IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE CYPRUS

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 eGovernment applications in Cyprus.

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

In Cyprus there is no eIDM system available at the moment, apart from the use of usernames and passwords for entering certain government sites as explained in more detailed below.

Nevertheless, the introduction of eIDM systems is currently being planned by the Government of the Republic of Cyprus, through the participation of the Department of Information Technology Services (DITS) of the Ministry of Finance in various working groups of the European Union. One such group where DITS actively participates is the "Working group of eID of the PPP (Provide eGovernment Good Practice Portability) Project.[3] Within this framework, DITS is examining the prospect of combining eIDM systems with Public Key Infrastructure (PKI).

In addition, DITS is planning to introduce electronic identities in form of Smart Cards in the future to be mainly used for services of the public administration. It is planning to open public tenders for this purpose. DITS is also planning to participate in the eEpoch project which is funded under the 5th Framework Programme and the purpose of which is to be a proof of concept of eEurope Smart Card Charter.

Furthermore, DITS will introduce a Government Gateway using PKI infrastructure for the purpose of providing the tier that enables interoperability, security and authentication with web-based workflow for interconnection of back-end systems. DITS is forecasting that within the framework of the Government Gateway, a single username and password will be required whenever a citizen enters a website of the public service.

It should be noted that in 1998 the Government of the Republic of Cyprus had introduced a type of eIDM system whereby IDs issued to citizens contained a chip. However, such chips were subsequently removed due to a decision of the Council of Ministers following concerns about data protection and privacy, with the Church being a key opponent of eID in this respect. These reactions were focused mainly on the fact that citizens would be monitored by the Government. This reaction led to the abortion of the whole project of introducing eIDM systems in Cyprus. Finally, the fundamental barrier for Cyprus is that the law does not currently allow a chip to be included on identity cards.

[3] http://www.eu-ppp.org/article.php3?id_article=317

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

eGovernment in Cyprus is coordinated at a national level due to the fact that the Republic of Cyprus has a centralist type of government. In general, executive power is vested in the President, who is also the Head of State. The President appoints the Council of Ministers which is the main executive instrument of the Republic. The Council of Ministers consists of eleven Ministers representing their own respective Ministries. The Ministry in charge of eGovernment is the Ministry of Finance, through its Department of Information Technology Services (DITS).

3.2.2 National Strategy for e-Government

Realising the significance of the revolution of information and communication technologies, the Government of the Republic of Cyprus commissioned the preparation of a study for a National eGovernment Strategic Plan in 1987 which was later on updated in 2002 and in 2004. The main strategic objective of this plan was to examine the Information needs of the Government of Cyprus and to identify candidate applications for computerisation. Based on the recommendations of this study, the Council of Ministers adopted a Government Computerisation Master Plan (GCP) in March 1989 which was later on revised in 1998 in order to take into account rapid technology changes, evolving user demands and EU accession requirements which necessitated the inclusion of new infrastructure and strategic projects.

The National Strategy for e-Government was subsequently drafted, focusing on key issues required to make the implementation of e-government successful. The e-government vision of the Government of Cyprus is to deliver one-stop services to the public via the web or through other electronic channels (kiosks, call centres, citizen support centres etc.). For this e-government vision to be achieved, three fundamental “building blocks” need to be implemented:

- At the “front end”, a multi-channel portal aggregating all information and services in one place, based on the life-event-cycle.
- A “middleware”, a government gateway providing the tier that enables interoperability, security and authentication, with web-based workflow for interconnection of back-end systems.
- At the “back-end”, web-enabled information systems and processes involved in service delivery.

Recently, the Cyprus National Strategy for the Information Society for 2004-2006 has been developed, and is being expressed through a series of high-level targets. Specific targets related to eGovernment are:[4]

[4] http://www.euser-eu.org/eUSER_eGovernmentCountryBrief.asp?CaseID=2213&CaseTitleID=1054&MenuID=

- Development of a general framework of electronic transactions and communication between the public (citizens and businesses) and the state (government and local authorities);
- Reinforcement of organization, human resource management, digital literacy and capabilities of personnel, the development of learning ability, and production and diffusion of knowledge, so that the human resources of Public Administration will be able to meet the anticipated chalenges of a knowledge-based society;
- Introduction of a comprehensive computerised system in the Public Sector, to limit expenses through more effective procedures of Public Administration. Such a system shall be able to provide high quality services to the public without the need of visiting any government department to obtain such services. In achieving this vision, a Government Gateway that aggregates all government information and services in one place is to be designed, implemented and made available to the public. It is intended to be the primary place where citizens go to get information about government services, and transact with government on-line.

