IDABC
European
eGovernment Services

eID Interoperability for PEGS

NATIONAL PROFILE TURKEY

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 Turkish 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

Turkey has implemented various eIDM systems in conventional public services and e-government practices. In most of these systems as well as some private institutions, domestic and national official registers operate by verification through unique identifiers used together with authorisation tools.

Most of such applications in Turkey use the unique identifiers in the MERNIS database administered by the General Directorate of Civil Registration and Nationality. The unique number which is used as an authentication attribute by some agencies is printed on the National Identity Card. Many agencies, non-governmental organizations (NGOs), and firms require copies of the identity card or all the information on it. Therefore, the unique number itself cannot be used as a secure authentication mechanism. For this reason unique identifiers are used not for the purpose of authentication but for the purpose of verification of the presented personal data.

The General Directorate of Civil Registration and Nationality put into operation the Identity Sharing System (Kimlik Payla••m• Sistemi-KPS, based on MERNIS database) at the beginning of 2005. Presently, the system offers various web services with different civil status data sets which are accessible by agencies after signing protocols.

Identification information with regard to legal entities is primarily stored in the so called Ministry of Finance Tax ID Number (Maliye Bakanl•• • Vergi Numaras•) which identifies legal entities by the so called enterprise number (real persons also used the Tax ID Number, but since 2006 it was decided to use the Turkish Republic (TR) Identity Number).

In late 2005, Turkey has contracted the construction of the e-Government Gateway. Pursuant to the protocol signed with Ministry of Transportation, TURKSAT, a state-owned firm, has been assigned with the development of the e-Government Gateway Project[3] that is still in progress.

The Law No 5070 on e-Signatures provided the same legal effect to secure e-signatures as hand written signatures. There are four electronic certificate service providers that started to operate after their notification to Telecommunications Authority were found to be compliant with the requirements.[4] As of February 2007 a mobile e-signature infrastructure has been completed and users can create legally binding e-signatures using their SIM cards.

[3] Official Gazette, April 20, 2006, Number: 26145; http://www.bilgitoplumu.gov.tr/mevzuat/e-DevletKapisi_20060420.pdf

[4] e-Guven www.e-guven.com, Turktrust www.turktrust.com, e-Tugra www.e-tugra.com, Kamu SM http://www.kamusm.gov.tr/

Internal Processing Regime and Free Trade Zone Projects run by the Under-Secretary of Foreign Trade are the first e-signature applications in the public sector that mandate the usage of e-signatures with full legal effect. However, there are other future projects that require the use of e-signatures for the purpose of identification. After completion of the mobile e-signature infrastructure, 5 major banks in Turkey have integrated e-signatures in their IT systems. The mobile signature is used both for ID verification and for signing transactions like money transfers.

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

eIDM system	Potential user base	Actual penetration	Actual use
Qualified Electronic Signatures	Estimated at 5 million (requires a token and a card reader, now mobile eSignature is available)	Estimated at 10.000 (around 0,012% of the population, and around 0,2% of the potential user base)	The number of qualified electronic certificates issued is 12038 by the end of 2006.
eGovernment Gateway Single Sign On Solution	Estimated at 30 million	Not being used yet since the project has not been completed.	No public statistics are available

3.2 Background and traditional identity resources

3.2.1 eGovernment structure[5]

e-Government leadership is provided by the e-Transformation Turkey Executive Board headed by the Deputy Prime Minister and Minister of State. This Board develops e-government policies and strategies. The Board used to consist of 13 people: the Deputy Prime Minister and Minister of State, Minister of Transport, Minister of Industry and Trade, Undersecretary of State Planning Organization (SPO), and Chief Advisor to the Prime Minister who have voting rights, four participants from the public sector and four from NGOs, who do not have voting rights.

According to the latest revision made by the Prime Minister's circular numbered 2007/7[6], the Board has been consolidated by including, Minister of National Education, Undersecretary of the Prime Ministry, Undersecretary of the Ministry of Interior, Undersecretary of the Ministry of Finance. The number of the participants from public as well as NGO's with no voting rights has also been increased.

The e-Transformation Turkey Executive Board is served by the Information Society Department (ISD) in the SPO. This department is responsible for providing support to policy making and overall

[5] OECD e-Government Studies TURKEY

[6] Official Gazette, April 03, 2006, Number: 26482; http://www.bilgitoplumu.gov.tr/genelgeler.asp

coordination of e-government including interoperability, metadata and an e-government gateway. The department reviews public entities' project proposals regarding IT investments.

An Advisory Board consisted of representatives of public institutions, NGO's and universities was revised by the aforementioned circular. The new Board consists of members from NGOs, universities and businesses, ensuring high-level representation from the civil society.

A new board named "e-champions" was established by the same PM circular. Board of e-champions will form a common platform to facilitate implementation of Information Strategy by ensuring cooperation among the public bodies and setting the common principles and standards in the process of transformation to the information society. This board consists of the heads of strategy development departments of the public institutions and members appointed by the Executive Board from universities and local governments.

Before the national information society strategy was put into force on 28th of July, 2006, A Short Term Action Plan consisting 73 of actions for 2003-2004 period and an Action Plan consisting of 50 actions for 2005, were implemented.

