Preliminary study on Mutual Recognition of eSignatures for eGovernment applications

NATIONAL PROFILE TURKEY

April 2007
This report / paper was prepared for the IDABC programme by:

Author’s name: Aylin AKCA OKAN, Siemens
Company’s name: Siemens - Lawfort
Company’s address (optional):
Company’s logo (optional)

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

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/

© European Communities, 2007
Reproduction is authorised, except for commercial purposes, provided the source is acknowledged.
Executive summary

The objective of the project is to analyse the requirements in terms of interoperability of electronic signatures for different eGovernment applications and services taking into account the relevant provisions of Directive 1999/93/EC on a Community framework for electronic signatures and their national implementation as well as the report on the Directive and the standardisation activities on the interoperability of electronic signatures.

This document represents the current situation regarding the use of eSignatures in Turkish eGovernment applications.
# Table of Contents

**EXECUTIVE SUMMARY**

1 DOCUMENTS
   1.1 APPLICABLE DOCUMENTS
   1.2 REFERENCE DOCUMENTS

2 GLOSSARY
   2.1 DEFINITIONS
   2.2 ACRONYMS

3 INTRODUCTION AND INSTRUCTIONS FOR SUBMISSION
   3.1 GENERAL OVERVIEW OF THE PROFILES' PURPOSE
   3.2 STRUCTURE AND CONTENT OF THE PROFILE
   3.3 RELEVANT SOURCES AND REFERENCES
   3.4 COPYRIGHT AND CREDITS

4 QUESTIONNAIRE
   4.1 GENERAL INTRODUCTION
   4.2 ORGANIZATION, ROLES & TARGETS
   4.3 CERTIFICATION AUTHORITY FOR THE GOVERNMENT
   4.4 EGOVERNMENT AND ESIGNATURE REGULATIONS
      4.4.1 ESIGNATURES REGULATORY FRAMEWORK
         4.4.1.1 History
         4.4.1.2 Scope and Coverage
      4.4.2 EGOVERNMENT REGULATORY FRAMEWORK
         4.4.2.1 Principles to be Followed Telecommunication Board in Regulating e-signature Services
         4.4.2.2 Conditions in order to operate as Certificate Service Provider
         4.4.2.3 The Duties of CSPs
         4.4.2.4 Termination of the services by the Board
         4.4.2.5 Cancellation of the Certificates and the CSPs deciding to terminate their services
         4.4.2.6 Activity Reports
         4.4.2.7 The legal liability of the CSPs
         4.4.2.8 Certificate Liability Insurance
         4.4.2.9 Foreign Electronic Certificates
      4.4.3 TURKISH ELECTRONIC SIGNATURE LAW
4.5  eGOVERNMENT APPLICATIONS USING ELECTRONIC SIGNATURES
  4.5.1  GENERAL PROCESS
  4.5.2  STANDARDIZATION ASPECT OF ELECTRONIC SIGNATURE AND SOME FIGURES
  4.5.3  INWARD PROCESSING REGIME - UNDERSECRETARIAT OF FOREIGN TRADE
  4.5.4  ePROCUREMENT INFRASTRUCTURE
    4.5.4.1  Government Supply Office Electronic Sale Project (e-Sale)
    4.5.4.2  Public Procurement Agency Electronic Public Procurement Platform

4.6  GENERAL ASSESSMENT

5  ANNEX A: CONTACT DETAILS OF NATIONAL CORRESPONDENTS

6  ANNEX B: NATIONAL REGULATIONS DETAILS

7  ANNEX C: APPLICATION QUESTIONNAIRE
  7.1  INWARD PROCESSING REGIME - UNDERSECRETARIAT OF FOREIGN TRADE
    7.1.1  APPLICATION IDENTIFICATION
    7.1.2  eSIGNATURE DETAILS
    7.1.3  INTEROPERABILITY
    7.1.4  MISCELLANEOUS
    7.1.5  ASSESSMENT
1 Documents

1.1 Applicable Documents

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

1.2 Reference Documents

| [RD2] | European Electronic Signatures Study |
| [RD6] | IDABC Work Programme Third Revision |
| [RD8] | Turkish Laws & Regulations regarding the e-Signature |
http://www.tkgov.tr/eng/duzenmaineng2.html (ENG)
2 Glossary

2.1 Definitions

In the course of this Questionnaire, 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.

- **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.

It should be noted that for the purposes of this questionnaire, only services which rely on eSignatures are relevant, and that the focus is on eGovernment applications offered to citizens and businesses (A2C and A2B, rather than A2A).

- **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. However, PKI solutions are the principal focus of this questionnaire, and non-PKI solutions should only be included if no PKI solutions are in common use. It should also be noted that the questionnaire only examines eGovernment applications in which the eSignature is used to sign a specific transaction, and not where the signature is merely used as a method of authentication of the eSignature holder as defined below.

- **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;

- **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 Directive1.

---

o **Authentication:** 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”). It should be noted that the questionnaire is focused on the use of eSignatures as a method of signing a transaction, and not on their use as a method for authenticating the eSignature holder.

o **Relying party:** any individual or organisation that acts in reliance on a certificate (in a PKI solution) or a eSignature.

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

### 2.2 Acronyms

**A2A** ............... Administration to Administration  
**A2B** ............... Administration to Businesses  
**A2C** ............... Administration to Citizens  
**BS** ............... British Standards  
**CEN** ............... Comité Européen de Normalisation  
**CIO** ............... Chief Information Officer  
**CP** ............... Certification Policy  
**CPS** ............... Certification Practice Statements  
**CRL** ............... Certificate Revocation Lists  
**CSP** ............... Certificate Service Provider  
**CWA** ............... CEN Workshop Agreement  
**DSA** ............... Digital Signature Algorithm  
**EAL** ............... Evaluation Assurance Level  
**ECDSA** ............ Elliptical Curve DSA  
**eID** ............... Electronic Identity  
**ETSI** ............... European Telecommunications Standards Institute  
**ETSI SR** .......... ETSI Special Report  
**ETSI TS** .......... ETSI Technical Specification
FIPS PUB........ Federal Information Processing Standards Publications
ICT .................. Information & Communication Technologies
IETF RFC......... Internet Engineering Task Force Request for Comments
ISO/IEC.......... International Organization for Standardization / International Electrotechnical Committee
ITU .................. International Telecommunications Union
KSM .................. Public Certification Center (Kamu Sertifikasyon Merkezi)
NGO ................. Non-Governmental Organization
OCSP ............... Online Certificate Status Protocol
PKI .................. Public Key Infrastructure
RIPEMD .......... RACE Integrity Primitives Evaluation Message Digest
RSA .................. Rivest-Shamir-Adleman
SCVP ............... Simple Certificate Validation Protocol
SHA .................. Secure Hash Algorithm
SME .................. Small and Medium-sized Enterprises
SPO .................. State Planning Organization
SSCD ............... Secure Signature Creation Device
STAP ............... Short Term Action Plan
TTP .................. Trusted Third Party
TÜB-TAK ........ Scientific and Technological Research Council of Turkey (Turkiye Bilimsel ve Teknolojik Arastirma Kurumu)
UAP .................. Urgent Action Plan
UEKAE .......... National Research Institute of Electronic and Cryptology (Ulusal Elektronik ve Kriptoloji Arastirma Enstitusu)
3 Introduction and instructions for submission

3.1 General overview of the profiles’ purpose

The IDABC Study Team, consisting of Siemens Business Services and Lawfort, has been contracted by the European Commission – DG Enterprise (hereinafter the Commission) to perform a Study (hereinafter the Study) in the context of the European Community Programme for the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (hereinafter IDABC). For more information on the IDABC Work Programme, see [RD6].

The objective of IDABC is to identify, support and promote the development and establishment of pan-European eGovernment services and the underlying interoperable telematic networks supporting the Member States and the European Community in the implementation, within their respective areas of competence, of Community policies and activities, achieving substantial benefits for public administrations, businesses and citizens.

The objective of the Study is to analyse the requirements in terms of interoperability of electronic signatures for different eGovernment applications and services taking into account the relevant provisions of Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures ([RD3]) and their national implementation as well as the report on the Directive and the standardisation activities on the interoperability of electronic signatures.

As part of the Study, the Study Team must provide an extensive overview of currently existing or envisaged relevant eGovernment applications in all Member States, which make use of electronic signatures (e.g. for public procurement, tax and social security declarations, request and delivery of documents, etc.).

Per Member State, a profile must be created and describe for each application the type of electronic signature legally required, the technical implementation of the interface between the application and the used electronic signature, the applicable technical restrictions notably regarding interoperability with non-national electronic signature and the authorities or institutions that have been contacted to obtain information. The Study Team has decided to meet this requirement through a network of national correspondents, who will assist the Study Team in drafting a national profile for their State.

The Study focuses on signature applications with regard to the interaction between governmental authorities and the public (A2B and A2C services, i.e. services to citizens, professionals, companies). Purely internal interactions (A2A services, i.e. the eGovernment back-office) as such are not within the scope of the Study. However, when eGovernment applications relying on electronic signatures have been specifically designed with cross-border functionality in mind (e.g. the exchange of criminal records between judicial or law enforcement entities), such applications are within the scope of the Study.

Applications merely serving entity authentication purposes (i.e. not involving electronic signatures) are not the aim of the Study and should therefore only be mentioned if this is deemed appropriate.

The objective of the programme of which this Study is a part, is to make progress in the field of interoperability of electronic signature applications between Member States. This emphasis should be taken into account when drafting the country profiles.

The results of the Study must allow the elaboration of a strategy on the required inputs and components to produce an interoperability solution for secure electronic signatures (including but not limited to eIDs).
The current document is a guideline for the national correspondents. It contains two major sections:

- The instructions which you are currently reading (section 3);
- The specific questions to be addressed by the national profiles (section 4).

In addition, a draft profile of Belgium will be delivered as an Annex to the Questionnaire. This draft profile will serve as a template for national correspondents, by giving them a more direct example of the expected input. National correspondents are invited to first read through this introduction and the guidelines, and to subsequently create their own State’s profile using the model report for Belgium as an example.

### 3.2 Structure and content of the profile

The profiles should provide a clear and concise analysis of existing or envisaged signature-based eGovernment applications in the correspondent’s State.

The national profiles will cover the following sections, which will be further detailed below:

1. **General eGovernment structure (focused on electronic signature-related issues):** a brief overview of the country’s eGovernment structure, the main governmental drivers of eGovernment and cooperation between the various governmental levels, general situation of electronic signatures (max. 2 pages).

2. **Legal framework for eGovernment and eSignatures:** an overview of the country’s general electronic signature legislation (specifically focusing on the transposition of the European eSignatures directive 1999/93/EC ([RD3](#)) and specific legal provisions for the use of electronic signatures in eGovernment applications (max. 2 pages).

3. **An overview of eGovernment applications using electronic signatures:** a list and description of the main eGovernment applications making use of electronic signatures, with for each application an overview of the legal and technical characteristics of the used signature. This should include a description of the technical implementation, i.e. an indication of how the signature is integrated into the application of the electronic signature. The section below indicates which sectors should be covered by the report. In any case, it is mandatory to describe every e-Procurement application. For the most relevant applications, the questionnaire as presented in [Annex C: Application questionnaire](#) must be filled in and provided as annex to the Country Profile.

4. **General assessment:** while the Study Team will assess the provided information separately, the national correspondents are requested to evaluate their own legal and technical eGovernment framework in the following section, as a provisional conclusion to their profile. As this assessment is provisional, it may be brief (1-1.5 pages total).