3.2.3 The Information Systems Strategy (ISS)

On the basis of the National Strategy for e-Government, the Government of the Republic of Cyprus adopted the Information Systems Strategy in 1998 with the aim of achieving the best possible quality of services offered to the public making full use of the new information technologies, for interconnecting government systems over the Government Data Network (GDN) and providing for the creation of a secure gateway on the web.[5]

In order to achieve this, government systems have been interconnected over the Government Data Network and a secure gateway on the web has been created so as to provide citizens with the facility to get services from anywhere. Furthermore, the Republic of Cyprus has also transformed completed information systems into web-enabled systems, in order to give information and services to citizens and businesses and give government information services to the public via internet.[6]

More specifically, regarding the interconnection of systems, the core systems (Civil Registry, Lands and Surveys, Registrar of Companies) which own data required by other ministries/departments have been completed. As a result, now it is both possible and required to interrelate these systems. The completion of the infrastructure projects (*i.e.* Office Automation, Government Data Network (GDN) and Government Internet/Intranet/Extranet (GIN)) facilitates the above target.

Furthermore, an Office Automation System, that handles automated procedures for office work, supports enterprise-wide document management services and the control of work-groups and workflow, has been introduced in a number of Government Ministries/Departments/Services and has

[5] ICA, ‘35th Conference Round Table Report: Cyprus’, created October 2001; available from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005093.pdf; accessed 27 March 2005.

[6] Council of Europe, ‘15th Colloquy on Information Technology and Law in Europe: ‘E-Justice: Interoperability of Systems’, (2002).

been successfully installed in most government departments. The Office Automation System, which has brought the benefits of a paperless office, enforces existing rules and regulations, improves productivity, speeds the communication between office workers, reduces operational costs, and also provides distance-working capability.

The GDN, which ensures the connectivity of all government ministries/departments using ATM technology with a backbone of 622 Mbps speed, has been completed and has an overhead of CYP 1,500,000 rent to the Cyprus Telecommunications Authority.

The third infrastructure project, which is the building of a government internet/extranet node, has been completed and the roll-out has started in all ministries/departments. All civil servants have an e-mail connection and access to the internet. The government website was released in 2001 and now most government departments have their own informative web site.

In addition, a Data Management Strategy has been adopted since 1997 which provides an integrated information structure capable of supporting its requirements for strategic and tactical management information systems as well as operational systems. This common model was provided through the medium of the Government Data Model (GDM) which defined all government strategic data. The strategic data for the Government of Cyprus (i.e. that data which is used by more than one operational information system) is based on the data models of the Civil Registry, Lands and Surveys and the Registrar of Companies.

On the basis of the e-government policy, several Government Ministries, Departments and Services offer services to the public through the web, thus creating a dynamic government, with the aim of improving the quality of services offered to the public.

The process of developing web-enabled systems in order to provide better services to the public through the Internet is underway. Some systems that were recently developed are fully transactional (Taxisnet for income tax returns, Theseas for customs clearing) and some others support two-way interaction (statistics, family allowances, candidate placement).

Additionally, all Government Ministries/Departments/Services have their own website. The majority of the websites are informative and provide downloading of forms and other documents. Some also support user interaction.

3.2.4 National Strategic Plan for eCommerce and Electronic Signatures

In addition, another strategy, the National Strategic Plan was formulated by the Government in 2001 which brought about the adoption of specific electronic signatures legislation. More specifically, the objectives of this study were the formulation of the legal framework and a national policy for an e-Commerce strategy to place Cyprus at the forefront of the most competitive and dynamic knowledge-based economies. As a result, a group of experts was selected by the Planning Bureau of the Republic for conducting an investigation regarding the market situation in Cyprus and propose measures in order to harmonise Information Technology issues with the *acquis communautaire*, including issues of Electronic Commerce and Electronic Signatures. Where electronic signatures are concerned, the group of experts' main responsibilities were inter alia, to propose a general strategy for e-commerce adapted to the Cyprus market and assess the existing legal framework and make suggestions for changes. As a result, legislation on e-commerce and electronic signatures matters was enacted on 29 April 2004. The Plan was recently updated in 2006.

3.2.5 Other eGovernment initiatives and developments[7]

In 2004, a National Strategy for the Development of Information Society was drafted by the Cyprus Planning Bureau. Furthermore, on 19 May 2004, the European Investment Bank (EIB) released the first EUR 35 million tranche of an overall approved financing of EUR 70 million to upgrade IT systems in the public sector of the Republic of Cyprus. The project, led by the Department of Information Technology Services (DITS) in the Ministry of Finance, is mainly driven by the priorities set in the Partnership Agreement concluded between Cyprus and the EU in 2000 and revised in 2002. It concerns investments in IT systems in various Cypriot Government Departments, encompassing investments in physical networks and hardware as well as the development of specialised software systems. Finally, TaxisNet (web-enabled service for income tax returns) and Theseas (web-enabled service for customs clearing) were launched in early 2004.

3.2.6 Traditional identity resources

Use of usernames and passwords as a method of identification

(a) Inland Revenue & Value Added Tax

The Inland Revenue Department of the Ministry of Finance which is responsible for the application and enforcement of direct tax legislation in the Republic of Cyprus operates the TAXISnet network which is a special network provided free of charge by the Inland Revenue Department. Through this network, taxpayers who are natural persons may submit initial tax returns by use of electronic communication methods.[8]

Under the TAXISnet network, taxpayers submitting an application to the Inland Revenue Department for access to the TAXISnet system, can apply for registration by filling out Form I.R.D 66 2004[9]. This form must be handed in filled out and signed to the District Management of Returns Sections or the TAXISnet office in Nicosia.

[7] http://ec.europa.eu/idabc/servlets/Doc?id=24769

[8] Income Tax Return Forms may be found electronically in .pdf format at the Department's website at http://www.mof.gov.cy/mof/ird/ird.nsf/dmldocsta_en/dmldocsta_en?OpenDocument and http://taxisnet.mof.gov.cy/static/help/files/TermsandContitions_En.pdf

[9] See http://taxisnet.mof.gov.cy/static/help/files/Application_Individuals_EN_66.pdf

The Inland Revenue Department will then provide a password to the taxpayer for use by the applicant in conjunction with the PIN number for access to the TAXISnet system. Registration is only possible after the user has provided his/her personal data, including the Taxpayer's Identification Code (T.I.C.). The PIN number is a secret personal identification number given and/or created by a taxpayer, in accordance with the instructions for use, in order to be used together with the password.

The TAXISnet service has been active since December 2004, whereby persons have initially become able to submit tax returns electronically through the XML Archives. This procedure has enabled the submission of all tax returns together, as prepared by auditing firms. The specifications of the XML Archives may be obtained from the various accountancy bodies and from the website of TAXISnet.

TaxisNet is available 24-hours. Taxpayers are immediately notified when their tax return has been received, and can monitor the process of the transaction through a special network. The system does not provide personalisation, but it is effective in fulfilling the taxpayers' expectations in the process of filing their tax return.

With regards to security conditions, the taxpayer must undertake to comply fully with the terms and conditions, the aim of which is to minimise the risk of unauthorised use of the TAXISnet system. The Inland Revenue Department reserves its liability towards the taxpayer for any loss of data resulting from his/her failure to comply with the terms and conditions of operation of the TAXISnet system. The taxpayer is under an obligation to keep his password and PIN number in a safe place and not to disclose it to any other persons, so that there is no irregular or unauthorised access or use of the TAXISnet system.

The system may be used by any taxpayer, being natural person registered withthe Tax Archive of the Inland Revenue Department and holding a Taxpayer's Identification Number.

There is only provision for the use of PIN numbers. No Government initiatives aimed at providing or encouraging the use of eID/eSignatures for this specific eGovernment application is envisaged and no awareness programmes have been set up. The legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application are due to the lack of implementation of specific secondary eSignatures legislation.

(b) Theseas Customs and Excise System

The Cyprus Information Systems Strategy has enabled the development of the *Theseas Customs and Excise System* for customs clearing which is a fully transactional system (www.mof.gov.cy/ce/theseas). Theseas is an information portal. It contains a number of administrative reform and trade facilitation components in order to examine current practices and procedures within the Customs and Excise Department.

It is designed for the traders to connect to the system via the Internet for the electronic submission of cargo and import declarations. Furthermore, the system is also designed for the electronic payment of customs duties through the banks. In general, where the Director of the Customs and Excise Department approves the submission of the documents by using an automated medium, he provides a code number to the person authorised to submit the documents in an automated manner.

