ANALYSIS OF ELECTRONIC SIGNATURE IN TURKEY FROM THE LEGAL AND ECONOMIC PERSPECTIVES AND THE AWARENESS LEVEL IN THE COUNTRY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF INFORMATICS
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

GÖKHAN İSKENDER

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF INFORMATION SYSTEMS

JULY 2006

Approval of the Graduate School of Informatics

_____

Assoc. Prof. Dr. Nazife Baykal

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Yasemin Yardımcı Çetin

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Dr. Altan Koçyiğit

Supervisor

Examining Committee Members

Prof. Dr. Semih Bilgen (METU) _____

Dr. Altan Koçyiğit (METU) _____

Dr. Ali Arifoğlu (METU) _____

Dr. Nur Saygı (Telecommunications Authority) _____

Assist. Prof. Dr. Uğur Soytaş (METU) _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Surname : Gökhan İSKENDER

Signature : _____

ABSTRACT

ANALYSIS OF ELECTRONIC SIGNATURE IN TURKEY FROM THE LEGAL AND ECONOMIC PERSPECTIVES AND THE AWARENESS LEVEL IN THE COUNTRY

İSKENDER, Gökhan
M.S., Department of Information Systems
Supervisor: Dr. Altan KOÇYİĞİT

July 2006, 161 pages

As in the case of other information technologies, the best way of obtaining efficient results from electronic signature application is integrating it to the legal and economic systems and increasing the awareness level of technology in the society. This thesis performs the legal and economic analyses of electronic signature in Turkey and measures the awareness level in the society. The analyses performed in the thesis show that electronic signature is not legally established in Turkey even the legal base is harmonious with European Union and it is expensive in practice even though its economic rate of return is high and the awareness level in the society which is measured in this study with a 20 questions test is not very high.

Keywords: Awareness Level, Digital Signature, Electronic Signature, Public Key Infrastructure, Survey on the Awareness Level of Electronic Signature.

ÖZ

ELEKTRONİK İMZANIN HUKUKİ VE EKONOMİK ANALİZİ VE TÜRKİYE'DEKİ BİLİNÇ DÜZEYİ

İSKENDER, Gökhan
Yüksek Lisans, Bilişim Sistemleri Bölümü
Tez Yöneticisi: Dr. Altan KOÇYİĞİT

Temmuz 2006, 161 sayfa

İletişim teknolojilerinin her biri türü için olduğu gibi elektronik imza uygulanmasında da verimli sonuçlar elde edebilmenin en iyi yolu söz konusu uygulamayı hukuki ve ekonomik sisteme iyi entegre etmek ve toplumdaki bilinç düzeyini arttırmaktır. Bu tez çalışması elektronik imzanın Türkiye için hukuki ve ekonomik analizlerini gerçekleştirmekte ve toplumun bilinç düzeyini ölçmektedir. Tezde yapılan yapılan analizler, yasal altyapı Avrupa Birliği ile uyumlu olmasına rağmen elektronik imzanın Türkiye'de henüz hukuki olarak yerleşmediğini, ekonomik olarak getirisi yüksek olmasına rağmen uygulamada pahalı olduğunu ve bu çalışmada 20 soruluk bir testle ölçülen toplumdaki bilinç düzeyinin de çok yüksek olmadığını göstermektedir.

Anahtar Kelimeler: Bilinç Düzeyi, Sayısal İmza, Elektronik İmza, Açık Anahtar Altyapısı, Elektronik İmzanın Bilinç Düzeyi Anketi.

To my family...

ACKNOWLEDGEMENTS

I am very pleased to present this thesis to Middle East Technical University to become part of the permanent collection of the library. In submitting the thesis, I complete a chapter of my life, one in which I had the fortune to interact with several great people who endowed me with faith, insight, and perseverance.

First, I thank my parents and sister who encouraged me to continue beyond my undergraduate studies, to my father who proceeded before me and to my mother and sister who encouraged me along the way.

To all my friends, especially Altuğ Kayışoğlu, Mustafa Kubilay, Hasan Karapınar, and Nurcan Alkış for sharing their brilliant ideas, advices, and for supporting me though the best and worst of times.

I give special thanks to my supervisor, Dr. Altan Koçyiğit, who recognized my potential, sparked my interest in this particular topic, and provided generous sponsorship along the way.

I also thank the staff of Middle East Technical University, Informatics Institute and the staff of Telecommunications Authority of Turkey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS AND ACRONYMS

AES	: Advanced Encryption Standard
APEH	: Hungarian Tax and Financial Control Administration
ATM	: Automated Teller Machines
B2B	: Business to Business
B2C	: Business to Consumer
B2G	: Business to Government
BİLTEN	: Information Technologies and Electronics Research Institute
BS	: British Standards
CA	: Certification Authority
CEN	: European Committee for Standardization
CENELEC	: European Committee for Electrotechnical Standardization
CESA	: Cyberspace Electronic Security Act
CIBC	: Canadian Imperial Bank of Commerce
CMR	: Cargo Management Re-engineering Project
CWA	: European Committee for Standardization Workshop Agreement
DEA	: Data Encryption Algorithm
DES	: Data Encryption Standard
DLL	: Dynamic Link Library
DSA/DSS	: Digital Signature Algorithm
DSİ	: General Directorate of State Hydraulic Works
EAL	: Evaluation Assurance Level
EBEV	: Electronic Tax System of Hungary
ECA	: External Certification Authority Program
ECDSA	: Elliptical Curve Digital Signature Algorithm

E-commerce : Electronic Commerce
ECSP : Electronic Certificate Service Provider
EDay1 : 1 September 2003
EDay2 : 1 February 2005
E-democracy : Electronic Democracy
EDI : Electronic Data Interchange
EEC : Elliptic Curve Cryptosystems
E-election : Electronic Election
EESSI : European Electronic Signature Standardization Initiative
EGM : General Police Headquarters
E-government : Electronic Government
ESC : European Standardization Committee
E-signature : Electronic Signature
ETSI SR : ETSI Special Report
ETSI TS : ETSI Technical Specification
ETSI : European Telecommunications Standards Institute
EU : European Union
FBI : Federal Bureau of Investigation
FIPS PUB : Federal Information Processing Standards Publications
G2B : Government to Business
G8 : Group of Eight Nations
HMAC : Keyed-hash Message Authentication Code
ICT : Information and Communication Technologies
ICTSB : Information and Communications Technologies Standards Board
IEEE : Institute of Electrical and Electronics Engineers
IETF RFC : Internet Engineering Task Force Request for Comments
IETF : Internet Engineering Task Force
IPP : Inward Process Project
ISC : International Standardization Committee
ISO : International Standards Organization
IT : Information Technology

ITC	: International Trade Chamber
ITU	: International Telecommunications Union
İMKB	: İstanbul Stock Exchange
KFTC	: Korea Financial Telecommunications and Clearance Institute
LUC	: Lucas Sequences
MD5	: Message Digest Algorithm Number 5
MİT	: National Intelligence Organization
NCC	: National Coordination Committee
NIST	: National Institute of Standards and Technology
NSA	: National Security Agency
OECD	: Organization for Economic Co-operation and Development
PDP	: Public Disclosure Project
PKI	: Public Key Infrastructure
RIPEMD	: RACE Integrity Primitives Evaluation Message Digest
RSA	: Rivest, Shamir and Adleman
SEEMail	: Secure Electronic Environment Mail
SHA	: Secure Hash Algorithm
SHA-1	: Secure Hash Algorithm Number 1
SPK	: Capital Markets Board
SSCDs	: Secure Signature Creation Devices
SSK	: Social Security Institution
TA	: Telecommunications Authority of Turkey
TNU	: Turkish Notary Union
TOBB	: Union of Chambers and Commodity Exchanges of Turkey
TSK	: Turkish Armed Forces
TÜBİTAK	: The Scientific and Technological Research Council of Turkey
UEKAE	: National Research Institute of Electronics and Cryptology
UNCITRAL	: United Nations Commission on International Trade Law
UNDP	: United Nations Development Program
US	: Unite States
USA	: United States of America

USB	: Universal Serial Bus
UYAP	: National Judgment Network Project
WTO	: World Trade Organization
XML	: Extended Markup Language

CHAPTER 1

Introduction

1.1. Overview

Development speeds of countries increase in parallel with their speeds of keeping up with technology. Internet which is the reflection of information age to today's life increases the speed of communication between people and institutions and it creates the opportunity of completing the processes, which were taking long time in the past, with one click today. This property of the Internet speeds up the information flow which is a part of business processes and this situation increases the importance of the concepts like confidentiality, security, reliability and non-repudiation of conveyed information. In the period between 1970's and today, studies were performed to provide secure communication and applications were developed to provide information security. The last reflections of these applications to today's life are public key infrastructure and electronic signature which depends on this infrastructure.

Handwritten signatures have been used as an approval mechanism for a long time. Article 14 of Turkish Law of Obligations Numbered 818 of 1926 states that, "Signature must be handwritten by the one who is under obligation. The signature which is formed by using a tool can only be valid if it is accepted by customs or if it is used in securities which are put into circulation in great quantity". [1]

What are the main reasons of making a handwritten signature so valid? The answers to this question can be derived as below if we look at the subject from a legal perspective:

1) Signature is trustworthy. In other words, it shows that the document is signed by the person who owns the signature.
2) Signature can not be duplicated. In other words, it shows that no one other than the person who owns the signature could have signed it.
3) Signature can not be used again. It is a part of document and can not be copied to another document.
4) Signed documents can not be changed.
5) Signature can not be repudiated.

In reality, these are not fully true. Signatures can be duplicated, they can be transported from one document to another or the content of a document can be changed after it is signed. The main aim of believing the truthfulness of the answers above is the difficulty of swindling and the weight of sentences[*].

These kinds of forgery can be performed in the electronic environment too. In fact, it is easier to duplicate signatures or change documents in the computer environment using powerful image or text editing software. On the other hand electronic transactions proliferate day by day in every part of the life including public and private sectors. People interact with governmental, financial or educational institutions over the Internet and their personal information is moved from one place to another many times as part of an electronic transaction. This huge amount of information transfer requires more and more advanced techniques to provide trust, security and reliability. Although there are a lot of techniques to

[*] For further information about the subject, please look at the Articles 208, 209, 210, 211 and 212 of Turkish Criminal Law No: 5237 which was published in the Official Gazette of 26 September 2004., Last Accessed August 12, 2005.

provide them, the newest and the most developed tool which can be used effectively is electronic signature.

Electronic signature can be defined as “data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication” [2]. In other words; electronic signature is a set of electronic characters, symbols and algorithms which are used to prove the identity of natural or legal persons. Electronic signature can be in many forms today:

1) Electronic signatures created by using biometrical properties of owners (e.g., fingerprint, eye retina, etc.).
2) Electronic signatures created by using special mathematical functions and algorithms (e.g., digital signatures).

Digital signature is a special kind of electronic signature which is added to electronically transmitted information by using a public key infrastructure. Digital signature and electronic signature will be used as synonyms after this point.

1.2. Background, Motivation and Rationale for the Study

Electronic signature started to be legally valid and to have a meaning in Turkey with the Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004. With this law, the responsibility of making secondary legislations was given to Telecommunications Authority of Turkey (TA). TA finished the preparation of secondary legislations including Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (Electronic Signature Ordinance) and Communiqué on Processes and Technical Criteria Regarding Electronic Signatures (Electronic Signature Communiqué) based on the studies of international organizations including the European Union (EU), World Trade Organization (WTO), International Trade Chamber (ITC), International Telecommunications Union (ITU), European

Standardization Committee (ESC), International Standardization Committee (ISC), European Telecommunications Standards Institute (ETSI) and United Nations Commission on International Trade Law (UNCITRAL) on 06 January 2005.

TA's second responsibility was the harmonization of electronic signature sector with Electronic Signature Law. Consistent with this aim, it was thought that, the root certificates of certification service providers should be generated in Turkey to make the application process easier and to use the infrastructure of electronic signature for the benefit of Turkey. In addition to this, all of the governmental institutions should be coordinated from the same organization and they should adopt the same infrastructure and standards to use the inadequate sources efficiently. As a result of these prerequisites, The National Research Institute of Electronics and Cryptology (UEKAE) which is a subsidiary of The Scientific & Technological Research Council of Turkey (TÜBİTAK) was assigned responsible for meeting the certification needs of governmental institutions. Some institutions related with internal and external security of Turkey including National Intelligence Organization (MİT), General Police Headquarters (EGM), and Turkish Armed Forces (TSK) were excluded from this rule because of their duties including higher security.

When the period between the beginning of these developments and today is analyzed, it is seen that, the process of integrating electronic signature to the governmental and private institutions has been continuing at a very low speed. As a prerequisite of using electronic signature, operations targeting inside and outside processes of institutions are being transferred to the electronic environment, but these transformations do not consider the studies of other institutions in an interoperable manner. As a result of this, the institutions form electronic gates to give information instead of establishing standardized infrastructures to perform electronic transactions in Turkey.

Widespread use of electronic signature could speed up the governmental applications such as: [3]

- Applications including governmental tests (e.g., Student Election Exam).
- Transactions between citizens and governmental institutions (e.g., Passport Application).
- Transactions between governmental institutions (e.g., Public Registration Office).
- Social security applications (e.g., The Pension Fund for Civil Servants).
- Health Applications (e.g., Health officials, hospital, pharmacy).
- Tax payments.
- Electronic election.

It is also expected that electronic signature will speed up the commercial applications such as:

- Internet banking.
- Insurance operations.
- E-orders and e-contracts.

The first step of providing a wider application of electronic signature is to examine the current situation from technical, application, legal and economic perspectives. The next step is to assess the awareness level and the ways to improve it.

The motivation behind this thesis is consistent with these steps which will broaden the level of understanding the subject. The thesis contains four main parts related to technical, application, legal and economic sides of the subject in addition to two surveys which aim to measure the awareness level. The thesis uses different methods like explanation, discussion, comparison, iteration, and modeling according to the characteristics of analyzed areas. The scopes of chapters are

designed to cover different perspectives to provide the readers an opportunity to understand the subject in a multi-perspective approach.

The chapter containing the technical analyses prepares a base for the readers to understand the technical basics of the subject while the chapter containing application analyses gives examples from the World, European Union and Turkey to enlighten the practical side of it.

The chapter containing legal analyses explains the entire Turkish legal base in a hierarchical way starting from Electronic Signature Law and continuing with related ordinances and communiqués. This chapter compares the Turkish legal base with other legal bases applied in European Union and other parts of the World and it evaluates the reflections of Electronic Signature Law on the other laws in addition to its special characteristics.

The chapter containing economic analyses has also a hierarchical structure which starts from the broadest perspective and ends with the narrowest one. This chapter firstly analyzes macro economic effects of electronic signature on the whole economy and then continues with micro economic effects on institutions and consumers.

The chapter containing awareness level analyses firstly focuses on institutional awareness level by using the results of a survey designed by Telecommunications Authority of Turkey. This chapter continues with evaluating the results of a survey designed for the study which aims to measure the personal awareness level.

1.3. Thesis Organization

This thesis focuses on technical, application, economic, and legal perspectives of electronic signature and aims to measure the awareness level of technology in Turkey. The thesis is composed of seven chapters. First chapter is the introduction.

Second chapter analyzes the subject from the technical perspective. Third chapter explains the development of electronic signature and gives application examples from World, European Union and Turkey. Fourth chapter contains a legal analysis which is performed over the current legal base of Turkey in a comparative manner with the practices of other countries from European Union and other parts of the World; while the fifth chapter contains an economic analysis which includes macro and micro perspectives. Sixth chapter focuses on institutional and personal awareness level. Seventh and the last chapter is the conclusion part which gives brief results about the analyses performed in preceding chapters and evaluates the possible future work.

CHAPTER 2

Cryptography and Electronic Signature: A Technical View

As electronic signature is a technological development, it is important to understand the technical side of subject to clarify the concepts used in the technology and to prepare a basis for the analyses in the following chapters. This chapter firstly focuses on history, current situation, popular approaches, usage areas and standards of cryptography and it continues with basic elements of good cryptographic methods, reflection of these elements on electronic signature and working logic of electronic signature.

2.1. History of Cryptography

Cryptography was firstly used by Egyptians nearly 4000 years ago. However, the most effective usage period of it was the two World Wars experienced in 20th century [4]. In this period, the main users were soldiers, diplomats and governments. Cryptography was used to hide national secrets and strategies.

In 1952, The National Security Agency (NSA) was established in USA. There were two aims of this organization one of which was capturing communication data of other countries and the other is providing military and state security [5]. After this, The National Institute of Standards and Technology (NIST) started to define

information security standards. This organization played an important role in defining the standards of Cryptography [6] [*].

In 1960's, with the advances in computer technology, it started to be important to protect electronically stored information and this led to a research project performed by Fiestel in IBM. This research was completed in 1974 and IBM patented "Block Cipher Cryptographic System" which provided a base for "Data Encryption Algorithm (DEA)". In 1977, "Data Encryption Standard (DES)" which depends on DEA was recognized as U.S. Federal Information Processing Standard. NIST re-certified DES in 1993 but announced that it would be replaced by "Advanced Encryption Standard (AES)" developed by Rijndael [7]. The main reason for this is that high performance/distributed systems can break DES in a short period of time. As a result of this, U.S. Government no longer uses it. Triple DES -three consecutive encryptions of the plain data by using DEA- is now being used until AES is adopted.

In 1976, Hellman and Diffie announced the "Public Key Cryptography" as a new dimension in cryptography. However the practical implementation of this subject was firstly performed in 1978 by Rivest, Shamir and Adleman [8]. This approach named as RSA (first letters of Rivest, Shamir and Adleman), is based on mathematical interactions of large prime numbers [**].

In 1991, the first international standard (ISO/IEC 9796) was accepted for the digital signatures. This standard depends on public key infrastructure of RSA [9]. In 1994, US Government accepted El Gamal public key infrastructure as a digital signature standard [10].

---

[*] For further information about the subject, please look at "Cryptography Section" at http://vote.nist.gov/032906cryptography-031420061.pdf, Last Accessed August 12, 2005.

[**] For further information about the subject, please look at "Public Key Cryptography History" at http://www.livinginternet.com/i/is_crypt_pkc_inv.htm, Last Accessed August 13, 2005.

2.2. Cryptography Today

In the cryptography area, research on creating new systems and research on improving existent systems continue nearly in the same speed today. New standards and new infrastructures are put into practice for the security needs of information society and it becomes difficult to categorize what is in cryptography and what is not because of the great expansion in the area. However any definition shall include the concepts of encryption, decryption and key.

Encryption means converting data into a form that can not be read without using sufficient information. Its main aim is preventing readability of documents even if they are captured by unauthorized people. Decryption is the reverse of encryption. Its main aim is providing the readability of encrypted documents. Encryption and decryption are performed by using secret information called as “key”.

Unencrypted message is called plain text. Encrypted message is called cipher text. The basic processes performed in a cryptographic application are illustrated in Figure 1.

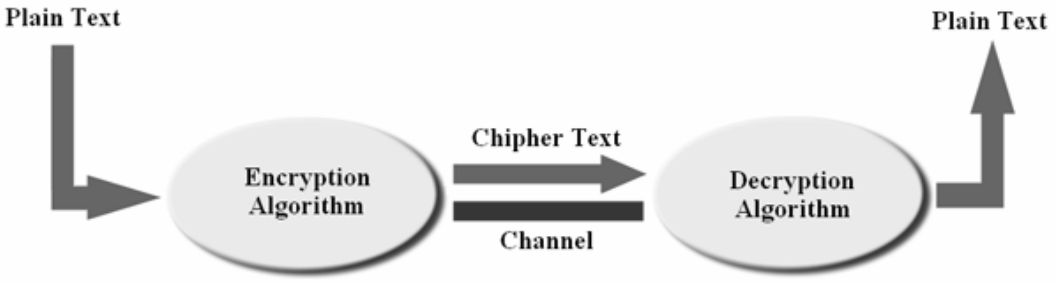


Figure 1: Encryption and Decryption

Today’s cryptography works with additional concepts which are further than encryption, decryption and key. One of these concepts is cryptanalysis. Cryptanalysis is the research area of solving complex cryptographic mechanisms

which contains interaction of hard problems. Another concept is cryptology. Cryptology is the discipline which combines cryptanalysis and cryptography.

2.3. Popular Approaches in Cryptography

A cryptographic algorithm is a mathematical relation which is used for encryption and decryption. If the reliability of this algorithm depends on hiding the working method of it, it is called a limited algorithm [11]. Limited algorithms are not sufficient for the security needs of today. This is because of the fact that a limited algorithm is known by a group which contains limited number of people and it must be changed each time a member of the group leaves. Furthermore these algorithms can not be applied widely because of the special structures of them. Although limited algorithms have some problems, they are used frequently in the processes which require low level of security because of their speed.

If the algorithm used in a cryptographic operation is not a limited one, it is called a key based algorithm. [11] Security and reliability of key based algorithms are dependent upon key(s). In other words, third parties can not decrypt the messages without knowing the key(s) used in the encryption process even if they know the working principles of algorithm. This property allows third parties examine the algorithm. Furthermore these algorithms can be published and mass production can be done over the products using these kinds of algorithms.

Today's cryptography is based mostly on key based algorithms and keys. Keys are special mathematical values which are used with known algorithms. All probable values that a key can take are called "key space" [12]. Some algorithms use same key for encryption and decryption while some do not. The ones using same key for both operations are called symmetric key algorithms while the others using different keys for each operation are called public key algorithms or asymmetric key algorithms.

2.3.1. Symmetric Key Algorithms

Symmetric key algorithms are called traditional algorithms and both the encryption and decryption process are performed by using the same key. These kinds of algorithms require users to come to an agreement on the key before the communication is performed. As a result of this, the reliability and security of these algorithms are dependent upon the secrecy of key. In other words, for a secure communication, the key shall not be known by third parties. Figure 2 illustrates the working principles of symmetric key algorithms.

Symmetric key algorithms can be classified into two groups. One of them is stream algorithms which work on a plane text by using one or eight bits. The other is block algorithms which work on a plane text by using bit blocks. Typical block size for modern symmetric key algorithms is 64 bits [13]. The most popular symmetric key algorithm is DES [14].

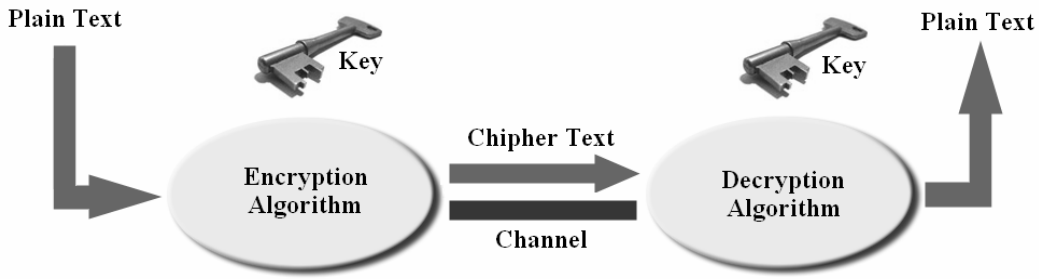


Figure 2: Symmetric Key Algorithms

2.3.2. Public Key Algorithms

Public key algorithms (also known as asymmetric algorithms) are designed with two keys instead of one. One of these keys is used for encryption and the other is used for decryption. The most important property of these algorithms is the fact that any of the keys can not be determined by using the other key. In this method, one of

the keys can be known by public. This key is often called “public key”. Other key is called “private key” and it is only known by the owner. Both keys can be used for encryption and decryption. If public key is used for encrypting the message, the process becomes encryption because of the fact that the cipher text can only be read by the owner of private key. If private key is used for encryption the process becomes signing as the cipher text can be read by everybody. Figure 3 illustrates the working principles of public key algorithms.

The most popular public key algorithm is RSA (Rivest, Shamir and Adleman). Other algorithms include Elliptic Curve Cryptosystems (EEC) and Diffie-Hellman Key Agreement Protocol [15]. Digital signature also uses RSA algorithm. However, it uses RSA for signing instead of encryption.

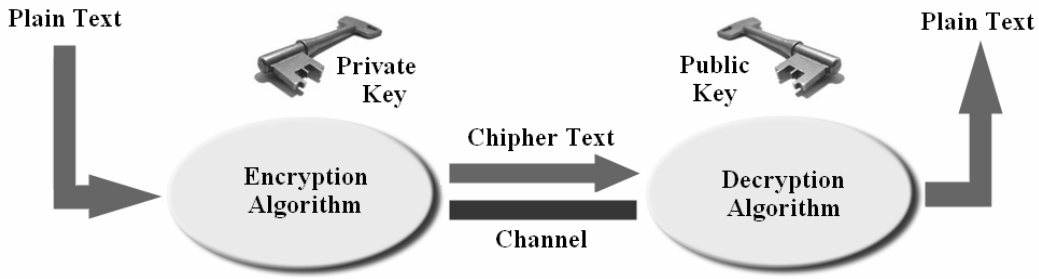


Figure 3: Public Key Algorithms

2.4. Usage Areas of Cryptography

Cryptography has a lot of usage areas. These areas can be classified as below:

- Secure communication: Secure communication is the main usage area of cryptography. Secure communication helps two or more people to communicate in a way that can not be understood by a third party. In smaller groups, symmetric key cryptosystems can provide a high level of security because it is easy to share secret keys in smaller groups. However in large

groups, especially in the ones which are geographically distinct, public key cryptosystems are more suitable since they allow two or more parties to communicate in an effective and secure way without knowing each other.

- Identification and authentication: Identification is a process of ascertaining the identity of an individual or an entity while authentication is the process of associating an individual or an entity with a predefined level of authority [16]. Authentication and identification are different. Identification requires that the verifier check the information presented against all the entities it knows about, while authentication requires that the information be checked for a single, previously identified entity. In addition, while identification must -by definition- uniquely identify a given entity, authentication does not necessarily require uniqueness [17]. For instance, someone logging into a shared account is not uniquely identified, but by knowing the shared password, he/she is authenticated as one of the users of the account. Furthermore, identification does not necessarily authenticate the user for a particular purpose.

- Secret sharing: One other usage area of cryptography is secret sharing. The basic idea in secret sharing is to divide the secret key into pieces and distribute the pieces to different people in a group so that certain subsets of the group can come together to recover the key [18]. This kind of an approach is used to distribute the risks and responsibilities between group members. All members of the subsets must come together to form the secret keys related with important data. As a result of this, the level of security increases.

- Electronic commerce: Electronic commerce covers areas like online banking, online trade, internet stores and etc. Today it is possible to buy a ticket, make a reservation, transfer money or lease a car over a computer. However, as the scope of the services increases, the possible and potential

security vulnerabilities also increase. Cryptography helps to encrypt personal data which flows between the users and service providers and blocks third parties viewing or altering these data. In a study that was performed by Koç Sistem over 1000 Turkish firms in 2004, it was seen that 87% of firms carried different security risks and 29% of them had high level security vulnerabilities [19]. Cryptography can help overcoming these security risks.

- Certification: Another usage area of cryptography is certification. In the certification process, trustworthy agents like certification authorities stand surety for unknown people or entities [20]. These trustworthy agents confirm the identities of third parties by using legal mechanisms like requesting ID cards and they create encrypted or signed certificates for them. Certification is developed for identification and authorization.

- Keys seizing: Key seizing means capturing private or secret key without notice to the user. This practice is useful in two situations. One of them is accidents. If a user deletes or looses his/her private key, seizing may be used to prevent bigger problems. The other situation is legal requirements. In some cases, government authorities like courts or police headquarters need private keys of people to enlighten crimes or to protect the continuity of state. In these situations, key seizing may be used. The legal validity of key seizing especially for the second situation is debatable. However in 1999, US Government passed the 4th Amendment of Cyberspace Electronic Security Act (CESA) [21] which defines the standards of seizing the decryption keys of users without notice [*].

- Access over a distance: Access over a distance means reaching important data which is found in another location. As the data and reaching point is

[*] For further information about the subject, please look at "Analysis of the CESA Access Standard" at http://www.cdt.org/crypto/CESA/cdtcesaanalysis.shtml, Last Accessed August 13, 2005.

geographically distinct, the confidentiality, integrity and availability of data shall be provided in a secure and reliable way. Cryptography provides high level of security for access over a distance.

- Other usage areas: Cryptography is not limited with computer world. It can be used in many areas ranging from cellular phones to broadcasting systems. The most important example of this is cellular phones. Cryptography is used for preventing unauthorized listening of cellular phones[*].

2.5. Standards of Cryptography

In order to work harmonious in cryptography world, there shall be some common standards. These common standards are developed with the cooperation of governments, private sector institutions, universities and other institutions. Today widely accepted standards about the cryptography and digital signature are mainly developed by International Standards Organization (ISO), International Telecommunications Union (ITU), National Institute of Standards and Technology (NIST), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF) and RSA Security. Appendix A lists these standards.

2.6. Basic Elements of Good Cryptographic Methods

Secure electronic communication depends on complicated cryptographic stages. There is no possibility of performing secure transactions without following these stages. These stages depend on the basic elements of good cryptographic methods. These elements can be classified as follows:

[*] For further information about the subject, please look at "Information About Clipper Wiretap Chip" at http://www.austinlinks.com/Crypto/non-tech.html, Last Accessed August 13, 2005.

2.6.1. Message, Encryption and Confidentiality

Electronic communication is a candidate for taking the place of written communication. The ability of performing secure communication over public electronic networks depends on confidentiality, security and reliability of information. Let us assume that a sender wants to send a message over a public network. As seen in Figure 4, this message is subject to listening and altering by third parties if it is not encrypted.

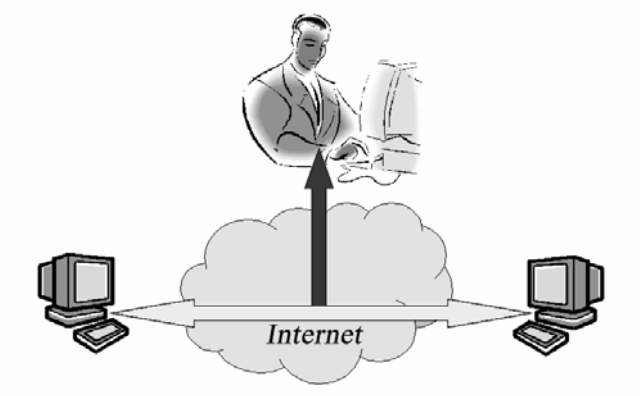


Figure 4: Listening by Third Parties.

2.6.2. Authentication, Identification, Integrity and Non-repudiation:

Cryptography must provide other services than confidentiality to provide real security. These services can be classified as below:

Authentication: A good cryptographic method shall allow authentication. Authentication confirms that all of the parties are clearly authorized to perform communication and no one other than authorized parties intervene the process. Authentication also helps identification if it links authentication information with identity information. The most common example of this linkage can be seen in automated teller machines (ATM). When the owner of a bank card enters his/her password, ATM uses this password for both authentication and identification of the user.

Identification: Identification means confirming the identity of other side (for both sender and receiver whether it is a real person or a server). Identification process guarantees the perfection of signatory to show the receiver who is involved in the process and from whom the actual message had come. A true and successful identification can be performed by using neutral and objective third party.

Integrity: A good cryptographic method shall provide message integrity. Message integrity ensures the message is not altered in any part of the communication process.

Non-repudiation: A good cryptographic method shall provide non-repudiation. Non-repudiation proves that message is really sent by the sender and it is really received by the receiver (Sender does not have a chance to claim that he/she did not send the message and the receiver does not have a chance to claim that he/she did not receive it).

2.7. Reflection of Basic Elements on Electronic Signature

As electronic signature is also a cryptographic application, it is also affected from basic elements of good cryptographic methods. When the reflection of basic elements on electronic signature is analyzed, it is seen that authentication, identification, integrity and non-repudiation has more importance than confidentiality in the electronic signature concept. This is because of the aim of the usage of electronic signatures. The main aim of electronic signature is to provide a secure and reliable trust relationship as in the case of handwritten signatures instead of a secrecy relationship. Providing authentication, identification, integrity and non-repudiation is sufficient for realizing this aim. As a result of this, confidentiality can be considered as the supporting element of electronic signature instead of basic element. Electronic signature technically allows providing confidentiality between two electronic signature owners. This can be performed by using the public key of receiver in the encryption of message. If the sender encrypts the message by using

the public key of receiver than the only person who can read the message will be the receiver. In other words only the private key can decrypt the message and the sole holder of it is the receiver.

Although it is technically possible, confidentiality is usually provided by other mechanisms like symmetric key algorithms or one time pads. This is because of the fact that public key algorithms work slower than most of the other algorithms. As a result of this, they are not usually preferred to sustain confidentiality.

2.8. Working Logic of Electronic Signature

There are a lot of public key algorithms which can be used for signing the documents. The most famous of them are Rivest Shamir and Adleman (RSA), El Gamal, Elliptic Curve, