council of State dismissed appeals against this decision and held also the processing is unlawful; see I. Iglezakis, *Sensitive Personal Data*, 2004, p. 154 et seq. (in Greek).

[17] Government Gazette A/297, 6.12.2005.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Syzefxis

In the framework of the Syzefxis project 50,000 smart cards and 10,000 card readers will be provided to public servants, but also 2,000 SSL certificates will be issued that would certify government servers. The objective of the development of PKI infrastructure in the public sector is to enable public servants to access electronic services, such as the Citizen Service Centres' information system and portal, the Syzefxis portal, etc. The implementation of this project will result to widespread the use of electronic signatures in the public administration (G2G) and also in eGovernment interactions. Similar projects oriented towards citizens will be also carried out in the future[18].

The infrastructure established by Syzefxis is used in a series of applications. For instance, the Deposit and Loans Fund is interconnected with the Citizens Service Centres, so that a certificate of interest loan for tax usage could be issued. Furthermore, many applications, which are different Ministries, are implemented though the Syzefxis project. Also information systems of the regions are implemented, e.g. the health information systems of East Macedonia, of Macedonia-Thrace etc., and systems of munipalities, such as the vehicle management of the Municipality of Karditsa etc.

Other systems[19]

TAXISnet

The TAXISnet system provides services to individual and corporate taxpayers, including through electronic submission of income tax forms, personalised electronic notification of the results of the tax return clearance process, electronic issuing of certificates by fax, electronic submission of VAT forms, and payment via banking system services[20].

In order to use the system, users of the TAXISnet system can sign up through a secure server, following a five-steps procedure; namely, the user has to enter his Tax Identification number, then choose between natural or legal person, fill in his personal information, including his identity card or passport number, and providing his e-mail address, etc. Accordingly, a password is sent to the e-mail

[18] The Hermes Project, which has not been awarded yet, will provide 300,000 smart cards to citizen and business for their transactions with public authorities.

[19] See I. Iglezakis, in: *Cyberlaw in Hellas*, 2005, p. 25

[20] See http://www.observatory.gr

address chosen by the user, who can use it to sign in the TAXISnet system once he has received the password.

The Social Insurance Institution's website

The Social Insurance Institution's (IKA) website provides employers the possibility to submit online periodical statements concerning social contributions that are payable to IKA. Users of the system have to sign up by providing their e-mail address, where a message is send, containing an activation link and a temporary password. After the link is activated, the user has to enter the password and proceed to enter information about his identity and the type of service he/she wants to make use of. Consequently, an e-mail message is sent to the user with the user name and password (PIN) and another with the PUK. The PIN and PUK are unique for every user and they are used in order to provide security of transactions.

Citizen Service Centre

The website of the Citizen Service Centre (http://www.kep.gov.gr) is the official site of administrative one-stop shops (physical locations) where citizens can have access to public service information and to a number of standardised administrative procedures[21]. The website offers the possibility to registered users of submitting applications online, which are dealt with by individual centres.

The Citizen Service Centres are spread around the country and provide a great number of services to citizens. This is performed through a specific network and software ("e-kep" platform), which supports the use of certified digital signature and enables real time on-line transactions between citizens and public administration.

Users that want to file an online application, have to sign-up, and this is done by typing of personal and identity information (including name, address, ID card number and tax number). An account number and an activation link is sent to the e-mail address chosen and the user has to activate his account, which is reached every time with the use of user name and account number.

Foreigners can register in Citizen Service Centres, since the ID card number and tax number is not mandatory for registration.

[21] See http://www.observatory.gr

Courts of Athens, Piraeus and Thessaloniki

The three major Courts of First Instance, i.e. Athens, Piraeus and Thessaloniki, have created an information system for the electronic filing of lawsuits, provision of information on lawsuits and filing of applications for the issuance of certificates from Courts. Access is granted mainly to lawyers of the corresponding Bar Association, who are given a user name and a password (no electronic signatures are used), but also other persons could register and gain access to certain services (not the filing of lawsuits and information on litigation).

Authentication policies

There is no official authentication policy in Greece that defines a hierarchy of the different authentication systems in use. However, from existing applications we can deduce a formal hierarchy for authentication:

Level	Registration citizen identity	Authentication citizen identity	Applications
0	None	None	Public information and services
1	On line by entering the identity card number and other personal data + send-out of a confirmation e-mail with activation to an e-mail address indicated by the citizen	By assigned user number in combination with a password chosen by the user	Information/services of average sensitivity
2	Physical identification at the Syzefxis contractors	Authentication certificate on the smart card	Services requiring an electronic signature

Thus, there are two level of authentication above public access: basic username/password (after registration using official register numbers) and use of the smart card's signature and authentication.

It is expected, however, in the future, that a large lumber of authentication systems will be based on electronic signatures.

3.3.2 Legal framework

There is no specific legislation for eGovernment in Greece. However, electronic communication in administration procedures is regulated, generally, in Law 2672/1998. Furthermore, P.D. 342/2002 describes the use of electronic communication for administrative purposes, in more particular. It provides namely that decisions and certificates can be communicated through e-mail from public services, legal persons of public law or organizations of local administration to private or legal persons, provided that they bear a digital signature.

With Law 3242/2004 (Article 8) it has been established that all administrative procedures concerning the issuance of an individual administrative act from the public sector can be concluded by electronic means also and in particular by advanced information systems providing interconnectivity. Freedom of information is established by Code of Administrative Procedure, i.e. Law 2690/1999 (and previously, Laws 1599/1986 and 1943/1991), which provides in Article 5 for the right of citizens to have access to public documents without prejudice of data protection and protection of secrecy provided for by specific laws, as well as of intellectual property rights[22].

The public administration has also a duty to answer citizens' claims and application (Articles 3 and 4 of Code on Administrative Procedure, Article 5 of Law 1943/1991). Administrative authorities are obliged to handle all cases within 50 days maximum, while certificates are to be issued within 10 days, at the maximum[23]. The Constitution provides also for the right to participate in the Information Society[24], but no specific law has been enacted yet, since the fulfillment of the task of facilitating access to the Information Society for all citizens entails un unbearable economic burden.

In the particular case concerning the PKI infrastructure created in the context of the Syzefxis project, it should be noted that the Greek Public Administration Root Certification Authority was established by virtue of Article 20 of Law 3448/2006. In particular, the Special Secretariat for the Implementation of Community Projects of the General Secretariat for Public Administration and eGovernment was assigned the responsibility for the certification, the definition of policy and the coordination of other public entities issuing digital certificates in the framework of the Syzefxis project. The Certification Regulation of this agency was issued on 18 October 2006, and took effect on 10 November 2006[25]. This Regulation implements the principles of the Act transposing the eSignatures Directive, Decree 150/2001, and the Regulation on the Provision of Electronic Signature Certification Services (Decision 248/71 of the EETT)[26].

[22] See Siouti, in: in Gerontas/Lytras/Pavlopoulos/Siouti/Flogaitis, *Administrative Law*, op. cit., p. 254 et seq.

[23] See Siouti, op. cit., p. 248 et seq.

[24] In Article 5A of the Constitution it is stated that "all persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as of the creation, exchange and diffusion thereof, constitutes an obligation of the State".

[25] Government Gazette B 1654/18.10.2006.

[26] Government Gazette B 603/16-5-2002.

It should be noted though that authentication is based on the information contained in identity cards or passports (for non Greek residents and non-nationals), according to Article 6 of Law 1599/1986. The Decree on e-Signatures of 2001 faithfully transposes the provisions of the e-Signatures Directive, but does not apply to authentication as such.

3.3.3 Technical aspects

The smart cards issued in the framework of the Syzefxis Project is the only eID token that has been elaborated so far in Greece, although it is to be expected in the future that electronic identity schemes will be developed. As mentioned above, the smart card is based on PKI technology and has two digital certificates, one for electronic signing and the second for cryptography.

In particular, the first is used for the electronically signing of documents and client authentication; and the second is used in cryptographic applications and tests as a certificate. The Certification Authority controls the public key of the first certificate whereas the holder of the card has the only available private key. The card is dependent on the use of a PIN-code. Each card is issued at the level of a registration Authority, which are functioning in five Ministries, that is, i) Ministry of Interior, Public Administration and Decentralization, ii) Ministry of Finance, iii) Ministry of Health, iv) Ministry of National Defence and v) Ministry of Public Order). On top of the hierarchy stands the Root Certification Authority, which supervises the functioning of the system. The card has a validity of 1 year, but can be renewed as many times as needed.