The interface with the users of the system is implemented with up-to-date technology. The internal or external end-users are connected through a Web based interface allowing both advanced ergonomic features and thin client benefits, especially in the management of the client systems. Business partners can use the system to exchange UN EDIFACT Customs standard messages.

As for the security features, user identification and confidentiality of the exchanges have to be implemented through the use of secure procedures and protocols based on Internet standards.

Access to the system is open to the following users:

- Customs Officers located in Customs Headquarters, and all Customs offices in the airports, the ports and post-offices and Nicosia district office. Customs Officers are connected through intranet and have access to Goods Processing Modules functions depending on their rights.
- External trade agents, carriers, importers, which are connected mainly through Internet, need a PC with internet access.
- Security officers and system administrators, which have the mission to define the rights of every users and the task of maintaining the system in operation, perform administration on the various servers, define the parameters of every network equipment (passwords for remote users).

The system allows the connection of more than 355 Customs users and several thousands of registered agents for extranet access.

The Theseas System is also the system to be used where, under the Customs Code, persons need to provide customs declarations. For example, the Theseas System contains an Import Declaration Processing Module, the purpose of which module is to support the clearance of imported goods according to Customs laws and regulations. Furthermore, the module maintains a complete database of up-to-date information about all imported goods, and produces figures for fiscal and foreign trade statistics. The module is based on the idea that all consignments can be cleared through the Customs by Customs clearance declarations worked out by the importers or Customs clearance agents before the actual consignments have arrived at the borders. When the consignments have reached the border destination and the necessary Customs clearance information is available for the Customs, the consignments can be released immediately for home use, if no Customs control activities have to be carried out by the Customs in relation to the actual consignment.

All customs stations are connected to the system via Intranet operating over the Government Data Network. An interface exists with the Cyprus Ports Authority for the electronic submission of cargo manifests and a standard XML development has been made available to the traders for bulk input to the system. The system is designed to enable the interface with the Customs systems of the EU and specific modules have been developed to ensure the interoperability with the systems of DG TAXUD.[10]

[10] http://www.ica-it.org/conf37/docs/Conf37_CountryRep_Cyprus.pdf

To submit a declaration by Internet, the declarant must have a special authorisation to make sure that there will not be any juridical problems or technical problems concerning communication between the enterprise and the Customs.

All users who connect to the manifest system must have a username, a password and a profile. All three are provided by the Customs after personal identification. Usernames must be unique, and only one profile can be assigned to a username. However, it is possible to assign several usernames to the same physical individual.

After receipt of the SAD, the Customs office first makes a documentary check. The entry and the supporting documents (invoices, transport documents etc.) are checked to ensure that the declaration is completed in such a way that the clearance may be accepted.

Checks are made to ensure that:

§ the entry form is correctly completed and signed;
§ the necessary supporting documents are present.

The Customs office then enters the declaration in the computer system. The computer before accepting the entry automatically checks if:

- the registration number of the authorised declarant is valid according to the Customs' Register of Enterprises;
- the declarant is entitled to act as declarant;
- the registration number of the importer is valid according to the Customs' Register of Enterprises;
- the importer is entitled to credit for duties and taxes;
- the codes used exist;
- the duty rate stated is in agreement with the classification;
- the exchange rate is correct.

The declarant is requested to be able to enter his declaration through a flat file on his workstation. Furthermore, authorised clearing agents and importers are provided with a set of files which enable the agent or the importer to validate the SAD off line and in advance.

National Register – natural persons

A (non-electronic) ID infrastructure exists. The Civil Registry and Migration Department under the authority of the Ministry of Interior issues a paper ID card to natural persons.[11]

In general, the Civil Registry and Migration Department deals with the following:

[11] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/NationalProfiles

- Cyprus Passports
- Civil Identity cards
- Refugee Identity cards
- Birth Certificates
- Death Certificates
- Election booklets
- Electoral list
- Acquisition of Cypriot Citizenship by aliens
- Registration of persons of Cypriot origin and spouses as citizen of the Republic of Cyprus
- Renunciation and deprivation of citizenship
- Residence Permit for alien visitors
- Entry and residence permits for alien workers
- Immigration Permits
- Entry and residence permits for alien students.