During the preparation period of these Plans, a participative governance model was maintained and the ISD worked with eight associated working groups handling different issues: e-government, infrastructure security, e-commerce, legal infrastructure, standards, e-health, monitoring, and human resources and education. These work groups which composed of public and NGO representatives, have collaborated with the SPO in developing action plans.

In the Information Society Strategy, the current situation of the main constituents of the society – citizens, public sector and businesses as well as the ICT sector – and Turkey's potential for transformation into an information society by 2010 have been evaluated, and a range of targets for 2010 have been identified together with the required steps for accomplishment of these targets within the framework of the strategic priorities determined henceforth. Furthermore, R&D and Innovation strategies of Scientific and Technological Research Council of Turkey's (TÜB•TAK) "Vision 2023" studies has been integrated into the strategy.

It is expected that the Information Society Strategy and its annexed Action Plan would be the basic reference document for citizens, the public sector, private sector and the NGOs, in short for all segments of the society, within the next five-year period, and will shed light to future schemes.

Local Government Collaboration

Being autonomous authorities, local governments (exceeding 3200) can develop and implement their own ICT strategies and investments; however they are bound by central government guidelines on interoperability. Large municipalities like Istanbul and Ankara have the resources to develop their own e-government applications. However, it is unrealistic to expect smaller municipalities to develop portals and e-services on their own. The Information Society Strategy's organizational structure model envisages a new coordination unit in the Ministry of Interior for e-local government oversight for standards and shared services as well as a liaison between local and central government. Information Society Strategy also proposed three main actions which primarily aim, inter alia, to develop local e-democracy, local e-government implementation and performance monitoring system.

Realisation of an e-Government Gateway

In order to ensure provision of public services through a single portal and access of citizens to governmental services electronically in a secure and efficient manner, the Council of Ministers decided on 24 March 2006 on the Resolution concerning the establishment, operation and management of an e-government portal[7].

According to this Resolution the duty and the responsibility of establishing the e-Government Gateway that will ensure the provision of public services in a common platform is granted to the Ministry of Transportation.

The Ministry of Transportation is entitled to establish work groups and commissions for the fulfilment of the assigned duties and responsibilities. The Ministry exercises its duties and responsibilities concerning the establishment and the operation of the e-government portal's technical infrastructure by the mediation of Türksat Uydu Haberle•me ve Kablo TV ••letme A• (TURKSAT). The procedure and the principles regarding the fulfilment of the said duties including the service fee shall be determined by means of a protocol to be concluded by and between the Ministry and TURKSAT. The scope of the project covers the studies concerning the standards and requisite legal regulation related to the review of the operation process, content management and integration for the provision of public services in a citizen centric electronic environment. Within the implementation process of the e-Government Portal Project, conformity to the goals, principles and policies that are set in the National Information Society Strategy carried out under the e-Transformation Turkey Project coordinated by the State Planning Organization is of essence. TURKSAT is also assigned with the establishment of essential infrastructures of e-Government concept such as secure government network and national disaster recovery centre for information systems within the Action Plan annexed to the Information Society Strategy.

3.2.2 Traditional identity resources

Turkey has a long tradition in civil registration. The establishment of the civil registers date back to the first population census conducted in 1904 during the last years of the Ottoman Empire. Proclamation of the Republic of Turkish in 1923, however, brought significant changes to the way civil registers are maintained. In 1928, following the acceptance of the Latin alphabet, Arabic letters and numbers were abandoned in the maintenance of the registers. In 1934, last names were granted to each family and individual, abolishing the practice of appellations. It was not until 1972, however, when the introduction of Law No 1543 and its successor Law No 1587 paved the way for the modernisation of the civil registration system in Turkey. The amendments made to the abrogated Law No 1587 envisaged that "The Ministry of Interior shall be empowered to ensure the transfer of family registers to registers kept in electronic format and to facilitate carrying out civil registration acts using these registers, to provide measures ensuring the security and privacy of the registers kept in electronic format, to repel the civil registers kept in paper format, to determine the civil registration offices empowered with issuing, registration and safekeeping of reference documents, to decide on the use of electronic signature in all kinds of civil registration acts carried out in electronic format, and to meet the requests for information from the records kept centrally in electronic format by the public institutions and the work flow in the headquarters and the districts in the scope of the principles and procedures to be determined within the completeness of civil registration services." The Law also

[7] http://www.bilgitoplumu.gov.tr/mevzuat/e-DevletKapisi_20060420.pdf.

dictated that the civil registers, comprised of family registers, special registers and microfilms maintained in paper or electronic format, are official documents maintained in paper or electronic format on a district and family basis which include information used to determine the rights and obligations of persons, their identity, family relations, nationality and civil status. Civil registers are official documents which have to be kept indefinitely. Currently, the main legislation covering all aspects of civil registration is the Civil Registration Services Law No 5490, dated 29.04.2006.[8]

The modernisation of civil registration system in Turkey culminated in 2000 with the introduction of the Central Civil Registration System (see below), or MERNIS at is known by its abbreviations in Turkey, set up after long and arduous work.

The basic document used for identification purposes in Turkey is the national identity card issued by the civil registration offices located in every district. The current design of the paper-based card dates back to 1989. Recently, however, in the scope of the modernisation of the civil registration services and the Information Society Strategy Action Plan[9], a new e-ID card project has been initiated (see below).