The aforementioned certificates comply with (a) the ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997 and (b) the RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 (RFC 3280). The structure of the certificates that are used for singing is in accordance with the “Qualified Certificate Profile” in the ETSI 101 862 specification. The signing certificates also comply with Directive 1999/93/EC and the RFC 3739, when there is no contradiction with the aforementioned profile. The PKI infrastructure is ensured to the Greek government through a service level agreement contract, and the provider has to ensure a security level for systems, communications, transactions and data in accordance with the approved standards - ISO/IEC 15408-3; ISO 17799; ETSI TS 101 456; ITSEC-E3 FIPS 140-1.

The public keys of every user are stored by the Certification Authority in a LDAP server in the form of a digital certificate, which contains also the user’s personal data, his/her administrative service’s information etc. Accordingly, each time a user of the Syzefxis network receives a signed document or has access to a certified web page or an information system, he or she could access the certification authority that issued the certificate, in order to determine the originality and validity of the identity concerned.

Smart cards are used as carriers of signature creation data (private cryptographic keys) and of digital certificates for the signature creation data, as a part of a secure signature creation device in combination with the appropriate means (hardware-software) in a user's workstation.

It is not reported whether the smart cards would include printed data of the holder. In any case, his/her personal data are stored on the chip of the card, as the certificate will also be. However, no biometric data are included or planned.

Concerning the technical characteristics of smart cards' certificates, the fields that can be used to the certificates are the following[27]:

Field	Value or Constrains
Version	According to the CPS the value is "0x2"
Serial Number	Unique Value for every Issuer
Signature Algorithm	At the moment the algorithm that is used is the sha1RSA (OID: 1.2.840.113549.1.1.5) according to the RFC 3279.
Issuer DN	According to the Issuing CA
Valid From	Universal Coordinate Time according to the RFC 3280.
Valid To	Universal Coordinate Time according to the RFC 3280.
Subject DN	According to the subject
Subject Public Key	According to the RFC 3280. The length of the keys can be either 1024bit RSA or 2048 bit RSA
Signature	Codified according to the RFC 3280

3.3.4 Organisational aspects

In the case of the Syzefxis PKI system, this is managed by the contractors, i.e. the ADACOM, OTENET/OTE consortium. They provide the infrastructure for the registration and physical authentication of users, which takes place in the so-called registration authorities' offices, maintained by the contractor. The registration authority will address the certification authority that will issue the smart card, which is also maintained by the contractors. The project involves, as mentioned above, the usage of secure signature creation devices (smart cards of the Italian vendor ST Incard; see www.incard.it) inside of which the end user signature keys will be created.

The certification policy and standards are defined by the Root Certification Authority, as mentioned above.

[27] See European eGovernment Services (IDABC), Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications, National Profile Greece, at 5.1.2.2.

3.4 Interoperability

Since there are no eIDM systems developed in Greece, with the exception of the Syzefxis project which is implemented restrictively within the public sector, interoperability is not ensured. Foreigners can use Taxisnet and the Citizens' Bureau, as described above, but the level of authentication is low in this case, and the number of services is limited. No specific interoperability plans to accept foreign eID systems are currently being planned.

3.5 eIDM Applications

The PKI services in the framework of the Syzefxis project will be used for authentication of public servants who use information systems of the public sectors, such as the KEP information system, etc.

There are no private sector applications relying on an eIDM system supported in public sector applications.

3.6 Future trends/expectations

As already mentioned, the development of eGovernment is a priority of the Greek government. After the infrastructure for the provision of integrated online services is created, it is expected that a generic eIDM solution for citizens will also be developed.

3.7 Assessment

There is still much to be done in the direction of developing a national eIDM infrastructure. Most eGovernment services are relying on a low level of authentication, and the lack of efficient security is evident. The use of eSignatures has not been developed to a full extent, as it could be. However, the legal framework for the eSignatures and the infrastructure for certification and accreditation have been developed and are ready to use, so it is a matter of time until the possibilities of PKI are fully exploited.

It is documented in the programme "Politeia 2005-2007", which sets the outlines for implementing eGovernment in all administrative levels and procedures, that projects will be developed where smart cards for citizens and business will be used for use in different types of applications, and this entails the introduction of eIDM systems as it is evident.