Identity data is contained in a central Civil Registry System (CRS). Cyprus has been developing its eGovernment strategy with a number of projects in recent years, and web enabling of the CRS is planned although no date has been fixed for this.[12]

Unique ID numbers are issued to each citizen at birth, and non-electronic identity cards are issued to citizens when they reach the age of 12. In fact, it is mandatory for every person above 12 years of age to have such an ID card.

The ID card containing a single identification number is issued for citizens of the Republic, persons of Cypriot descent as well as for aliens who are legally residing in Cyprus whether temporarily or permanently. The single identification number of the identity card is accepted by both public authorities and private organizations, such as banks.

Cyprus links the following attributes of a natural person to a person's single identifier (beyond others):[13]

- name, first name(s), sex, date of birth, place of birth, and address;
- former names, parent names, nationality, marital status, and religion;
- photograph;
- legal right to stay in the country.

According to one study, Cyprus stores 24 fields overall and keeps historical data for some of them.[14]

Other application specific identifiers that are derived from the single identification number are:

[12] http://www.eu-ppp.org/article.php3?id_article=317

[13] https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/CyprusProfile

[14] Identity Management and Data Sharing in the European Union; Proceedings of the 39th Hawaii International Conference on System Sciences – 2006; by Benoit Otjacques, Patrik Hitzelberger, Fernand Feltz; Centre de Recherche Public – Gabriel Lippmann, Luxembourg.

- social insurance number;
- driver license number;
- military number;
- electoral booklet number;
- refugee booklet number.

Companies Registration System

Under the Department of the Registrar of Companies and Official Receiver (D.R.C.O.R.) of the Republic of Cyprus, the Companies Section deals with the registration, follow up, control and striking off of companies, of oversea companies, of partnerships and of business names. Single identification numbers are used

An application is available at the website of the D.R.C.O.R. where persons can perform a search on Names Index of the D.R.C.O.R.[15] Persons can also submit an application for name approval on line through the same application.[16] On-line Applications can be submitted by Customers who applied to the D.R.C.O.R. for a Customer Number and a PIN Number and they have an account with the Department.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Cyprus is at a crossroads in terms of eID. Until now, the move towards eID has been held up by concerns about data protection and privacy, with the Church being a key opponent of eID in this respect. The fundamental barrier for Cyprus is that the law does not currently allow a chip to be included on identity cards.[17]

As a result, in Cyprus there is no eIDM system available at the moment, apart from the use of usernames and passwords for entering certain government sites as explained above.

[15] http://www.mcit.gov.cy/mcit/drcor/drcor.nsf/search_catalogue_en/search_catalogue_en?OpenDocument

[16] The application uses an Oracle application server

[17] http://www.eu-ppp.org/article.php3?id_article=317

3.3.2 Legal framework

The main legal framework for or in relation to (non-electronic) ID cards is the the Civil Register Law of 2002 (Law 141(I) of 2002), regarding the population registers and identity cards, which is the basic legal source.

Chapter Three, Part two of the Law[18] provides for the issuing of Identity Cards, following an application by the interested person and Chapter Four, Part One provides for the issuing of passports and other travel documents. There is no provision in the Law for electronic IDs.

Other relevant legislation includes the Legal Framework for Electronic Signatures and Associated Matters Law of 2004, Law No. 188(I)/2004.[19] The Law was enacted on 30 April 2004 for the purpose of implementing Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.[20] The Law also implements Commission Decision 2000/709/EC on the minimum criteria to be taken into account by Member States when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC.[21]

The enactment of the Law is the result of a comparative study prepared by the Department of Information Technology Services (DITS) in cooperation with the Law Office of the Republic, in relation to digital signatures concerning the use and legal value of digital signatures, with particular emphasis to the particularities of Cyprus.

It effectively establishes the legal framework governing electronic signatures and certain certification services for the purpose of facilitating the use of electronic signatures and their legal recognition. It does not, however, cover aspects related to the conclusion and validity of contracts or other legal obligations which are governed by requirements as regards their form. Furthermore, it does not affect rules and limitations in relation to the use of documents provided by other applicable legislation in force.

The Law affords power to the Minister of Commerce, Industry and Tourism (the Competent Authority) to exercise control over and ensure the effective application of this Law, and, in particular, to:

(a) Supervise and monitor certification-service providers established in the Republic, as well as public or private certification providers appointed by him;
(b) Monitor the compliance of signatures with the requirements for secure signature-creation devices;

[18] Section 63.

[19]

[20] OJ L13, 19 January 2000, p. 12.

[21] OJ L289, 16 November 2000, p. 42.

(c) Prescribe public or private providers for the purpose of certifying the compliance of secure-signature-creation devices;

(d) Regulate voluntary accreditation, that is, a licence to certify electronic data, setting out rights and obligations governing the provision of certification services and which is granted by the Minister upon request by a certification-service-provider appointed by the Minister.

In addition, the Law affords power to the Council of Ministers to issue Regulations prescribing the details concerning the exercise of the functions, powers and duties of the Competent Authority concerning the supervision of the implementation of the legal framework governing electronic signatures, the better implementation of the Law, as well as anything which must or should be regulated in this Law.[22] It is important to note that, due to the nature of the legal system in Cyprus, the issuing of these Regulations is essential to the actual use of electronic signatures in Cyprus. Unfortunately, the Council of Ministers has not yet issued any such Regulations; therefore, the rules governing the use of electronic signatures do not yet exist.

Furthermore, it is also useful to mention that according to section 15 of the Law, power is granted to the Minister who acts as the Competent Authority to issue Orders prescribing the technical procedures and the details on the exercise of the functions, powers and duties of the Competent Authority and concerning any issue regarding the monitoring of the legal framework governing electronic signatures and in particular regarding:

the determination of technical standards which shall apply from time to time;

the determination of the fees;

the amendment of the Schedules of this Law for the purpose of direct adjustment with the laws of the European Union.

Nevertheless, no such Orders have yet been adopted by the Minister, therefore, the above matters are also left outstanding.

3.3.3 Technical aspects

In Cyprus there is no eIDM system available at the moment.

3.3.4 Organisational aspects

In Cyprus there is no eIDM system available at the moment.

[22] Section 14 of the Law.

3.4 Interoperability

In Cyprus there is no eIDM system available at the moment.

3.5 eIDM Applications

In Cyprus there is no eIDM system available at the moment.

There are no eID card applications.

There are no paper token applications.

3.6 Future trends/expectations

Cyprus is planning for the introduction of ePassports, as required by EU regulations. These will contain biometric information - facial recognition information and fingerprints - as specified by the EU. It is thought that developments such as this have the potential to change attitudes to electronic travel and identity documents.[23]

Cyprus is also considering the potential for collaboration between the Belgian eID scheme, which is the good practice case at the basis of the PPP eID working group, and the Cypriot scheme. From the point of view of the PPP project, there are a number of similarities between the system under development in Cyprus and the Belgian system, which provides the good practice basis for the eID working group. The systems are essentially similar, with identity data contained in civil registers, infrastructure in place prior to eID roll-out and a government gateway for access to services.[24]

eServices will be provided through a government gateway which is in development. Its implementation will be phased and pilot projects are either in progress or are planned. Access control will be based initially on two-factor authentication - username and password or PIN. But smartcards are seen as an 'obvious' authentication method. The Cypriot authorities see no barrier because of availability of card readers: new laptops are already being issued with these as standard.[25]

[23] http://www.eu-ppp.org/article.php3?id_article=317

[24] http://www.eu-ppp.org/article.php3?id_article=317

[25] http://www.eu-ppp.org/article.php3?id_article=317

Finally, no eSignatures scheme has yet been introduced in Cyprus. It is not known whether such a system will be introduced in the future although such a system may be put in place after secondary legislation has been enacted allowing for the use of such systems.

3.7 Assessment

In Cyprus there is no eIDM system available at the moment, therefore, no assessment of the system can be provided. The situation is hampered by the fact that no eSignatures scheme has yet been introduced in Cyprus. This is because no secondary legislation has been enacted prescribing the specific rules governing the use of electronic signatures, the determination of technical standards, the supervision of certification-service providers established in the Republic or the appointment of public or private certification providers. In addition, no rules have been put in place regarding the monitoring of the compliance of signatures with the requirements for secure signature-creation devices and no public or private providers have been prescribed for the purpose of certifying the compliance of secure-signature-creation devices.

The reason that no action has yet been undertaken for adopting secondary legislation in Cyprus for the purpose of granting authentication certificates is because there is no infrastructure in place or the necessary know-how in Cyprus as yet. In addition, no decision has yet been adopted as to which authority in Cyprus will grant authorisations for PKI and in general which body will undertake this responsibility. It is currently being discussed with the Department of Electronic Communications, of the Ministry of Communications and Works that this department will be responsible for granting authorisations.