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

The Central Civil Registration System (MERNIS)

The Central Civil Registration System (MERNIS) is a centrally administered system where any changes in civil status are registered electronically in real time over a secure network by the 923 civil registration offices spread throughout the country. The information kept in the central database is shared with the public institutions for administrative purposes. The aim of the system is to ensure the up-to-datedness and secure sharing of personal information and therefore increase the speed and efficiency of the public services provided to the citizens. The system works over a WAN and uses star topology. Currently, work is underway to change the system to XML architecture.

The project has a long history of development and after arduous work conducted in the late 1990'sthe project finally come into being in 2000 and is continuing its successful operation and evolution ever since.

MERNIS has become the backbone of the e-Government infrastructure in Turkey. Within the scope of the project, more than 500 public bodies are using the updated data from the MERNIS database. Currently, the MERNIS database houses more than 130 million personal data files. The services provided by MERNIS are as follows:

- Modernisation of civil registration services by transferring the civil registers into electronic format
- Assignment of an unique Turkish Republic Identity Number to every Turkish national

[8] http://www.nvi.gov.tr/attached/nvi/nufus_mevzuati_pdf/kanun_pdf/nufus_kanunu.pdf

[9] http://www.bilgitoplumu.gov.tr/btstrateji/Eylem_Plani.pdf

- Provision of on-line exchange of personal information using the identity numbers as identifiers
- Provision of better demographic statistics using information technologies
- Enabling easy, fast and secure delivery of public services to the users by sharing identity information with public sector institutions and agencies and thus reducing bureaucracy

By 2002 every Turkish national was allocated a unique Turkish Republic Identity Number in order to:

- Resolve problems arising from identical names
- Provide fast and efficient identification
- Register all civil status events from the moment of birth
- Provide fast and efficient services to the users of public services by ensuring efficient exchange of identity information among public institutions and agencies

The ID number is comprised of 11 digits which do not contain personal information. With the introduction of the unique Turkish Republic Identity Number for every Turkish national, the applications of different numbers issued by different institutions were abandoned.

The web site of the General Directorate of Civil Registration and Nationality is offering a free-access identity number enquiry module.

On the other hand, as dictated by the Civil Registration Services Law No 5490, aliens who for whatever reason have obtained residence permit for aliens to remain in Turkey for at least six months period are also entered by the General Directorate of Civil Registration and Nationality in the register of aliens and allocated a unique ID number. The information is provided by the General Directorate of Security and aliens entered in this register are under obligation to declare every change in civil status event to civil registration offices.

MERNIS is a constantly evolving and expanding system. In 2006, as set out by the Law No 5490, the latest addition to the system was the Address Registration System which mandates that every Turkish national has to declare a mandatory domicile address. With the latest addition, the services provided by the General Directorate of Civil Registration and Nationality cover all the aspects of civil registration.

The Identity Sharing System (KPS)

The Identity Sharing System (abbreviated KPS in Turkish) went into operation in 2005 as an extension of MERNIS. Public institutions and agencies can access ID information stored in MERNIS database via the KPS under strictly specified conditions in the respective access protocols. KPS works over a Virtual Private Network and every user is assigned with a user name and password. The system keeps logs of every user and all the enquiries conducted. The system offers the following enquiry services:

Web Sites

- Enquiry of personal information using the TR Identity Number
- Enquiry of TR Identity Number using personal information
- Enquiry of identity information based on information of the place of registration

- Enquiry of copy civil status records using various criteria

Web services (XML Infrastructure)

The private sector and institutions are able to conduct inquiries by accessing KPS web services using add-ons to their existing applications or by developing new applications. They are also able to view the enquired data directly from their own applications and automatically update their own databases with the enquired information.

For the private sector to benefit from the MERNIS Project, an agreement must first be concluded with the General Directorate of Civil Registration and Nationality. However, any information kept in MERNIS is only available to domestic public and private sector. Access by foreign entities is prohibited.

e-Government Gateway

In late 2005, Turkey has contracted the construction of the e-Government Gateway. Pursuant to the protocol signed with Ministry of Transportation, TURKSAT, a state-owned firm, has been assigned with the development of the e-Government Gateway Project[10] that is still in progress. The TURKSAT team monitors and supports the development of the project. TURKSAT also focuses on the organisational and legal issues of the system with a ministerial level encouragement.

The e-Government Gateway natural persons' SSO solution envisages developing 4 levels for authentication purposes:

Level	**Registration of user Identity**	**Authentication of user identity**	**Applications**
0	None	None	General public information
1	On line by entering the national identity number, and personal information	National identity number in combination with a password chosen by the user	Information/services of limited sensitivity
2	Level 1 + a confirmation message that implies the USER LICENSE and send-out of an ENVELOPE with a PASSWORD to the address specified by citizens and may be checked with the one in MERNIS	Level 1 + entering PASSWORD mentioned on the ENVELOPE (which contains a number of sequences)	Information/services of average sensitivity
3	Physical identification at the commune for the acquisition of a secure eSignature.	Authentication certificate on the eSignature + signature certificate on the eSignature	Services requiring an electronic signature

[10] Official Gazzette, April 20, 2006, Number: 26145; http://www.bilgitoplumu.gov.tr/mevzuat/e-DevletKapisi_20060420.pdf

Thus, there are three levels of authentication above public access: basic username/password (after registration using national identity numbers), use of PASSWORD printed and closed on an ENVELOPE via a strictly secure way then delivered by PTT personnel (being the governmental institution legally authorized to serve official communications) and use of the e-signature card's signature and authentication.

The National e-ID Card Project

In 2006, the Social Security Institution initiated the Electronic Social Security Card Project. The stakeholders of the project included all the citizens integrated in the social security system. Since almost all citizens are covered by the social security system, it was decided to revise the Electronic Social Security Card Project into a national e-ID Card Project and the Ministry of Interior, General Directorate of Civil Registration and Nationality was assigned with the responsibility for the coordination of the project within the Information Society Strategy Action Plan[11] (Action No 46).

Pursuant to the Prime Ministry Circular No: 2007/16, dated 04.07.2007[12], the new e-ID card will contain only static personal information and biometrics (fingerprints) and will only be used for identification and authentication purposes. Agency and/or service-based smart card applications will not be allowed. The card will be in ID-1 format equipped with sufficient visual and forensic security features, contain contact chip developed by TUBITAK (The Scientific and Technological Research Council of Turkey), taking into account relevant international standards, most notably the emerging CEN 15480 and ISO 24727 standards. The first stage of the pilot phase, development of chip and operating system is complete. The second stage of the pilot phase is to be initiated in early 2008 where 10.000 cards will be tested in cooperation with Social Security Institution and the Ministry of Health within a district. The third stage of piloting will cover testing the card for 300.000 people within a province. The pilot will be followed by a country-wide implementation by 2010.

e-Passport

The e-Passport Issuance Project aims at the production of electronic passports that are in conformity with ICAO and European standards.

The tendering process of this Project has been finalised and issuance of the new generation passports is planned to commence during the first quarter of 2009.

Following the completion of the Project, utilization of electronic passports that work with RFID includes the specification of machine readability. The new generation passports feature RFID chip which contain fingerprints.

Qualified Electronic Certificates

After the Electronic Signature Law No 5070 entered into force, the use of electronic signature that has the same legal effect as a hand written signature has been initiated. Four electronic certificate service

[11] http://www.bilgitoplumu.gov.tr/btstrateji/Eylem_Plani.pdf

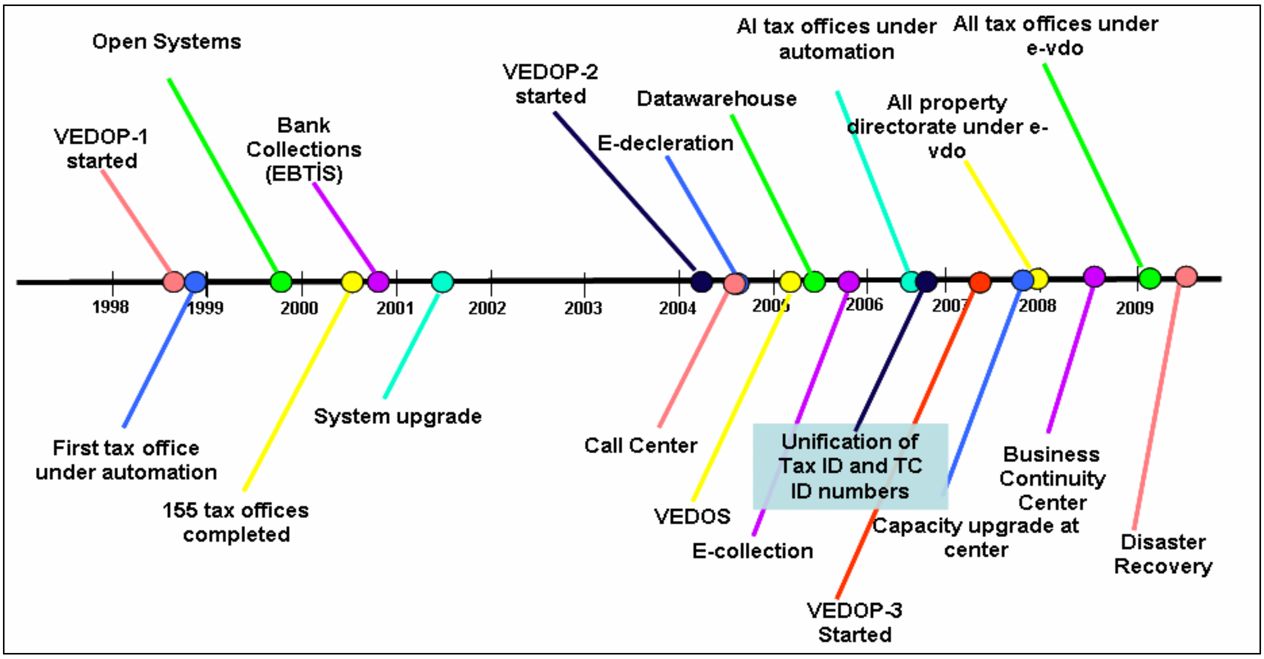
[12] http://www.basbakanlik.gov.tr/genelge_pdf/2007/2007-0010-006-08281.pdf#page=3

providers that have notified to the Telecommunications Authority continue their activities under the scope of the Law[13]. Four electronic certificate service providers have issued approximately twelve thousand qualified electronic certificates in total as of end of 2006. This number definitely does not meet the expectations of both the sector and the administration. As a result of the experience gained with the electronic signature applications, it is observed that there is a direct connection between the number of qualified electronic certificates and the number of mandatory e-Government applications with electronic signature infrastructure. Therefore, various studies are being carried out in order to provide the integration of electronic signatures in e-Government applications and the improvement of e-Government applications with electronic signature infrastructure.