National correspondents are required to maintain the structure outlined above, and may not omit or disregard any sections.
3.3 Relevant sources and references

National correspondents are required to include references to the legal sources that they have consulted. This includes references to laws, other regulations, and doctrine, in such a manner that a legal expert with knowledge of the national legal system would be able to retrieve the sources.

As the Study examines not only the legal framework and its impact in day to day eGovernment practice, but also the resulting technical implementation, national correspondents are asked to keep into account existing administrative practices in eGovernment, and assess whether or not any given solution is actually used in practice (and if not, to identify the reason why). For this reason, the consultation of national governmental bodies, relevant organisations and trusted third parties (TTPs) is mandatory.

In order to allow the Study Team to conduct follow-up research, the list of contacted authorities and persons in the national administrations, including the dates of their interviews, must be provided.

Whenever referring to national regulations or institutions, the correspondents are required to provide the local name as well as an English language translation of the regulation’s title.

If available, links to on-line resources (legislation, judicial decisions, governmental websites, and professional organisations) should be included.

Concretely the following forms have to be filled in and annexed to the country profile:

- Annex A: Contact details of National Correspondents
- Annex B: National Regulations Details

3.4 Copyright and credits

Copyright of all contributions will be transferred to the Commission, who may use the information without restriction. The information may be reproduced, reused, and disseminated in its original, edited or abbreviated form by the Commission, including through print publications or on-line in electronic form, although the Commission is not required to do so.

The contributing authors will be credited as the main source of the contribution in the final draft of the Study Team’s report. Only the person directly contacted by the Study Team will be credited as the main source of the contribution, unless this person explicitly asks that other persons be mentioned as well.

The affiliation of the contributor (e.g. law firms, university, public institute,…) will be mentioned if it is known to the Study Team unless the contributor opposes this.

The Study Team reserves the right to edit the contributions of national correspondents before submitting a final result to the Commission.
4 Questionnaire

4.1 General introduction

The Turkish State is a Republic (Constitution Art.1) and Turkish Republic is a democratic, secular and social state governed by the rule of law (Constitution Art.2). As for the administrative structuring, Turkey consists of 81 provinces, 933 districts (sub regions of provinces) and 3226 municipality. Since Turkey is a unitary state; the laws are binding throughout the whole country. As Turkey is a member of the Continental Europe Civil Law System; just like all the laws of the Country, Commercial Code and Code of Obligations reflect the features of the said law system. Commercial Code being a separate and individual Code is under the influence of Laws of many European countries. The Code of Obligations constituting an integral part of the Civil Code is adopted from Swiss Civil Code - Code of Obligations. Currently alongside with numerous laws; the draft amendments of both the Commercial Code and the Code of Obligations have been prepared in order to ensure the legal harmonization in line with the EU negotiation process.

The Judicial Courts in Turkey are organs charged with criminal and civil As the Budapest Ministerial Conference, held in February 2004, has brought the eEurope+ Initiative to conclusion, Turkey, along with other candidate countries have become a part of eEurope 2005. Turkey has speeded up her efforts to transform into an information society as she joined eEurope+ together with other candidate countries. It is a fact that there has been little progress in the past in Turkey. But soon after the eEurope+ Initiative, Turkey started a new program, eTurkey Initiative, which is almost identical to eEurope+, and gathered different projects under one umbrella.

Turkey has embraced the common goals and priorities with other EU member and candidate countries since the eEurope+ Action Plan in June 2001. Through coordination among all stakeholders and public consultations, Turkish Government is striving to make sure that public institutions, civil society organizations, and citizens are aware of the potential benefits of information society. Along with other coordination activities, e-Government lies at the core of these efforts. Bearing in mind that the recent public administration reform studies are at the top of the Government’s agenda, e-Government has been emphasized more than before in the last couple of years.

In Turkey, eGovernment projects are underway for years, and an integrated e-government approach that incorporates those separate applications has been recently put on the agenda of the government. With the launch of e-Transformation Project in November 2002, a new integrated approach has been adopted. Until recently, policy-making and coordination in e-government issues has been quite vague. This has resulted in negligence of some important issues such as interoperability, one-stop shop portal, access channels and so forth.

Since the previous government took place in December 2002, there is a new approach that urges public institutions to take necessary measures in order to remedy longterm problems, like financial stability, public management, social security administration, agriculture, and manufacturing. These actions on the most needed areas of interest are combined in Urgent Action Plan (UAP), which takes place in the core of 58th and 59th Governments’ Program. As part of this Urgent Action Plan’s Public Management Reform Section, transformation into an information society was declared as one of the most significant projects. e-Transformation Turkey Project aims at fostering the evolution and coordination of information society activities, which were previously carried out in a decentralized and uncoordinated manner.

Since the early 2000s, initiatives towards transformation into an information society are observed to be increasing all around the world. New products and services as well as increased productivity stemming from the developments in the ICT have also started to change the nature of international competition which used to be defined by the quantities of production factors. The Lisbon Strategy which aims to make the European Union the most competitive and dynamic knowledge-based economy in the world by 2010 is one of the most comprehensive examples of the efforts to adapt to
this change. The eEurope 2002 Action Plan prepared within this framework has continued with the eEurope 2005 Action Plan which includes new and more refined objectives. The Lisbon Strategy which was updated in 2005 as i2010 is redirected towards new targets with information, innovation and social inclusion as its core topics.

In Turkey, endeavours on transformation into an information society have also started to gain momentum since early 2000s in parallel to these developments. Turkey has become a party to the eEurope+ Initiative, which has been designed for EU candidate countries in 2001. The “eTransformation Turkey Project” that was included in the 58th and 59th Government Urgent Action Plan was launched in 2003 and hence all individual studies being carried out in our country have been gathered under an umbrella project and accelerated. The eTransformation Turkey Project aims to carry out the process of transformation into an information society in a harmonious and integrated structure all over the society with all citizens, enterprises and public segments. General coordination of the Project has been assigned to the State Planning Organization and the eTransformation Turkey Executive Board with the participation of the State Minister and Deputy Prime Minister, Minister of Transportation, Ministry of Industry and Trade, top-level bureaucrats and non-governmental organizations (NGOs), and the Advisory Council with the participation of public and private sectors and NGOs have been established.

In this process, “Turkey’s Information Society Transformation Policy” which was prepared with the participation of all relevant parties, has been adopted by the eTransformation Turkey Executive Board. The policy document states Turkey’s vision of transformation into an information society as follows: “To be a country that has become a focal point in the production of science and technology, that uses information and technology as an effective tool, that produces more value with information-based decision-making processes and that is successful in global competition, with a high level of welfare”.

Since the inception of eTransformation Turkey Project, which was formulated with a participative approach, two action plans covering 2003-2004 and 2005 periods were launched and implemented successfully. In conjunction with the short-term targets of the action plans, an initiative for preparation of Information Society Strategy covering 2006-2010 was also started in 2005 in an attempt to enable Turkey to benefit from ICT effectively and to identify the middle and long term strategies and targets for the realization of transformation.

4.2 Organization, Roles & Targets

The Minister of State and Deputy Prime Minister, Mr. Abdüllatif ener was appointed as e-minister and he has the high level political responsibility of the e-Government under eTransformation Turkey Project. Underneath e-Minister, State Planning Organization (SPO) is responsible for coordinating all e-Government activities. e-Transformation Turkey Executive Board also has a supervision and steering role in e-Government project. Advisory Committee is chaired by the Deputy Undersecretary of SPO and acts as the discussion platform with the participation of 41 members representing ministries, central public agencies, NGOs and universities. There is no CIO assigned for coordinating national e-government policy. However, Deputy Undersecretary of SPO, who reports to the e-minister and responsible for overall policymaking and coordination, could be considered as a CIO equivalent post.

SPO is responsible for overall coordination of countrywide economic and social development programs, allocation of funds to public investment projects, and advising to the Government. Prime Ministry, NGOs, and all public institutions are identified as affiliated organizations for the project. To clarify the objectives and principles of the project, a Prime Minister’s Circular, dated February 27, 2003 has been issued. According to this Circular, the objectives of eTransformation Turkey Project are as follows:
• Policies, laws, and regulations regarding ICT will be re-examined and changed if necessary, with respect to the EU acquis; eEurope+ Action Plan, initiated for the candidate countries, will be adapted to Turkey.
• Mechanisms that facilitate participation of citizens to decision-making process in the public domain via usage of ICT will be developed.
• Transparency and accountability for public management will be enhanced.
• Through increased usage of ICT, good governance principles will be put in place in government services.
• Widespread usage of ICT will be enhanced.
• Public IT projects will be coordinated, monitored, evaluated and consolidated if necessary in order to avoid duplicating or overlapping investments.
• Private sector will be guided according to the above-mentioned principles.

In order to realize these objectives and to ensure the success of the project, a new coordination unit, Information Society Department within SPO was established. This Department is responsible for the overall coordination of the project. Before this project was launched, lack of efficient coordination between institutions made the progress slow and ineffective. For the first time in Turkey, a dedicated department, which is believed to be a crucial element for success, has been named as the coordinator of information society activities.

In line with the government's schedule, the initial focal point in this project has been the Short Term Action Plan (STAP), for implementing specific tasks. Actions aiming at establishing interoperable and secure online information services have the first priority in STAP. Besides, actions in STAP are in line with actions of Urgent Action Plan that covers restructuring of public management, increasing efficiency in public services and introducing citizen-oriented services.

Besides the Strategy, STAP has the following main topics:
• Legislation regarding regulatory and legal framework,
• Technical infrastructure and information security,
• Education and human resources for planning of required human capital,
• e-Government for introducing electronic services to citizens without bureaucratic barriers,
• Standards for integrated and interoperable services,
• e-Health, which is one of the important thematic issues in eEurope,
• e-Commerce for the development of e-Business environment, especially for SMEs.

In the Information Society Strategy, the current situation of 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 together with the required steps for accomplishment of those targets have been identified within the framework of the strategic priorities determined henceforth. Furthermore, R&D and Innovation strategies have been integrated based on Scientific and Technological Research Council of Turkey's (TÜBİTAK) “Vision 2023” studies and on the decisions of the Higher Council of Science and Technology; consequently, the integrity of the strategy has been ensured. On the other hand, measurement criteria and methodologies have been introduced for monitoring and evaluation of the implementation, together with new structures to support the strategy implementation. 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 onto future schemes.
Turkish government’s approach to e-Government project could be characterized as more centralized. Until very recently, the approach that envisions provision of integrated services through portal was not in place, so there was a strong need to emphasize this new approach and to coordinate centrally the implementation of public IT projects. Besides, results of applications carried out by government agencies and provincial governments have not been satisfactory so far. Therefore, there is also a need to promote public agencies to provide better online services and make necessary changes in their processes if needed. This approach creates a common understanding of e-government and by doing so an interoperable and secure information system will be assured.

SPO’s unique role at the center of government also reinforces this organizational approach. SPO reviews project proposals of public entities and prepares annual investment programs. Therefore, SPO takes another role in eliminating unduly or overlapping e-government projects, including application projects, ICT expenditures, etc. At present, there is no central IT fund for e-government activities and projects are financed with national budget resources. Since the Short Term Action Plan is affiliated with annual public investment programs, which are prepared and monitored by the SPO, these programs are deemed to be suitable policy implementation tools to ensure e-government policy coherence with ministries and agencies. Nevertheless, under Short Term Action Plan an ad-hoc committee will be established to study ways and means of creating such a fund.

In short, there is an increasing need for coordination in basic elements of an integrated information system, such as interoperability, metadata, one-stop shop, etc. Therefore, Information Society Department’s role is not limited to provide support to policy-making, but also covers implementation of e-Government portal, and coordination among public agencies.

4.3 Certification Authority for the Government

Information security in development of e-Government is one of the indispensable and preliminary applications. For this reason, confidentiality integrity of information and identification should be guaranteed via the technical and legal infrastructure to be established. Within this framework, it can be said that the most vital legal regulation for the e-Government to be realized is the Electronic Signature Act No. 5070. Date of entry into force of the Law developed by the Ministry of Justice was determined as 23 July 2004, and extra time was granted for regulations until 23 January 2005, authorization to make regulation and supervision was granted to Telecommunication Authority.

The Telecommunication Authority was appointed to prepare secondary regulations about secure electronic signature creation devices, secure electronic signature verification devices, electronic certificate service providers, revocation of qualified electronic certificates, certificate financial liability insurance and foreign electronic certificates, in the field of e-signature that is of primary importance since the signatures used in operations carried out in electronic media provide the same legal validity as handwritten signatures.

Within this framework, “e-Signature National Coordination Board” was established within the Authority so as to ensure the monitoring of works on electronic signature within the Authority and the clear and transparent preparation of the secondary regulations laid down in the said Act. Various works concerning the preparation of secondary regulations were undertaken by study groups on “Infrastructure”, “Information Security and Standards” and “Law and Regulations” formed within this Coordination Board.

In these study groups, about 200 persons from public sector, private sector, non-governmental organizations and universities made several contributions to the preparative works on secondary regulations, in technical and legal perspectives.

As a result of these works, “Ordinance on the Procedures and Principles Pertaining to the Implementation of Electric Signature Law” and “Communiqué on Processes and Technical Criteria Regarding Electronic Signatures” were prepared on 12 November 2004 and dispatched to the Prime Ministry as to be published in Official Gazette. The mentioned ordinance and Communiqué were published in Official Gazette No. 25692 dated 06.01.2005.
On the other hand, “Ordinance on Certificate Financial Liability Insurance” prepared in consultation with the Undersecretariat of Treasury pursuant to the said Law was published in Official Gazette No. 25565 dated 26 August 2004, and “Mandatory Certificate Financial Liability Insurance General Terms and “Schedule and Instructions on Certificate Financial Liability” prepared by the Undersecretariat of Treasury in regard to the implementation of the said Regulation were published in Official Gazette No. 25709 dated 27 January 2005.

The Law on e-Signature (dated on January 15, 2004 and No: 5070) was put into effect and the opportunity to take an e-signature certificate individually from a certificate service provider eligible in accordance with the conditions specified in this Law was introduced to the public entities and organizations. In June, 2004; the National Research Institute of Electronic and Cryptology (UEKAE) which is affiliated to TÜBİTAK was assigned the duty of establishing the Public Certification Center (Kamu Sertifikasyon Merkezi - KSM). Later with the circular dated September, 2004 of the Prime Ministry; it was decided that the electronic certificate need of the public entities and organizations would be met by one single center and this duty was assigned to TÜBİTAK-UEKAE. Undersecretariat of the State Planning Organization was given the responsibility of the coordination of the works to be carried out in the public entities and organizations in order to harmonize them with this new structure.

According to the regulations, public establishments need to obtain their e-signatures from TÜBİTAK-UEKAE while individuals can receive their own e-signatures from three assigned companies. Private establishments and citizens can obtain their e-signature certificates from TürkTrust, e-Tugra or e-Güven.

4.4 eGovernment and eSignature regulations

4.4.1 eSignatures regulatory framework

Electronic Signature Act was published in the Official Gazette dated 15 January 2004 and entered into force in 23 July 2004. By virtue of this Act, Telecommunications Authority is given the duty of preparing and publishing secondary legislations and supervision of electronic certificate service providers. By the Authority it was considered as very important to make all relevant parties take part in the process of preparation of regulations, and within this framework “e-Signature National Coordination Committee”, composed of about 200 representatives from public sector, private sector, non-governmental organizations and universities, and within this Committee “Infrastructure”, “Information Security and Standards” and “Law and Regulations” study groups were established. The Authority prepared the secondary regulations as also taking into account the contributions from aforementioned study groups. As a result; “Ordinance on Certificate Financial Liability Insurance” was published in Official Gazette No.25565 dated 26 August 2004, “Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law” and “Communiqué on Processes and Technical Criteria Regarding Electronic Signatures” were published in Official Gazette No. 25692 dated 06.01.2005. Finally, “Schedule and Instructions on Certificate Financial Liability” was prepared by the Undersecretariat of Treasury in regard with the “Ordinance on Certificate Financial Liability Insurance” and published in Official Gazette No. 25709 dated 27 January 2005. All these regulations entered into force at the date of publications. Consequently, legal basis to electronic signatures has been established in Turkey.

In the 11th Article of the “Communiqué on Processes and Technical Criteria Regarding Electronic Signatures”, it is stated that “ECS (Electronic Certificate Service Providers) shall be awarded the certificate BS 7799-2 which is obtained from an authorized institution or organization”. Since an equivalent Turkish standard of BS 7799-2 was not available at that time the Communiqué was published in Official Gazette (06.01.2005), only BS 7799-2 certification was asked as a notification requirement from ECSPs. However after the publication of the said Communiqué, Turkish Standards
Institution (TSI) published the standard TS 17799-2 which is an equivalent of BS 7799-2 on 17.02.2005. Then, TSI stated that it would be appropriate to add TS 17799-2 to the Communiqué. After the evaluation of TSI’s proposal with the collaboration of candidate ECSPs, it was agreed by all to make a revision and 11th Article of the said Communiqué was changed as “ECSP shall be awarded the certificate BS 7799-2 or TS 17799-2”. This revision was published in Official Gazette No. 25849 dated 18.06.2005.

4.4.1.2 Scope and Coverage

“Electronic Contracts” in a broad sense expresses the contracts that are concluded by means of electronic communication devices and methods. Under Turkish Law the term “electronic” used in concept of “electronic contract” emphasizes the devices used merely in the conclusion and occasionally in the execution of the contract. According to the jurisprudence; just because of its abovementioned feature there is no need to create a separate and peculiar contract category as “electronic contracts” and to stipulate special rules to be applied to such contracts. Accordingly, it is possible for the provisions of the Code of Obligations regarding the conclusion, validity and execution of contracts to be applied on the contracts concluded in electronic environment to the extend that this is applicable in terms of the features of these contracts. In that sense; there is no special provision in the Code of Obligations relating to the electronic contracts.

Generally Turkish Law is considerably flexible as to the validity of the contracts. Under Turkish contracts law; it is sufficient for the parties to declare their mutual and compatible will and to have consensus on the essential elements of the contract to ensure the conclusion of a contract. With respect to the form of the contracts Turkish Code of Obligations recognizes the principle of freedom of contracts as a rule. Thereby, in cases where a form is not explicitly required by law (for example the sales and purchase of movable goods) the parties can express their wills verbally. Nevertheless; law may stipulate a precise form (such as official form, written form etc.) as a condition for the validity of some contracts such as bailment, assignment of claims, promise of donation. In case law requires a contract to be concluded in a precise form, as a rule the stipulated form is a “validity condition”.

Thus, contracts that are not concluded in the statutorily required form are void.

The Electronic Signature Law that is published in the Official Gazette dated 23.01.2004 and that has entered into force in 23.07.2004 states that the Secure Electronic Signature has the same legal affect and consequence as the handwritten signature. The Turkish Electronic Signature Law that was prepared based on EU 99/93/EC Directive; includes provisions with regards to the consequences of electronic signature in terms of substantive law and evidence law.

---

2 Falcio, Lu, Mete Özgür; Electronic Sales Contract and Its Conclusion Under Turkish Law, Ankara 2004, pg. 78; Saa lam Atabarut, "pek; Electronic Contracts, Istanbul 2003, pg. 50.
4 Art. 9/A of Law Regarding the Protection of the Consumer setting forth the definition of the distant contracts is a provision where the definition of the electronic contract is legally expressed: “the contracts that are concluded in written, visual, telephone and electronic environment or by means of use of other communication devices and without face to face contact with the consumers and by which the instantaneous or afterwards delivery or performance of the goods and services are agreed”.
5 Code of Obligations Art. 1, 2.
6 Code of Obligations Art. 11/f.1 “The validity of the contract is not bound to any form unless there is an explicicy in law”.
7 Code of Obligations Art.. 11/f.2.
8 Such as sales and purchase contract for real estates.
Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications

NATIONAL PROFILE TURKEY

April 2007

Directive; The Turkish Electronic Law does not make a distinction as qualified electronic signature and advanced electronic signature\(^{11}\); but it merely puts legal emphasis on secure electronic signature based on qualified electronic certificate.\(^{12}\) As a consequence of this emphasis; as explained above it is merely the electronic documents signed by secure electronic signatures that will have the same legal effect as the written documents that are signed on paper; and it is clearly set forth as a legal interpretation that only the electronic documents signed by secure electronic signatures have the power of proof in terms of evidence law and will be deemed as conclusive proof until otherwise is proved.

Although Article 6 of Electronic Signature Law states that secure electronic signature shall have the same legal effect and consequence as hand-written signatures in terms of substantive law, it is silent about the legal effect and consequence of electronic documents signed by secure electronic signature from a substantive law perspective. At that point; the interpretation to be conducted in the light of basic principles set forth by Electronic Signature Law and Code of Obligations; leads us to the above stated determination and in other words it may be said as an outcome that electronic documents signed by secure electronic signature and written documents signed by hand-written signatures on paper will be subject to same legal consequences.

23 January 2004 Electronic Signature Law No.5070 was published. TA was authorised to prepare secondary legislation until 23 January 2005 and inspect the market

23 July 2004 The Law entered into force

26 August 2004 By-law on Certificate Financial Liability Insurance

6 January 2005 By-law on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law

6 January 2005 Communiqué on Processes and Technical Criteria Regarding Electronic Signatures

1 June 2006 Telecommunications Board’s Decision Regarding security requirements for signature creation application and electronic signature format

\section*{4.4.2 eGovernment regulatory framework}

The Act on e-Signature which came into force on 23rd of July 2004 was prepared with the guidance of EU Directive and the practice of the member states such as Germany, France, Austria, and Belgium. e-signature Regulation and Communique has been entered into force on 6th January 2005 by way of publication in the Official Gazette.


\(^{12}\) The secure electronic signature is defined in Article 4 of Electronic Signature Law as follows:

\textit{“ARTICLE 4. — Secure Electronic Signature is an electronic signature, which;}

a) exclusively belongs to the signatory,

b) is cerated only by means of secure electronic signature creation device that is under the exclusive disposal of the signatory,

c) enables the identification of the signatory based uppon qualified electronic signature
d) enables the determination as to whether any subsequent alteration has been made in the electronic data that is signed”. This definition is a mixed definition including the requirements attached to advanced electronic signature by virtue of Article 5/1 of EU 99/93/EC Directive. For detailed information please see Keser Berber/ Beceni/ Sevim, a.g.e.
Differing from EU Directive, Turkish e-signature Act provides detailed provisions only for the secure digital signature amongst other types. Turkish Act does not make distinction between secure, qualified and advanced e-signatures as provided in the EU Directive. The Act thoroughly explains the qualified electronic certificate as being one of the requisites of a secure digital signature and provides that a secure digital signature would bear all legal consequences of signature by hand.\textsuperscript{13} Besides, the Act also provides that secure digital signature could not be used for the transactions of guarantee contracts and for those which are required to be effected by either official form or procedure. Accordingly under Turkish Law, sale of real property or marriage ceremony may not be effected by secure e-signature.

The Act on e-signature (No:5070) is a new regulation area for Turkish Telecommunication Board.\textsuperscript{14} Accordingly, the provisions of the Act\textsuperscript{15} designate the Board as the authorised body for many issues such as the review of the notifications to be made by the Certificate Service Providers in order to start operation, inspection of the quality, stability and reliability of the service, and finally the preparation of the necessary regulations.

4.4.2.1 Principles to be Followed Telecommunication Board in Regulating e-signature Services

Both the Act and the Regulation determine some principles for the Board to be taken into account while regulating the activity. The Directive provides for: The inspection of the qualitative stability, reliability and the efficiency of the service together with optimum use of the sources, transparency and openness, protection of the consumer rights, the provision and support of the effective and sustainable competition environment in the market, compliance with the international standards regard to advancing technology, the nation wide expanding of the E-signature practice and support of the new investments. It is also essential that a holder of the electronic certificate should not be imposed to purchase other services and financing of a service with the price of another service is prohibited.\textsuperscript{16}

4.4.2.2 Conditions in order to operate as Certificate Service Provider

In the light of above e-signature sector shall be regulated as follows: Under the existing law, in order to operate as a Certificate Service Provider (CSP) in Turkey, a notification to the Board is sufficient and permission from the Board is not required. A CSP complying with the conditions provided in the Act and the Regulation may start to operate within 2 months. The Board immediately starts investigation upon the receipt of the notification. The Board requires the following documents and information with the notification: The use of the secure systems and equipment, provision of a reliable service, the provision of all measures to prevent the destruction or counterfeiting of the certificates, communication details, details of the company, and the details of the employees, the Certification Policy (CP) and Certification Practice Statements (CPS), time stamp policy and time stamp practice statements, sample of the certificate, liability insurance, a copy of the contract to signed with the e-signature holders and with service receivers where service.\textsuperscript{17}

\textsuperscript{13} Act Article 5/1
\textsuperscript{14} http://www.tk.gov.tr
\textsuperscript{15} Act Article 3/j
\textsuperscript{16} Directive Article 5
\textsuperscript{17} Directive Article 6,7
If there is a missing information or document the Board gives CSP one month period. If all requirements are not met within this period. The Board shall make a decision to determine that the applicant does not qualify as a CSP anymore.18

The Board is responsible to announce in its website: the notifications, information about the foreign CSPs operating in Turkey and samples of the certificates. An other responsibility is to prepare a report on the progress and the general conditions of the sector.19

The Board shall also determine the principles regarding the margins of the tariffs. However, since E-signature is a new sector, the Board shall not determine any figures until the market reaches a stable condition. According to the provisional article contained in the Regulation, CSPs shall determine the prices in accordance with the above mentioned principles until a further notice received from the Board. The same principle is also applicable for administrative fees. The Board shall ask for %0.4 of the previous year's turnover as the fee.

4.4.2.3 The Duties of CSPs

According to e-signature Act article 10, the duties of a CSP are as follows:

The employment of the qualified personnel, recording of true identity based on the official documents of the persons that are given certificates, determining the true identity and authority of any legal representatives for the usage of e-signature produced by the CSP as well as by the certificate holder; providing security of the data used for the formation of the e-signature either by the CSP or by the certificate holder within the premises belonging to the CSP; providing the security of the procedure where the e-signature is produced by the certificate holder by the tools provided by the CSP; before the delivery of the certificate informing of the certificate holder on the usage of the certificate and the method for resolving any disputes together with the legal requirements and, informing the certificate holder of the fact that e-signature had all the legal effects of a signature by hand with the proviso of exceptions; warning of the certificate holder that he/she should not allow other persons to use the data to form e-signature; keeping of the records for all transaction for 20 years; notification to the electronic certificate holder and the Board 3 months prior to the termination of the services.

CSP cannot maintain or store a copy of the e-signature data.

4.4.2.4 Termination of the services by the Board

The Board is also responsible for the stability of the E-signature services. The Board shall inspect every CSP either on complaint or on its own motion in every two years.20

The Telecommunication Board shall follow the below principles in inspection of the CSPs: Impartiality in the conduct of the inspection, assessment and consequently in preparation of the report, to avoid any occurrence which my jeopardize impartiality and diligence, to act with utmost care in all procedures.21 The review of the applications to operate as CSP and the reports subsequent to inspection shall be conducted by a Committee chosen within the Telecommunication Board.

18 Directive Article 7
19 Directive Article 17
20 Act Article 15; Directive Article 22
21 Directive Article 27, 28
Following to inspection where the Board finds out that the CSP is lacking one or more of the notification conditions, the CSP shall be suspended of its activities and shall be provided one month period to remedy the situation. Failure of compliance within a month shall result with the termination of its services.\textsuperscript{22}

A CSP that its services has been terminated, may agree with an other CSP for the transfer of the qualified electronic certificates within 15 days following to the termination. Where such agreement exists the Board decides for the transfer of the certificates and in the absence of such agreement the Board shall choose a CSP on its own motion. The CSP which is the transferee shall finish renewal of the certificates within in a month starting with the notification of the decision for the transfer.

The CSP that its services has been terminated, shall provide the documents needed for identity verification, the index, the archive and other records of the canceled certificates to the transferee CSP.

Where the Board is unable to designate a CSP for the transfer, the certificates shall be canceled. The CSP that its services has been terminated, shall provide records of the cancellation until the expiry date of the latest certificate and shall maintain the archive for 20 years.

Upon the notification of the Board's decision as to the termination of the services, the CSP may no longer offer services of electronic certificate, time seal and e-signature. However shall continue with the certificate cancellation records until the renewal of the certificates by the transferee CSP are completed.

The CSP that its services are terminated, shall prepare the cancellation records at the end of the expiry date of the latest certificate and destroy all e-signature data and respective back up.

The decision for the transfer of the qualified electronic certificates shall be promulgated in the web site of the Board. The CSP that its services are terminated, shall electronically notify the certificate holders of the transfers.

\textbf{4.4.2.5 Cancellation of the Certificates and the CSPs deciding to terminate their services}

- A CSP shall cancel the certificate where it is demanded by the holder, where it is found that the information contained in the electronic certificate database was inaccurate, forged or changed, where it is found that the certificate holder has been limited of his/her capacity, the bankruptcy, absence or the death of the certificate holder.

- The CSP shall keep a record which enables to determine the exact time of cancellation and easily accessible by the third parties.

- Where the services of a CSP are terminated by the Board and certificates are not transferred to another CSP, the certificates shall be cancelled immediately.

- A CSP may not cancel certificates as having retrospective effect.

- A CSP deciding to cease its services, shall notify the Board in writing 3 months in advance. Following such notification, the CSP may not accept new applications and cannot issue a new qualified electronic certificate.

\textsuperscript{22} Directive Article 29
A CSP deciding to cease its services, shall inform the holders of its decision in its website and in 3 national newspapers of highest circulation 3 months in advance.

A CSP may transfer certificates that have expiry dates exceeding the date on which the services shall be terminated, to another CSP until a month before the termination. The transferee CSP shall finish the renewal of the certificates within one month following to the notification of the transfer.

The CSP that its services has been terminated, shall provide the documents needed for identity verification, the index, the archive and other records of the canceled certificates to the transferee CSP.

Where it has not been possible to transfer the certificates or the service cannot be continued by another CSP, the CSP terminating its services shall cancel the certificates latest at the date of termination of its services. The CSP shall notify the certificate holders of the cancellation latest 15 days in advance of the cancellation.

The CSP that its services has been terminated, shall keep records of the cancellation until the expiry date of the latest certificate and shall maintain the archive for 20 years.

The CSP that its services are terminated, shall prepare the cancellation records at the end of the expiry date of the latest certificate and destroy all e-signature data and respective back up.

4.4.2.6 Activity Reports

All CSPs shall provide to the Board an annual report of the previous year in every March. The report shall at least contain the below:

- Types of issued certificates and respective numbers
- The number of the canceled certificates for each type.
- Documents and information indicating the financial situation of the CSP
- The information as to the transferred certificates, if exist any.
- The market projection of the CSP for the coming year.
- Other documents and information required by the Board.

4.4.2.7 The legal liability of the CSPs

As to the legal liability of the CSPs the Act on E-signature provides that\(^{23}\) the liability of a CSP against the certificate holder is covered by the general rules of liability. Accordingly a CSP is liable for the damages sustained through an action of the CSP which violates the rules contained in the Act or the Regulation. The CSP is burdened with proving it had no negligence in order to discharge liability. Where the act is committed by an employee of the CSP, then the CSP may not benefit from the relevant provisions of the Code of Obligation which allows an employee to present evidence to discharge its vicarious liability.

Apart from the limitations arising from the technical specifications and the substantial scope of the e-signature, any agreements or covenants excluding the liability of a CSP, are null and void.

\(^{23}\) Act Article 13
4.4.2.8 Certificate Liability Insurance

Differing from other e-signature laws, Turkish Act on E-signature does not require the provision of some security in order to start operating as a CSP. Instead, CSPs are obliged to purchase insurance to cover any damages arising from the incompliance with the duties vested by the Act. The rules and the procedure for this insurance shall be determined by a separate regulation of the Board after having received the opinion of the Undersecretariat of Treasury. The regulation has been prepared and entered into force as published in the Official Gazette on 26.08.2004. Accordingly, CSPs are required to have insurance to cover the damages arising from incompliance with the statutory duties. The scope of the insurance is to cover the damages of the third parties sustained through the incompliance of the duties as to usage of secure products and systems for electronic certificates, conduct of services in a secure manner and avoid forgery or replication of the certificates. The art. 8 of the Regulation as to Liability Insurance provides that the general clauses, tariffs and other conditions of the insurance shall be determined by the Undersecretariat of Treasury.

The general clauses and tariffs prepared by the Undersecretariat was submitted to the Board as of the end of November 2004. The Clauses provide that the scope of the insurance will cover certificate holders as well as third parties. Assuming that the risks are minimised due to the technical aspects of e-signature, Tariffs set relatively low premiums.

4.4.2.9 Foreign Electronic Certificates

The acceptance of foreign electronic certificates requires either an international agreement or the surety of a domestic CSP. The Board is responsible to publish the information about the foreign CSP and a copy of the certificate in its web site. The CSP in Turkey is jointly liable for any damages to be sustained as a result of the usage of an accepted foreign certificate.

The consequences of foreign certificate issued abroad are regulated in the Act as follows: many EU members provide that the legal status of foreign electronic certificates shall be regulated by international agreements. Despite the reference in many national laws, such agreement does not exist yet. Secondly the Turkish Act states that where a foreign certificate is accepted by a CSP in Turkey, such certificates are deemed to be qualified electronic certificates and both the foreign and the local CSP shall be jointly liable for damages resulting from the usage of these foreign certificates.

The Regulation brings the below minimum requirements for the acceptance of foreign certificates:

- The foreign certificates should bear all technical specifications of a qualified electronic certificate,
- The foreign certificate issuer must qualify as a CSP in its country of origin.
- The accepting CSP in Turkey shall submit to the Board one month in advance the below information for any foreign certificate to be accepted.
- A certificate sample of the foreign CSP
- The document proving the qualification of the foreign CSP as issued by the relevant authority in the country of origin.

---

24 Act Article 13/5
25 Act Article 5
26 Act Article 14
27 Directive Article 32
• Documents to prove that foreign certificates bear all technical specifications of a qualified electronic certificate,

The Board shall publish the certificate sample and other relevant information as to the foreign CSP in its web site. It is repeated in the Regulation that the local CSP shall be jointly liable with the foreign CSP.

Another vital issue with electronic documents is the time stamp. Both the Act and the Directive provides that CSPs are obliged to give time stamp service. Users having qualified Electronic Certificates are entitled to this service.

With a view to assist the Board and inform about the problems of the sector, the CSPs are required to submit a report to the Board until the March of every year.
4.4.3 Turkish Electronic Signature Law

Below is the unofficial Translation of Turkish Electronic Signature Ordinance by Telecommunications Authority and it must be noted that the original Turkish text shall prevail in case of divergent interpretation.

ELECTRONIC SIGNATURE LAW  (Published in the Official Gazette ref 25355, 2004-01-23)

SECTION ONE
Purpose, Scope and Definitions

Purpose
Article 1 – The purpose of this Law is to define the principles for the legal and technical aspects and application of electronic signatures.

Scope
Article 2 – This Law covers the legal status of electronic signatures, operations concerning electronic signatures and the activities of Electronic Certificate Service Providers (ECSPs).

Definitions
Article 3 – The definitions and abbreviations used in this Regulation have the following meanings:

a) Electronic Data: Information which are generated, transferred or stored in electronic, optical or similar methods,

b) Electronic Signature: Data in electronic form that are attached to other electronic data or linked logically to that electronic data and used for authentication,

c) Signature Owner: A natural person, who uses an electronic signature creation device in order to generate electronic signatures,

d) Signature Creation Data: Unique data such as password and cryptographic keys belonging to a signature owner and being used by the signature owner in order to create electronic signatures,

e) Signature Creation Device: Software or hardware products using the signature creation data in order to generate electronic signatures,

f) Signature Verification Data: Data such as passwords and cryptographic public keys used for the verification of electronic signatures,

g) Signature Verification Device: Software or hardware products using the signature verification data for verification of electronic signatures,

h) Time-Stamping: An record signed electronically by the ECSP for the purpose of verification of the exact time of creation, alteration, sending, receiving and/or recording of an electronic data,

i) Electronic Certificate: Electronic data binding the signature verification data of the signature owner to identity data of that person,

j) Authority: Telecommunications Authority.

SECTION TWO
Secure Electronic Signature and Certification Services

PART ONE
Secure Electronic Signature, Secure Electronic Signature Creation and Verification Devices

Secure Electronic Signature
Article 4-A Secure Electronic Signature shall be a signature that;
a) is exclusively assigned to the Signature Owner,
b) is generated with the Secure Electronic Signature Creation Device which is kept under the sole control of the signature owner,
c) enables the identification of the Signature Owner based on the Qualified Electronic Certificate,
d) enables detection as to whether signed electronic data has or has not been altered or not subsequent to the signature being applied.

Legal Effect and Area of Application of Secure Electronic Signature
Article 5- A secure electronic signature shall have the same legal effect as that of a handwritten signature.
A secure electronic signature shall not be applicable to legal proceedings subject to a special procedure or an official form pursuant to laws and warranty contracts.

Secure Electronic Signature Creation Devices
Article 6-Secure Electronic Signature Creation Devices are Signature Creation Devices which ensure that;
a) Electronic Signature Creation Data produced by those devices are unique,
b) Electronic Signature Creation Data recorded in those devices cannot be derived in any means and that their secrecy is assured,
c) Electronic Signature Creation Data recorded in those devices cannot be obtained or used by third parties and that electronic signatures are protected against forgery,
d) The data to be signed cannot be altered by anyone except the signature owner and can be seen by the signature owner before the generation of a signature.

Secure Electronic Signature Verification Device
Article 7-Secure Electronic Signature Verification Devices are Signature Verification Devices which;
a) display without any alteration the data used for verification of the signature to the person who makes verification,
b) manage the signature verification process in a reliable and accurate way, and display the results of verification without any alteration to the person who makes verification,
c) ensure that signed data is displayed in reliable manner when necessary,
d) display without any alteration its results to the person who makes verification establishing in a reliable manner the authenticity and validity of the electronic certificate used for the verification of the signature,
e) display without any alteration the identity of the signature owner to the person who makes verification,
f) ensure the detection of any alterations that effect the conditions relevant to the verification of the signature.

PART TWO
Electronic Certificate Service Provider, Qualified Electronic Certificate and Foreign Electronic Certificates

Electronic Certificate Service Provider
Article 8 – For the purposes of this act, Electronic Certificate Service Providers shall be public entities or establishments or natural persons or private law legal entities that provide qualified electronic certificates, time-stamping and other services related to qualified electronic signatures.

Electronic Certificate Service Providers shall commence its operations within a period of two months from the date of notification.

Electronic certificate service providers shall show in detail in their notification that they ensure the provisions related to;

a) Using secure products and systems,

b) Managing operations in a reliable way,

c) Taking all necessary measures in order to avoid certificates being copied or distorted.

If the Authority determines the incompleteness or infringement of any of the above terms, the Authority shall grant a period of up to a month to the Electronic Certificate Service Provider in order to remedy this incompleteness; during this period the Authority shall suspend the operations of electronic certificate service provider. At the end of the period, in the event that the incompleteness is not remedied, the operations of the electronic certificate service provider shall be terminated. An objection may be raised against such decisions of the Authority pursuant to the provisions in paragraph 2 of Article 19.

Should Electronic Certificate Service Providers fail to comply with the provisions mentioned in this article during their operations, the provisions of above paragraph shall be applied.

Electronic Certificate Service Providers shall comply with such lower and upper fee limits to be determined by the Authority.

Qualified Electronic Certificate

Article 9 – It is required that Qualified Electronic Certificates shall include the following;

a) an indication that the certificate is a “qualified electronic certificate”,

b) the identity information of the Electronic Certificate Service Provider and the country in which it is established,

c) the identity information by which the Signature Owner can be identified,

d) Signature-Verification Data which correspond to Signature-Creation Data,

e) the date of the beginning and the end of the validity period of the certificate,

f) serial number of the certificate,

g) the information regarding the authorization of the certificate holder if the holder acts on behalf of another person,

h) when the certificate holder so requests, occupational and other personal information,

i) information related to conditions of the usage of the certificate and limits on the value of transactions, when applicable,

j) the Secure Electronic Signature of the electronic certificate service provider that verifies the information in the certificate.

Electronic Certificate Service Provider Liabilities

Article 10 – Electronic Certificate Service Providers shall be liable for;

a) Employing personnel qualified for the services provided,

b) Determining reliably, based on official documents, the identity of the person to whom a Qualified Electronic Certificate is issued,
c) Determining reliably, based on official documents, any information relating to the Qualified Electronic Certificate holder's authorization of acting on behalf of anyone, or any occupational or other personal information which is to be contained in the certificate,

d) Providing confidentiality of operation in cases where the Electronic Certificate Service Provider generates Signature Creation Data or the applicant generates it on the premises of the Electronic Certificate Service Provider or provide confidentiality of process when the signature creation data are generated by tools provided by the Electronic Certificate Service Provider,

e) Informing the applicant in writing, before delivering the certificate to them, that a qualified electronic signature has the same legal effect in transactions as a handwritten signature unless otherwise specified by laws, and about the limitations concerning the use of certificates and dispute resolution procedures,

f) Warning and informing the certificate holder in written form to not allow third parties to use Signature Creation Data associated with Signature Verification Data in the certificate,

g) Keeping all records regarding the services provided for the period determined in ordinance,

h) Informing the electronic certificate holder and the Authority at least 3 months prior to the termination of operations.

Electronic Certificate Service Providers shall not store or keep a copy of generated signature creation data.

Revocation of Qualified Electronic Certificates

Article 11 – Electronic Certificate Service Providers shall immediately revoke the qualified electronic certificates upon;

a) the request of the certificate holder,

b) the detection of any forgery or falsification of the information existing in the database or changes in such information,

c) the detection of the disability to act, bankruptcy or legally accepted disappearance or death of the certificate holder.

Electronic Certificate Service Providers shall create a record including the date and time when a certificate was revoked and which can be determined precisely and available by third parties in a secure and prompt way.

Electronic Certificate Service Providers shall immediately revoke all qualified certificates they have issued in the case of terminating their operations and in case the usage of certificates can not be available by any operating electronic certificate service provider.

In the event that the Authority terminates the operations of electronic certificate service provider, the Authority shall decide to transfer the qualified electronic certificates generated by the regarding electronic certificate service provider to another electronic certificate service provider and shall notify it to relevant parties.

Electronic Certificate Service Providers shall not retroactively revoke qualified electronic certificates.

Protection of Personal Data

Article 12 – Electronic Certificate Service Providers;

a) shall not request any information from the applicant except that necessary to issue an electronic certificate and shall not acquire such information without the consent of the applicant,

b) shall not keep the certificates available in public places where third parties may have access without the consent of the electronic certificate holder,
c) shall prevent third parties from obtaining the personal data without the written consent of the applicant. Electronic Certificate Service Providers shall not pass the related information to third parties and use such information for any other purposes without the consent of the certificate holder.

Legal Liability

Article 13 - Liabilities of Electronic Certificate Service Providers towards certificate holders shall be subject to general provisions of Turkish law.

Electronic Certificate Service Providers shall be liable for compensation for damages suffered by third parties as a result of infringing the provisions of this Law or the ordinances published in accordance with this Law. Liability of compensation shall not occur if the Electronic Certificate Service Provider proves the absence of negligence.

Electronic Certificate Service Providers shall be liable for damages arising from infringements made by their employees. Electronic Certificate Service Providers shall not be relieved of this liability by submitting any proof of evidence as described in Article 55 of the Turkish Code of Obligations.

Any requirements limiting or removing the liability of Electronic Certificate Service Provider against certificate holders and third parties are invalid, excluding the stated limitations of the usage and value of the Qualified Electronic Certificates.

Electronic Certificate Service Providers shall be liable for compensation for damages suffered by third parties as a result of infringing the provisions of this Law or the ordinances published in accordance with this Law. Liability of compensation shall not occur if the Electronic Certificate Service Provider proves the absence of negligence.

Electronic Certificate Service Providers shall be liable for damages arising from infringements made by their employees. Electronic Certificate Service Providers shall not be relieved of this liability by submitting any proof of evidence as described in Article 55 of the Turkish Code of Obligations.

Any requirements limiting or removing the liability of Electronic Certificate Service Provider against certificate holders and third parties are invalid, excluding the stated limitations of the usage and value of the Qualified Electronic Certificates.

Electronic Certificate Service Providers must take out “certificate financial liability insurance” in order to cover the damages incurred upon the failure in fulfilling the liabilities required by this Law. Principles and procedures of this Regulation are determined by the ordinance prepared by the Authority taking advice of the Undersecretary of the Treasury.

Certificate financial liability insurance foreseen in this article is provided by insurance companies authorized in this branch. These insurance companies shall be liable for providing certificate financial liability insurance. The insurance companies that infringe regarding liabilities may be fined up to eight billion TRL by the Undersecretary of the Treasury. The provisions of Article 18 address procedures for the collection of and appeals against this fine.

Electronic Certificate Service Providers shall be obliged to deliver electronic certificates to the signature owners after taking out certificate insurance.

Foreign Electronic Certificates

Article 14 – The legal effects of electronic certificates issued by any Electronic Certificate Service Provider established in a foreign country shall be recognized under international agreements.

In case that electronic certificates issued by any Electronic Certificate Service Provider established in a foreign country are recognized by an Electronic Certificate Service Provider established in Turkey, such electronic certificates are deemed to be Qualified Electronic Certificates.

The Electronic Certificate Service Provider established in Turkey shall be liable for any damages arising from use of those electronic certificates.

SECTION THREE

Inspection and Penalty Provisions

Inspection

Article 15 – The inspection of Electronic Certificate Service Providers’ operations and transactions regarding the implementation of this Law shall be fulfilled by the Authority.

The Authority, as it considers necessary, may inspect Electronic Certificate Service Providers. During inspection, Electronic Certificate Service Providers and relevant individuals shall present all notebooks, documents and records and provide samples, written and oral information to the Authority’s inspectors, permit the inspectors to enter their premises and enable them to access their accounts and transactions.
Use of Signature Creation Data without Consent

Article 16 – A person who obtains, delivers, copies or recreates the signature creation device or data in order to create electronic signatures without the consent of the certificate holder shall be sentenced from 1 year to 3 years and fined a minimum of 500 million TRL (Turkish Lira).

In the case where crimes mentioned in the above paragraph are committed by the employees of an Electronic Certificate Service Provider, these penalties shall be scaled up by 50 percent.

Any damages arising from the crimes mentioned in this article shall be compensated separately.

Forgery in Electronic Certificates

Article 17 – A person who partly or fully generates electronic certificates, or falsify or copies electronic certificates generated as in valid, generates electronic certificates without authorisation or knowingly uses such electronic certificates shall be sentenced from 2 years to 5 years and fined a minimum of one billion TRL (Turkish Lira), even if their deeds become another crime.

If the crimes mentioned above are committed by the employees of an Electronic Certificate Service Provider, these penalties shall be scaled up by 50 percent.

Any damages arising from the crimes mentioned in this article shall be compensated separately.

Administrative Fines

Article 18 – Within this law:

a) An electronic certificate service provider who breaches Article 10 shall be fined 10 billion TRL,

b) An electronic certificate service provider who breaches Article 11 shall be fined 8 billion TRL,

c) A person who breaches Article 12 shall be fined 10 billion TRL,

d) An electronic certificate service provider who breaches the paragraph 5 and paragraph 7 of Article 13 shall be fined for 8 billion TRL,

e) An Electronic Certificate Service Provider who breaches Article 15 shall be fined 20 billion TRL

The administrative fines in this Law are determined by the Authority. Decisions about fines shall be notified to the persons concerned pursuant to The Notification Law number 7201. Any appeals against these decisions may be made to the competent administrative court within a period of 7 working days starting from the date of notification. An appeal shall not nullify the fulfilment of the decision. An appeal shall not nullify the fulfilment of the decision regarding the closure. An appeal, when it is not necessary, shall be concluded by making analysis over the documents as soon as possible. It is possible to apply to the Regional Administrative Court against the decisions that are taken regarding the appeal. The decisions of the Regional Administrative Court will be the final decree. The administrative fines imposed pursuant to this Law by the Authority shall be collected by the Ministry of Finance pursuant to the provisions of the Law about Procedures Collecting Public Receivables.

Repetition of Administrative Crimes and Closure

Article 19 – If any crimes described in Article 18 of this Law are repeated within a period of 3 years from the date of the first instance, administrative fines are doubled, and in should the same crime be committed for a third time, the Authority may decide to close Electronic Certificate Service Provider concerned.

Any decision regarding closure shall be notified to relevant individuals pursuant to Notification Law No. 7201. Any appeal against such a decision may be made to the competent administrative court within a period of 7 working days from the date of notification. An appeal shall not nullify the fulfilment of the decision. An appeal shall not nullify the fulfilment of the decision regarding the closure. An appeal, when it is not necessary, shall be concluded by making analysis over the documents as soon as possible. It may be applied to the Regional Administrative Court against the decisions that are
taken regarding the objection. The decisions of the Regional Administrative Court will be the final decree.

SECTION FOUR
Miscellaneous Provisions

Ordinance

Article 20 – The procedures and the rules pertaining to the implementation of the Articles 6, 7, 8, 10, 11 and 14 of this Law shall be described in the ordinances to be published by the Authority within the period of six months from the execution date of this Law with the collaboration of all interested parties.

Exemptions about Public Entities and Establishments

Article 21 – The public entities and establishments providing certification services are exempted from the forth and the fifth paragraphs of Article 8, 15 and 19 of this Law.

Article 22 – The following sentence has been added to the first paragraph of Article 14 of the Turkish Code of Obligations dated 22.04.1926 No. 818:

“Secure electronic signature has the same effect as a handwritten signature”

Article 23 – The following 295/A article has been added to Article 295 of the Turkish Code of Civil Procedure dated 19.6.1927 No. 1086:

“Article 295/A – Electronic data that are generated with secure electronic signatures in accordance with procedures are equivalent to bill. These data are accepted positive evidence until the contrary is proved.

Should any party deny the data generated by secure electronic signatures and alleged against him, Article 308 of this Law shall be imposed through comparison.”

Article 24 – The following Subclause (m) has been added to the first paragraph of Article 7 of the Turkish Radio Law dated 5.4.1983 No.2813 and therefore existing subclause (m) of the current Law has been succeeded as subclause (n):

“m) undertaking the duties assigned by the Electronic Signatures Law”

Entry into Force

Article 25 – This Law shall enter into force six months after the date of its publication.

Execution

Article 26 - The provisions of this Law are executed by the Council of Ministers.
4.5 eGovernment applications using electronic signatures

4.5.1 General Process

The act on electronic signatures was enacted in 2004. With this act, it is stated that qualified electronic signatures produced according to the identified procedures will have the same legal impact as handwritten signatures. Related secondary legislation has also been completed by Telecommunication Authority as mandated by the Law. 3 electronic certificate service providers have been authorized as of November 2005. One of these is the “Public Certificate Center” which is the responsible body to provide electronic certificate services to all public institutions. KSM (Kamu Sertifikasyon Merkezi - Public Certification Center) was established in 2005 within Ulusal Elektronik ve Kriptoloji Arastirma Enstitusu (UEKAE) a subsidiary of Türkiye Bilimsel ve Teknolojik Arastirma Kurumu (TUBITAK). KSM is authorized by the Telecommunications Authority to operate according to the act of Electronic Signature Law 5070 published on January 15, 2004. The Center was established with a Prime Minister’s circular and it is mandated that all public institutions needing electronic certificate services will acquire this service from the mentioned body.

KSM specializes in qualified certification services to confirm the identity of individuals, provide reliability and security of e-documents, electronic data and hardware. Use of qualified electronic certificates issued by KSM in electronic signatures enables the identification of the signature owner and detection as to whether signed electronic data has been altered.

KSM is obligated to prepare Qualified Electronic Certificates, to load signature creation data with these certificates into the Secure Electronic Signature Hardware and to deliver the certificate to the certificate owner. KSM uses secure products and systems to collect applicant data, to prepare and deliver the certificates, manage operations in a reliable way, and to take all necessary measures in order to avoid certificates being copied or distorted.

Services provided by KSM are based on UEKAE PKI technology and aimed at public government and businesses. The scope of the services covers the following fields:

- Issuing and management of qualified electronic certificates for secure e-signature: Qualified electronic certificates, are used for verification of identity of the signor in reliance upon a “qualified electronic certificate” and can be used for detection of any subsequent change or modification in a signed “electronic data” Qualified electronic certificates are issued according to X.509 standards and can be installed on web browsers, smart cards and tokens that respect to the standard.

- Issue of ordinary certificates for general e-signature, logging on domains, databases, applications and www; protection of e-mails; protection of SSL servers; development of the VPN’s; protection and signing of software;

- Supply software libraries (applets and APIs) for integrating existent infrastructure to e-signature applications.

- Providing additional services: trusted time stamping, OCSP server; Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Online Certificate Status Protocol (OCSP) is a method for determining the revocation status of an X.509 digital certificate using means other than CRLs. It is described in RFC 2560 and is on the Internet standards track.

- Consultancy and special training in e-signature;
### 4.5.2 Standardization Aspect of Electronic Signature and Some Figures

<table>
<thead>
<tr>
<th>Operations of ECSP</th>
<th>ETSI TS 101 456 and CWA 14167-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>QES</td>
<td>ETSI TS 101 862 and ITU-T Rec. X.509 V.3</td>
</tr>
<tr>
<td>SC and V Data of Signatory</td>
<td>• 1024 bits for RSA or DSA or • 160 bits for ECDSA Up to 31/12/2008</td>
</tr>
<tr>
<td>SC and V Data of ECSP</td>
<td>• 2048 bits for RSA or DSA or • 256 bits for ECDSA Up to 31/12/2008</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>RIPEMD – 160 or SHA – 1 or SHA-224 or SHA-256 or WHIRLPOOL</td>
</tr>
<tr>
<td>CP &amp; CPS</td>
<td>IETF RFC 3647</td>
</tr>
<tr>
<td>SSC and V Devices</td>
<td>CWA 14169 or assured to EAL4+ in accordance to ISO/IEC 15408 (-1,2,-3)</td>
</tr>
</tbody>
</table>
Security Criteria | CWA 14167-1, ETSI TS 101 456 and ISO/IEC 17799
---|---
Time-stamp | CWA 14167-1 and ETSI TS 101 861
ECSP Certification | ISO/IEC 27001
Security Requirements for Signature Creation Applications | CWA 14170
e-Signature Format | ETSI TS 101 733 or ETSI TS 101 903

Below are the some figures about the status of e-signature in Turkey:

- To use the e-signature if there exists an available system, is possible : in minimum 2 months, maximum 6 months
- If the system is not available or ready for e-signature, then another 2-6 months must be added.
- 10-60 days of the phase/time needed for transformation for e-signature, min 2 - max 6 months is for the processes of KSM – UEKAE.
- By January 2007,
  - The number of institutions that applied for certificates : 55
  - The number of institutions that received certificates : 29
  - The number of institutions with inadequate infrastructure : 28
  - The number of certificates produced : 4223

4.5.3 Inward Processing Regime - Undersecretariat of Foreign Trade

After electronic signature regulations were completed and electronic certificate service providers commenced their operations, since secure electronic signature has become available, public organizations have started to develop projects in order to use electronic signature in electronic media while running their operations with related parties for the aim of ensuring sustainable development environment, reduction in operating costs, increase in public revenue, timely introduction and dissemination of public services at maximum quality and minimum cost and reduction in bureaucracy. Interior Processing Regime (IPR Automation) Project, which is initiated by Undersecretariat of Foreign Trade (UFT), is the first project in this field.

UFT is the coordinator of the project, “eDocuments in Foreign Trade”. The basic component of this project is the Inward Processing Permission Certificates under the responsibility of the UFT. In Turkey, firms apply to the UFT, filling out Inward Processing Permission Certificates, which are in the form of paper documents.

UFT constituted an "Inward Processing Regime Project" in order to eliminate bureaucratic difficulties before the exporters, to implement an approach that gives priority to exportation in the government institutions and to use the information technologies for increasing the exportation effectively, in accordance with the targets set in ‘Exportation Strategic Plan (2004-2006)’.

UFT decreased its workload through the project’s advantages such as time saving, rapid decision making process, tracking, querying assessment of transactions, and electronic document flow and archiving facilities. All the information about past and future importations and exportations will be accessible simultaneously.
Workload of UFT was decreased by using new technologies, and as a result the specialized personnel of the institution have more time to set new policies to increase the exportation. Inward Processing Certificate, Tax Duty Expenditure Exception Document and External Processing Certificates may be prepared in the same day thanks to the system; before the implementation of the project the preparation of these documents took very long time. It is planned to form a data warehouse by electronically archiving the information of exporters.

Within the scope of the project, the companies can create exportation and importation lists, prepare the expenditure table for raw materials, apply for and follow their documentations on any computer connected to Internet. In addition, they can apply for revisions, cancellations and undertaking closing for the documents received. Exporters can follow their application from beginning to end in anywhere.

As a part of the project, already integrated with General Secretariat of Exporter Associations and Turkish Customs Authority, the integration works for UFT with Turkish Union of Chambers and Commodity Exchanges and Turkish Union of Banks still continues. As this integration will enable information exchange in the electronic environment it will help to prevent the time consumption of guarantee returns, to realize the deduction of guarantee once the exportation is realized, and to reduce the financing cost by eliminating the damnifications of the companies.

This project will contribute to provide a higher level of investment and, in parallel, higher level of life standard through an important step towards the sustainable exportation increase in Turkey.

For realization of the project, in total 25 persons played a role in software production and in formation and configuration of infrastructure. Test and product quality personnel were also appointed in addition to the software production process. Overall labor force of the project was approximately 100 man/month.

The project consists of 7 stages:

1. Defining organisation and users
2. Defining the companies
3. Getting the application for the forms & documents
4. Evaluation of document flow & documents
5. Import & export processes (Undersecretariat of Custom)
6. Revising and tracking the documents (Exporter Union)
7. Finalizing the documents (Exporter Union)

In automation project of inward processing regime, multi-layer J2EE architecture and PKI infrastructure were used. This is the first project in Turkey, which serves the citizens utilizing electronic signature and PKI infrastructure. In order to provide a secure platform to the companies for the utilization of the applications and on-line application facilities of the system, intelligent cards (Security Certificate) with digital signatures are provided. Designs of internal processing regime project, totally developed on web based technologies, were realized by taking into account ease of usage, communication speed, security and ergonomics.

With the “Project of Monitoring Inward Processing Permission Certificates”, the UFT takes steps forward in paperless trade. In the context of Inward Processing Regime, this project is aimed at transferring all operations to electronic form. With the completion of this project, the following services are available:

- Receiving firm applications securely through the Internet (convenient with the utilization of technologies such as digital certificate, electronic signature),
- Evaluation of electronic certificates by experts,
- Filing all information related with the certificate in a central database,
• Processing the documents by Exporter Unions via intranet,
• Enabling the firms to monitor their processes online,
• Monitoring all movements related with the certificate. UFT and Exporter Unions, authorized by Inward
• Processing Regime to carry out various processes, will be able to use the system on-line and the system will be integrated with the Customs Automation.

4.5.4 eProcurement Infrastructure

The State Supply Office (DMO) has been serving with its 22 regional offices as a centralised public purchase institution in Turkey. DMO has more than 1,100 supply types in 203 different categories. With the Electronic Sale Project (e-Sale), an important step has been taken, by transforming all the catalogue purchase services to a web environment. DMO, which has the largest sale portfolio in the country, aims to become a model user in the government sector. DMO has initiated feasibility studies on electronic bidding.

Besides DMO, a Public Procurement Agency established in Turkey, aims to establish an Electronic Public Procurement Platform in cooperation with DMO. According to the statements of the e-Transformation Turkey 2005 Action Plan, the first phase of the eProcurement system will result in a database of procuring public agencies and vendors bidding for public tenders. The platform will ensure secure document exchange among the bidding and procuring parties, including the necessary legislative steps.

The Turkish public procurement system underwent a major reform in 2002 in order to address shortcomings identified such as:

- Most of the public agencies were not covered by the law, and had the right to issue their own regulations on procurement. This resulted a dozen of regulations covering different public agencies.
- Publication of notices was not required for all procurement methods and even when it was obligatory, announcement periods were too short to inform interested economic operators.
- Selection and evaluation criteria were not objectively determined and pre-announced.
Unsuccessful bidders were not informed about the decision of the contracting entity.

With the 2002 Public Procurement Law, an agency responsible for public procurement – the Public Procurement Authority (PPA) – was established at the central governmental level to ensure impartiality of procurement decisions and protect procurement officials from political influence in order to promote a level playing field for bidders.

The Public Procurement Authority, an administratively and financially autonomous entity which is also a legal person, is comprised of the Public Procurement Board, the Presidency and service units. Members of the Public Procurement Board are appointed by the Council of Ministers and must fulfill criteria, including higher education, more than 12 years of experience in public institutions, and knowledge and experience in the field of national and international public procurement procedures. Candidates cannot be actively engaged in the activities of a political party. Members of the Board are nominated for a five-year term, and can be re-elected once. Members cannot be revoked before the expiry of their term. Only in the event of serious illness or of a final court ruling can them be dismissed, on the approval of the Prime Minister. The Council of Ministers selects the Chairperson (and the Deputy Chairperson) of the Public Procurement Board from among its members. The Chairperson of the Board is also the President of the Public Procurement Authority.

The successful establishment of a separate body within the central administration responsible for public procurement matters is a distinctive positive step forward to regulate and monitor transparency and efficiency in procurement. The Public Procurement Authority has demonstrated its capacity to fulfill its primary functions, in particular:

- A comprehensive legal framework has been established;
- The Public Procurement Bulletin is issued regularly without delays, and the system of review is fully operational;
- Further efforts of the Authority also include;
- Developing guidance for ensuring the proper implementation of the legislation;
- Providing training for public and private sectors; and
- Compiling statistics related to procurement.

On the other hand, Information Society Strategy of Turkey particularly leans on the subject. In the strategy, establishment of an electronic public procurement system is considered as one of the essentials for modern public service transformation and savings on public sector expenditures. It is planned that a considerable portion of these savings will be created through electronic procurement expected to reach 90% in 2010.
4.5.4.1 Government Supply Office Electronic Sale Project (e-Sale)

The Government Supply Office (DMO) has been serving with its 22 regional offices as a centralized public purchase institution in Turkey. DMO has more than 1,100 supply types in 203 different categories. With the e-Sale project, an important step has been taken, by transforming all the catalogue purchase services to internet environment. DMO aims to be a model user in the government sector and also to have the largest sale portfolio of the country. With the e-Sale project, all the purchase services, which have been managed traditionally by paper, phone, and fax, had been transformed to electronic environment and the entire purchase process has been realized over internet. As well as order and shipment processes becoming much faster and communication costs decreasing sharply; human resources have also been used much more efficiently and effectively with the new system. Also, the scope of the office has been enlarged and a system, which is equally reached from all regions of the country, has been established.
4.5.4.2 Public Procurement Agency Electronic Public Procurement Platform

The objective of Electronic Procurement Systems is to support fundamentals and formalities to be observed in the process of public procurement while promoting basic principles by making use of information and communication technologies and to realize procurement transactions at minimum work load and cost expended by buyers and sellers. Electronic Procurement Systems can reduce the cost of the procurement process in duration, effort and economy of both buyers and sellers at the rate of two thirds and when operated properly it can save up to 20% of the public procurement budget.

Hence, erroneous or divergent interpretation of regulations in public procurement process by buyers and sellers, causing wrong or corrupt practices, are widely eliminated.

The Electronic Public Procurement Platform is a web environment in which administrations and suppliers are brought together and all documents related to tendering process can be exchanged securely. Administration will send their tender notices together with tender documents to the Electronic Public Procurement Platform and suppliers who are registered to the Electronic Public Procurement Platform will be able to read and download tender notices and documents.

Development of Supplier’s Database related to suppliers who want access to the Electronic Procurement Platform and read/buy tender notices and documents will be developed. Tender notices could be electronically mailed to registered suppliers according to the line of business that they deal with. A Supplier Database will be developed 3 stages:

Planned Architecture
4.6 General assessment

The field of e-Signature has not been adequately defined and regulated by laws. The arrangements made in this field were limited with the formation of a secure e-signature and specification of some technical criteria for the confirmation instruments. This situation shall create some risks that may give rise to the transformation of these investment made in this sector into lost investments. These risks may adversely affect the integration and interoperability of e-signature and e-implementation and cause this investment to become lost investment.

- The existing infrastructure and the business procedures should be reviewed and made ready for the usage of e-signature.
- A comprehensive and coordinated transition plan should be prepared so as to determine which entities start to use e-signature at what date and the cost savings and benefits obtained through the implementation of e-signature should be determined.
- In the investments to be made in the e-Government services; the e-signature necessities should be taken into account as well.
- The activities that should be carried out are not limited with the establishment of the KSM. At the same time; e-Signature should be established in the public entities. The costs of e-Signature can be classified under three titles. These are as follows:
  - The costs related to the implementation of the e-Signature.
  - The costs required for the harmonization of the e-Signature with the existing software.
  - Costs of certificate and card.

Apart from these costs, the public entities should conduct studies in order to establish the systems such as electronic document management and electronic archive and to ensure the information security in the transition to e-signature. These are all different cost items that require financing the amounts of which should not be underestimated and no study has been carried out so far concerning the cost of these items. Several public entities started to deliver e-Services before the e-Signature arrangements. Most part of the e-Services were designed without considering the usage of e-Signature. Thus this shall create problems in the implementation of the e-Signature and/or interoperability and the solutions to each of these problems shall bring out additional costs.

In order to ensure the most effective utilization from the limited resources:

- The priorities in the field of e-Signature should be designated in the public sector by considering the cost/benefits of the institutional projects.
- How the financing is obtained and the alternative financing opportunities should be evaluated by calculating the total costs resulted from the transformation of the public entities to e-Signature.
- A system should be developed in order to secure the procurement and production of new implementing softwares which are in compliance with the standards and e-Signature.
- Measures should be taken to harmonize the existing implementations about e-Services with e-signature in the most economic way.
- By considering the incompetency of the public officers in terms of information and experience; the legal framework of these fields and the rights and obligations of the software suppliers should be formed so as not to cause any waste of resources in short time.
5 Annex A: Contact details of National Correspondents

Contact Information of the person(s) completing the questionnaire. The person(s) will be contacted for any queries related to this questionnaire.

<table>
<thead>
<tr>
<th>Primary Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Organisation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alternative Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Organisation</td>
</tr>
</tbody>
</table>
### 6 Annex B: National Regulations Details

<table>
<thead>
<tr>
<th>National regulation title</th>
<th>National regulation translated title (English title)</th>
<th>Relevant links to on-line resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>5070 Sayı Elektronik mza Kanunu</td>
<td>e-Signature Law, #5070</td>
<td><a href="http://www.tk.gov.tr/eimza/eimzaya_yasasi.htm">http://www.tk.gov.tr/eimza/eimzaya_yasasi.htm</a></td>
</tr>
<tr>
<td>Elektronik mza ile İlgili Süreçlere ve Teknik Kriterlere İlişkin Teklif 'de Değişiklik Yapılmasına Dair Teklif</td>
<td>Communique for changing the communique of the processes and technical criteria of e-signature</td>
<td><a href="http://www.tk.gov.tr/Duzenlemeler/Hukuki/tebligler/eimza_degisiklik_20_06_06.doc">http://www.tk.gov.tr/Duzenlemeler/Hukuki/tebligler/eimza_degisiklik_20_06_06.doc</a></td>
</tr>
<tr>
<td>National regulation title</td>
<td>National regulation translated title (English title)</td>
<td>Relevant links to on-line resources</td>
</tr>
<tr>
<td>----------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
7 Annex C: Application questionnaire

7.1 Inward Processing Regime - Undersecretariat of Foreign Trade

7.1.1 Application identification

<table>
<thead>
<tr>
<th>Application/Service Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application/Service Name</td>
</tr>
<tr>
<td>Application/Service Type</td>
</tr>
<tr>
<td>Concerned sector</td>
</tr>
<tr>
<td>Application/Service Cross-Border Type</td>
</tr>
<tr>
<td>Level of Online Sophistication Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Intended &quot;clients&quot;</td>
</tr>
</tbody>
</table>

Abstract Description

Inward Processing Regime, this project is aimed at transferring all operations to electronic form. UFT is the coordinator of the project. In Turkey, firms apply to the UFT, filling out Inward Processing Permission Certificates, which are in the form of paper documents.

Identification of Application/Service Entities

Companies, Undersecretariat of Custom, Exporter Union

Procedural Details

Authentication and signature with e-ID.

Current status

Live since August 2005

Expected future developments

-

<table>
<thead>
<tr>
<th>Responsible Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organisation Name</td>
</tr>
<tr>
<td>Organisation Type</td>
</tr>
<tr>
<td>Date of interview</td>
</tr>
</tbody>
</table>
Application/Service System Details

<table>
<thead>
<tr>
<th>Communications Information</th>
<th>Project consists of the stages below:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Defining organisation and users</td>
</tr>
<tr>
<td></td>
<td>• Defining the companies</td>
</tr>
<tr>
<td></td>
<td>• Getting the application for the forms &amp; documents</td>
</tr>
<tr>
<td></td>
<td>• Evaluation of document flow &amp; documents</td>
</tr>
<tr>
<td></td>
<td>• Import &amp; export processes (Undersecretariat of Custom)</td>
</tr>
<tr>
<td></td>
<td>• Revising and tracking the documents (Exporter Union)</td>
</tr>
<tr>
<td></td>
<td>• Finalizing the documents (Exporter Union)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External interface</th>
<th>• Getting the application for the forms &amp; documents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Import &amp; export processes (Undersecretariat of Custom)</td>
</tr>
<tr>
<td></td>
<td>• Revising and tracking the documents (Exporter Union)</td>
</tr>
<tr>
<td></td>
<td>• Finalizing the documents (Exporter Union)</td>
</tr>
</tbody>
</table>

| Data structures processed by the application | • Applications submitted via internet |
|                                             | • All practices such as renewing, modifying, discharging |
|                                             | • done through on-line system |

7.1.2 eSignature details

<table>
<thead>
<tr>
<th>Legal aspects</th>
<th>The system relies on e-signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the system rely on a simple / advanced / qualified / other signature?</td>
<td>The system relies on e-signature</td>
</tr>
<tr>
<td>Is the signature required/recommended?</td>
<td>Required</td>
</tr>
<tr>
<td>Which strategies are planned for the future? Should different types of the electronic signature be supported, or are the strategies only related to the wide distribution/extension/circulation of the qualified electronic signature?</td>
<td>-</td>
</tr>
<tr>
<td>What is the legal basis (law, decree,…) for this application?</td>
<td>• Customs Law No. 4458 (Art.80, 108, 111, 115, 121) (OG No. 23866, dated 04.11.1999)</td>
</tr>
<tr>
<td></td>
<td>• Council of Ministers Decree No. 2005/8391 on Inward Processing Regime (OG No. 25709, dated 27.01.2005)</td>
</tr>
</tbody>
</table>
### Technical aspects

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How is liability/responsibility regulated? Does the national legal framework regulate more than the minimum demand of the directive 1999/93 EC?</strong></td>
<td>For this application, the user remains fully responsible for the timely and correct filing of the declaration.</td>
</tr>
<tr>
<td><strong>What are the parties involved in the signature process?</strong></td>
<td>The company (as the signatory), the UFT (as the relying party) and the Certification Authority (UEKAE (for the public institutions), e-Guven, Turktrust,...)</td>
</tr>
<tr>
<td><strong>What kind of token or credentials are used (smart cards, software certificates, paper tokens ...)?</strong></td>
<td>Software certificates</td>
</tr>
<tr>
<td><strong>What are the hardware requirements on the client side (e.g. smartcard reader/USB tokens) for the use of eSignature?</strong></td>
<td>Mostly smartcard or token</td>
</tr>
<tr>
<td></td>
<td>Minimum 256 MB</td>
</tr>
<tr>
<td></td>
<td>Minimum 256 KB ADSL</td>
</tr>
<tr>
<td></td>
<td>Gemsafe Card Reader / Omni Card Reader / Vasco Card Reader / ACS Card Reader</td>
</tr>
<tr>
<td><strong>What are the software requirements on the client side (e.g. OS/specific driver/middleware) for the use of eSignature?</strong></td>
<td>Windows XP or Windows 2000</td>
</tr>
<tr>
<td></td>
<td>Internet Explorer 6.0 +</td>
</tr>
<tr>
<td></td>
<td>Gemsafe Libraries 4.2.0 SP4</td>
</tr>
<tr>
<td></td>
<td>GTwinPRO Smart card reader Version 1.0.0.4 / OMNIKEY CardMan 3x21, Version 1.1.0.32 / Vasco DigiPass 850 Smart Card Driver</td>
</tr>
<tr>
<td></td>
<td>Java 1.5 Java Runtime Version 1.5.06 +</td>
</tr>
<tr>
<td><strong>What information is signed by the user and what is the objective of the signature?</strong></td>
<td>Authorization / authentication / application forms / required documentation</td>
</tr>
<tr>
<td><strong>Is this an application with multiple signatures for the same data and, if yes, what is the relationship between the signatures?</strong></td>
<td>No</td>
</tr>
<tr>
<td><strong>What are the relevant policies (CPS, certificate policy, signature policy)?</strong></td>
<td>-</td>
</tr>
</tbody>
</table>
### Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications

**NATIONAL PROFILE TURKEY**  
**April 2007**

<table>
<thead>
<tr>
<th>How are the signature/certificate presented to the application?</th>
<th>When user has filled-in his declaration, he is prompted to sign the data using his card or his token.</th>
</tr>
</thead>
<tbody>
<tr>
<td>What information is included in the certificate, and what is the role of this information in the functioning of the application?</td>
<td>Company profile for the identification &amp; authentication</td>
</tr>
<tr>
<td>Does the application rely on an existing generic eSignature framework (i.e. a set of commonly agreed standards)? If yes, describe the framework in the country general profile.</td>
<td></td>
</tr>
<tr>
<td>If no, specify which standards have been implemented in the eSignatures application? Depending on the signature type, this may include standards regarding certificates, signature formats, signature algorithms, token formats, other information security standards, etc.</td>
<td></td>
</tr>
<tr>
<td>Operations of ECSP</td>
<td>ETSI TS 101 456 and CWA 14167-1</td>
</tr>
<tr>
<td>QES</td>
<td>ETSI TS 101 862 and ITU-T Rec. X.509 V.3</td>
</tr>
</tbody>
</table>
| SC and V Data of Signatory | • 1024 bits for RSA or DSA or • 160 bits for ECDSA  
Up to 31/12/2008 |
| SC and V Data of ECSP | • 2048 bits for RSA or DSA or • 256 bits for ECDSA  
Up to 31/12/2008 |
| Hash Algorithm | RIPEMD – 160 or SHA – 1 or SHA-224 or SHA-256 or WHIRLPOOL |
| CP & CPS | IETF RFC 3647 |
| SSC and V Devices | CWA 14169 or assured to EAL4+ in accordance to ISO/IEC 15408 (-1,-2,-3) |
| Security Criteria | CWA 14167-1, ETSI TS 101 456 and ISO/IEC 17799 |
| Time-stamp | CWA 14167-1 and ETSI TS 101 861 |
| ECSP Certification | ISO/IEC 27001 |
| Security Requirements for Signature Creation Applications | CWA 14170 |
| e-Signature Format | ETSI TS 101 733 or ETSI TS 101 903 |

<table>
<thead>
<tr>
<th>How is the signature verified and how is the verification data processed and stored (directly connecting to the corresponding CA validation service or just through a Validation Service provided by a Validation Authority)?</th>
<th>Through a Validation Service provided by a Validation Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>What types of validation protocols are used for the electronic certificate validation? (OCSP, CRLs, SCVP…)</td>
<td>See above</td>
</tr>
<tr>
<td>How is the long term validity of the signatures (including long-term archiving of certificates and signatures) ensured?</td>
<td>-</td>
</tr>
</tbody>
</table>

### Organisational aspects
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which institutions, providers, etc. are involved in the signature scheme, and how do they relate?</td>
<td>General Secretaries of Exporters Unions, CSPs, companies</td>
</tr>
<tr>
<td>Who are the relying parties?</td>
<td>Authorization certificate can only be granted to the firms which can submit necessary documents to Undersecretariat for Foreign Trade (UFT) via General Secretaries of Exporters Unions (GSEU). These documents are inward processing project form, table of raw materials, signature circular, petition, trade registration journal, capacity report and other technical documents in some special cases. The firms have to put in a request for authorization certificate to UFT via GSEU with the necessary documents counted above. Applications are evaluated on the basis of economic criteria stated in IPR.</td>
</tr>
<tr>
<td>Who issues/manages credentials (e.g. certificates)?</td>
<td>-</td>
</tr>
<tr>
<td>What is the validity period of a credential (e.g. a certificate) and under which conditions can a credential be suspended or revoked?</td>
<td>-</td>
</tr>
</tbody>
</table>

28 « Relying Party » : shall mean an individual or organisation that acts in reliance on a Certificate or a eSignature
### 7.1.3 Interoperability

<table>
<thead>
<tr>
<th>Interoperability aspects</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the system accessible to non-nationals, and if so, how? If not, can the system be upgraded for cross-border interaction?</td>
<td>If valid certificates are provided from the mentioned CSPs, non-nationals can use the system.</td>
</tr>
<tr>
<td>What measures, if any, have been taken to ensure interoperability with signatures created and/or certificates issued in other countries?</td>
<td>-</td>
</tr>
</tbody>
</table>

### 7.1.4 Miscellaneous

<table>
<thead>
<tr>
<th>Miscellaneous</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there any statistics on the actual use of electronic signatures for this application (if not: please provide an estimation)?</td>
<td>-</td>
</tr>
<tr>
<td>Are there any legal/technical/organisational difficulties regarding the way in which electronic signatures are used in this application?</td>
<td>-</td>
</tr>
<tr>
<td>Are there any Government initiatives aimed at providing/encouraging the use of eID/ eSignature &quot;for this specific eGovernment application&quot; (e.g. through an awareness programme)?</td>
<td>-</td>
</tr>
</tbody>
</table>

### 7.1.5 Assessment

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please give your own assessment on the way how eSignature have been implemented in the concerned application (strengths, weaknesses).</td>
<td>-</td>
</tr>
<tr>
<td>Take this opportunity to bring any fruitful information that was not addressed by previous questions.</td>
<td>-</td>
</tr>
</tbody>
</table>