Aside from the improvement of electronic signature applications, studies for facilitating and generalising the use of electronic signature are also being carried out. In that line, a mobile signature project has been developed by a GSM operator and an electronic certificate service provider, and the project has been implemented as of March 2007. Within the mobile signature project, the GSM operator also functions with the capacity of the registration authority.

VEDOP[14]

Revenue Administration, accomplished an integrated country-wide Tax Office Automation Project called VEDOP (VErgi Dairesi Otomasyon Projesi). It is used in 448 Tax offices, 52 district treasurers, 29 district tax office commissions and Revenue Administration Headquarters. VEDOP fully automates tax administration tasks and establishes a decision making and management information system in the Data Processing Centre of Revenue Administration.


Open Systems
VEDOP-1 started
Bank Collections (EBTİS)
VEDOP-2 started
E-decleration
Datawarehouse
Al tax offices under automation
All property directorate under e-vdo
All tax offices under e-vdo
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
First tax office under automation
155 tax offices completed
System upgrade
Call Center
VEDOS
E-collection
Unification of Tax ID and TC ID numbers
VEDOP-3 Started
Capacity upgrade at center
Business Continuity Center
Disaster Recovery

[13] e-Guven www.e-guven.com, Turktrust www.turktrust.com, e-Tugra www.e-tugra.com, Kamu SM http://www.kamusm.gov.tr/

[14] http://www.maliye.gov.tr/kalite/kitap/bolum2_d3.pdf.

Figure : VEDOP Timeline

Tax ID Registration

Since 1995, the Ministry of Finance is assigning a life long unique ID number to registered tax payers. In total of 43,213,826 unique Tax ID numbers are registered to date for active and potential tax payers. Since the unification of Tax ID number and Turkish Republic (TR) ID Number in 2006 real persons can use their TR ID numbers where Tax ID number is required. Tax payer information is queried online from the Identity Sharing System using their TR ID number on registration.

The ID numbers are used for the following operations:

- Vehicle Registration and trade in cooperation with the Ministry of Interior
- Real Estate trading, land registry and mortgages
- Banking and Financial operations
- Founding a company

e-VDO Operations (Fully Automated Tax Office WEB Application)

The tax officers can perform all tax functions using e-VDO, the OLTP application. All operations require the identification of tax payers using either Tax ID or TR ID numbers.

All the produced documents include TR ID number for real persons and Tax ID number for legal entities.

Over 25,000 tax officers are authenticated and authorized using their TR ID numbers to the VEDOP applications.

e-Declaration Application

The tax payers file their tax returns electronically with ***e-Declaration*** application feature of VEDOP since October 2004. With this application, tax payers will no longer have to go to the tax administrations to file their tax returns, thus saving time and work and minimizing costs. It is aimed to utilize the application in a way that all other services carried out in tax administrations will be also available in the electronic media.

E-Declaration application is implemented by means of encrypted data transfer through the Internet.

The tax payers file 85% of Income Tax, 88% of VAT and 99.45% of Corporate Tax returns via e-Declaration though it is not mandatory.

E-Collection via Banks

Tax payers can get their accrual via tax offices or online via e-Declaration and they can pay through banks or tax offices. The collections by banks require banks to identify the tax payer with either Tax ID or TR ID number to query amount of tax due online from Revenue administration database. Also the collections are sent to Revenue Administration with the same IDs for matching the collection to the accrual.

Data Warehouse

All taxation related financial operations are matched and connected using Tax ID or TR ID number of the involved parties. Invoices over a predefined amount are filed annually and plans include incorporating all invoices' data into this data warehouse in the scope of the currently developing e-

Invoice project. The related planned project e-Haciz (seizure) will use both IDs to execute seizure non compliant tax payers' bank accounts.

Tax Auditing Units

More than 2000 tax auditors are using the fully integrated taxation data to make their audit cases which are selected by the data warehouse. They track the taxpayer relations via Tax ID or TR ID numbers.

Management Information System

The high management of Revenue Administration and all auditing and inspecting units can access and use the tax payers' records with access privilege levels assigned to them. These records are identified by Tax ID or TR ID numbers.

NATIONAL JUDICIARY NETWORK PROJECT (UYAP)[15]

General Information

The Ministry of Justice has prepared a "National Judiciary Information System (UYAP)", which is to implement an information system between the Courts and all other institutions of the Ministry, including prisons. UYAP is an e-justice system as a component of the comprehensive Turkish e-government initiative. It has been developed in order to ensure fast, reliable, soundly operated and accurate judicial system. As a central network project it covers judicial institutions such as courts, public prosecutors services, prisons and other government departments in Turkey. UYAP equipped these institutions with computers, network and internet connection and given them access to all legislation texts, the precedents of the Court of Cassation and other judicial records (i.e. criminal records, police records etc.).

The project started in 2000 and is expected to be completed by the end of 2007. By this date, all the judiciary processes, transactions and trials will have been moved to the electronic environment.

Thus, UYAP not only networked judicial institutions but is also ready to interoperate with other government institutions, criminal records and the judicial record database will be accessed on-line. All cases in courts can be accessible on line by judges. After full integration with other public databases, the birth certificate registrations can also be accessed online, land registries and driver registers can be retrieved instantly at the beginning of the trials.

Citizen Portal[16]

Citizens can access and examine their case information via Internet and learn the day of the trial without going courts. They can be informed via web site about their cases or hearing dates. They can submit their petitions to court by electronic signature and review their files over the internet. Text messages for court attendance can be sent by the system. It also allows users to ask for alerts to be sent to them whenever any chosen event occurs, by email or text messaging.

[15] http://www.uyap.gov.tr

[16] http://vatandas.adalet.gov.tr/proxy/lib/vatandas.html

Lawyer Portal[17]

The Lawyer Portal is open only for certificated lawyers. The system enables the lawyers to review the stages of their lawsuits or to learn the date of hearing on-line. It also enables lawyers to deposit fee, to take legal action from their office, provides them with access their dossiers data and documents. Lawyers are provided with a password on a CD for accessing the system. Smart cards and tokens are not used. The portal also supports electronic signature, in fact some procedures requires e-signature to be finalized. On the other hand, some of the bar associations asked electronic certification service providers to combine the e- signatures and the logon certificate given by the Ministry of Justice in the same smart card for user convenience.

UYAP is currently being used by over 40.000 users, 130 Heavy Penalty Courts, 23 District Administrative Courts, all Prisons and Detention Houses, 509 Rural Courthouses, and 8680 Courts in total. Roll out rate of UYAP is approximately 90%.

The project was awarded twice (in 2004 and 2005) annual e-government prize due to its significant contribution to the justice system.

3.3.2 Legal framework

Information regarding legal framework for the projects mentioned in this report are presented as follows:

- Republic of Turkey Identity Number was implemented in all e-government applications upon the Circular of The Prime Ministry dated 20 June 2002[18].
- The Under Secretariat of State Planning Organization is assigned with the monitoring, coordination, evaluation and the direction of e-Transformation Turkey Project by the Circular No 2003/12 dated 27 February 2003 which specifies the purpose, organisational structure and application principles of the e-Transformation Turkey Project[19].
- By virtue of the Law No 5070 that has entered into force in 23 July 2004 following its publication on the Official Gazette dated 23 January 2004, the legal framework is set forth regarding the legal structure of the electronic signature, the activities of the electronic certificate service providers and transactions regarding the use of electronic signature in all fields, except in cases when the presence of person is stipulated by the Law. By virtue of Article 5 of the Law it is provided that secure electronic signatures have the same effect as the hand written signature[20].
- By virtue of the Circular of the Prime Ministry No 2004/21, published in the Official Gazette dated 06 September 2004 it has been decided to establish a Public

[17] http://www.uyap.gov.tr/avukatport/avukat.htm.

[18] T.C. Kimlik Numaras•, 2002/22 say•l• Ba•bakanl•k Genelgesi

[19] 27 • ubat 2003 tarihli ve 2003/12 say•l• Ba•bakanl•k Genelgesi

[20] 15 Ocak 2004 tarihli ve 5070 say•l• Elektronik •mza Kanunu

Certification Centre in order to meet the needs of public bodies and institutions for corporate certificates ensuring the electronic signature applications to work in an interoperable and compatible manner in all public bodies and institutions[21].

- The Guide for Interoperability has entered into force with the Circular of the Prime Ministry No 2005/20 dated 04 August 2005[22].
- By virtue of the Decision of the Council of Ministers No 2006/10316, published in the Official Gazette dated 20.04.2006, the establishment, operation and management of the e-Government Gateway is stipulated and the authorization thereof is granted to TURKSAT [23].
- Civil Registration Services Law No 5490[24], dated 29.04.2006, introduces, among others, the Address Registration System and the register of aliens, and regulates all aspects of civil registration.
- The Prime Ministry Circular No 26572[25], dated 04.07.2007, specifies the implementation details of Action No 46 of the Information Society Strategy Action Plan regarding the new e-ID Card Project.

3.3.3 Technical aspects

Secure Electronic Signature and Qualified Electronic Certificates

The Electronic Signature Law No 5070 and its by-laws determine the criteria and the international standards, which the secure electronic signatures to be used in the electronic signature application, the signature creation devices, the devices to be used and the security measures to be abided by the electronic certificate service providers, the processes of secure electronic signature creation and verification shall comply with.

According to the “Communiqué on Processes and Technical Criteria Regarding Electronic Signatures” prepared by Telecommunications Authority:

- Electronic Certificate Service Provider (ECSP) shall apply the following standards to its all operational phases;
  - § ETSI TS 101 456 and
  - § CWA 14167-1
- Qualified electronic certificates shall be generated in conformity with the following documents;
  - § ETSI TS 101 862 and
  - § ITU-T Rec. X.509 V.3

[21] 6 Eylül 2004 tarihli ve 2004/21 say•l• Kamu Sertifikasyon Merkezi Olu•turulmas• Hakk•nda Ba•bakanl•k Genelgesi

[22] Birlikte Çal••abilirlik Rehberi

[23] 2006/10316 Say•l• Bakanlar Kurulu Karar•

[24] http://www.nvi.gov.tr/attached/nvi/nufus_mevzuati_pdf/kanun_pdf/nufus_kanunu.pdf

[25] http://www.basbakanlik.gov.tr/genelge_pdf/2007/2007-0010-006-08281.pdf#page=3

- Signature creation and verification data and hash algorithms shall be generated in conformity with ETSI TS 102 176-1 standard and the following algorithms and parameters;
  - § Signature creation and verification data of signature owner
    - • at least 1024 bits for RSA or
    - • at least 1024 bits for DSA or
    - • at least 163 bits for ECDSA
  - § Signature creation and verification data of ECSP
    - • at least 2048 bits for RSA or
    - • at least 2048 bits for DSA or
    - • at least 256 bits for ECDSA
  - § Hash algorithms
    - RIPEMD-160 or
    - SHA-1 or
    - SHA-224 or
    - SHA-256 or
    - WHIRLPOOL

- ECSP shall prepare CP and CPS conformant to IETF RFC 3647.
- Secure signature creation devices shall be conformant to CWA 14169 or assured to EAL4+ in accordance to ISO/IEC 15408 (-1,-2,-3).
- Secure Signature Verification Devices (SSVD) supplied by an ECSP shall be conformant to CWA 14171 and ECSP shall also make a declaration of conformity for these SSVDs.
- ECSP shall adapt following standards for its security;
  - § CWA 14167-1,
  - § ETSI TS 101 456 and
  - § TS ISO/IEC 17799 or ISO/IEC 17799
- ECSP shall meet the following requirements regarding time-stamps and time-stamping services;
  - § CWA 14167-1 and
  - § ETSI TS 101 861
- Time-stamp policy and time-stamping practice statement shall be prepared conformant to ETSI TS 102 023.
- ECSP shall be awarded the following certificate(s) obtained from authorized institutions or organizations;
  - § TS ISO/IEC 27001 or ISO/IEC 27001, and

§ for its Secure Signature Creation Devices showing that they either;

- Meet the requirements identified in FIPS PUB 140-1 or FIPS PUB 140-2 level 3 or higher, or
- Meet the requirements identified in CWA 14167-2, or
- Meet the requirements identified in CWA 14169 and assured to EAL4+ or higher in accordance to TS ISO/IEC 15408 (-1,-2,-3) or ISO/IEC 15408 (-1,-2,-3)

- It is recommended by the Telecommunication Authority that the process of electronic signature creation shall comply with CWA 14170 document, whereas the electronic signature formats shall comply with ETSI TS 101733 and/or ETSI TS 101 903 documents.

The links regarding the root certificates and the repositories containing the certificate practice statements and certificate policies of the four electronic certificate service providers operating in Turkey, are as follows:

- e-Guven: http://www.e-guven.com/
- Turktrust: http://www.turktrust.com.tr/
- e-Tugra: http://www.e-tugra.com/
- Kamu SM: http://www.kamusm.gov.tr/

Electronic certificate service providers issue the qualified electronic certificates by signing them with their own root certificates. It is not required for the root certificates of the electronic certificate service providers to be signed by an authorized institution but it is stipulated that the electronic certificate service providers shall publish their root certificates on their own websites and announce the hash value of their root certificates by publishing it in the newspapers. So far, the existing electronic certificate service providers have not cross certified with other certification authorities neither domestic nor foreign, and there is no existing bridge CA structure either.

3.3.4 Organisational aspects

With respect to e-Government applications in Turkey, each application manages its own electronic identity system. And as for the applications with electronic signature infrastructure, the qualified electronic certificates are provided by the electronic certificate service providers that started to operate after their notification to the Telecommunication Authority. Upon the completion of the e-Government Gateway Project, the portal will be accessible both via electronic signature and via the usernames/passwords to be provided by TURKSAT.

In the electronic signature application, electronic certificate service providers are responsible for the correctness of the identity information placed in the qualified electronic certificates. For the purposes of verifying the identity information, certificate service providers make a face to face identity control relying on official certificates and compare the identity information at hand with that contained in the MERNIS Database. According to Electronic Signature Law No 5070, upon the request of an individual who applies for qualified electronic certificate, information regarding the authority, role and profession shall be placed in the certificate, however since the electronic certificate service providers do not encounter such requests in practice, the existing certificates do not contain information in the aforementioned context. Issues such as how to regulate the information regarding role and authority, related diagrams and standardization studies have been discussed during the meetings of the National Electronic Signature Coordination Board, nevertheless no official study has been taken up yet.

Since the database in the MERNIS Project is maintained by the Ministry of Interior, the General Directorate of Civil Registration and Nationality, based on the civil registration data, a separate verification system is not being used as the accuracy of the said information falls under the responsibility of the said administration. Most of the e-Government applications using their own eIDM systems verify identity information through the MERNIS database.

3.4 Interoperability

It is not possible to say that there is a complete interoperability between the existing e-Government Applications in Turkey. Since each e-Government application uses its own authentication mechanism, there is no interoperability between those mechanisms either. The only structure, where interoperability is provided, is the electronic signature. However, the e-Government Gateway Project aims to provide interoperability between all e-Government applications in terms of authentication systems by providing a single authentication system and a central share point for web services. In addition, Guide for Interoperability has been prepared in order to provide interoperability between the e-Government applications in general. In certain sections of the guide authentication systems are also mentioned; it is expected that the forthcoming versions of the Guide will be centred more on authentication systems.[26]

The Guide for Interoperability that was drawn up with a participative approach under the coordination of State Planning Organisation aims to provide benefits in terms of the efficiency of the public investments in information and communication technologies. The Guide was prepared within the frame of “determining the interoperability principles and publishing a guide thereof” as set forth by the e-Transformation Turkey Project Short Term Action Plan (KDEP) and under the coordination of the State Planning Organisation with the maximum effort to reach all concerned parties from private sector and the NGOs that may contribute. As it contains technical elements, it will improve, enlarge and comply with the changes in time and it has the character of a document which is open to the contribution from all parts of the society.

The principles that were drawn up cover the technical aspects of interoperability needs in three dimensions: ensuring interoperability on the application level by means of the minimum common standards to be abided by the institutions; setting the tools to be used in satisfying the needs in higher layers (such as conceptual and organisational needs); and determining the minimum common standards to be abided by in the proposed investments.

Determination of the services to be provided and accessed from the common platform (e-Government Gateway Project), determination of the organisational needs, modelling of the business flows regarding these services and developing applications are not under the scope of this Guide,

[26] http://www.bilgitoplumu.gov.tr/yayin/2005BirlikteCal•sabilirlikRehberi.pdf., August 2005.

which only sets policies and standards to be complied with by public institutions providing services. While setting forth the principles, compliance with the studies of the European Commission is ensured and the studies that are carried out and the reports that are drawn up within the scope of Interchange of Data between Administrations Program (IDA), were taken as a reference.

3.5 eIDM Applications

As mentioned before in this Report, there is no general electronic identity system in Turkey as each application has its own electronic identity system. Only the Inward Processing (DIR) Project and the Free Zones Project[27] that are implemented by the Under Secretariat of Foreign Trade do not use their own electronic identity systems. Since the e-Government Gateway Project is not operational yet, the identification verification is conducted by means of electronic signatures, which are created by qualified electronic certificates provided by electronic certificate service providers.

DIR Automation Project ensures the implementation of the process from the stage of issuing Inward Processing Permission Documents to the stage where the commitment accounts are closed, through internet by means of a web based program.

As for the Free Zones Project, it aims the transfer of activities conducted in free zones to the electronic environment, to form a healthy database regarding the zones and to monitor the free zone transactions, to provide integration between the Under Secretariat of Foreign Trade and the Directorates of Free Zone, Companies, Customs, Turkish Statistical Institute and other related institutions in a manner that will facilitate the data flow from the free zones and finally to ensure the implementation of the transactions with the use of electronic signature.

3.6 Future trends/expectations

As mentioned above, the Action No 46 of the Information Society Strategy Action Plan has envisaged the development of a new electronic identity card. The card will have a contact chip on it containing minimum set of personal data and biometrics and will be used for identification and authentication purposes only. The card's body will contain forensic and visual security features. The project is scheduled to be completed by 2010. With the commencement of the project, issuance of other cards by public entities will not be allowed.

[27] https://edtm.dtm.gov.tr/basvuru/giris.jsp

3.7 Assessment

There are different and individual eIDM systems used in e-Government applications in Turkey. Furthermore, the legal framework concerning the electronic signature has been completed and their application, albeit on a limited scale, has started. Aside from the electronic signature, for the authentication in e-Government Gateway, user names and passwords will also be used and they will be distributed to the users by TURKSAT who is assigned with operation of the e-Government Gateway. As to the MERNIS database, which is the biggest electronic identity warehouses in Turkey, it does not offer electronic e-authentication on its own but is used as a basis for authentications conducted with other systems. Therefore, it is not possible to call MERNIS exactly an e-IDM system in the context of e-ID interoperability. As it can be seen, there is no national eIDM system yet within the existing structure in Turkey. Nevertheless, the policy has been set with the Information Society Strategy and the work is in progress in this regard.

As the authentication systems of most of the existing e-Government applications are based on usernames/passwords, such systems fail to provide a solution that is secure and efficient enough. In case of any dispute there may be difficulties, since the serving of the data formed by such services as evidence before the courts and the responsibility structures are not settled yet (the contradiction between the users responsibility to protect his/her password and the service provider's responsibility to establish requisite security measures as well as the approval mechanisms).

Despite the existence of many lawsuits and disputes in the private sector due to the existing authentication systems, there are no disputes or lawsuits arising from the e-Government applications just as yet. Nevertheless, such risk is likely to materialise upon the widespread application of e-Government.

As mentioned above, merely the electronic signature and the national e-identity card, which is still being developed, can be deemed as eIDM systems. Electronic signatures are not widely used because the distribution channels are not widespread and due to the lack of applications using electronic signature infrastructure. Users do not prefer electronic signatures due to relatively their high prices and lack of applications, whereas on the other hand, the application developers fail to develop applications due to the low electronic certificate penetration. Electronic signatures fail to become widespread in Turkey due to this double sided reservation. As a solution to this problem, studies are still being carried out by the administration in order to develop mandatory electronic signature applications.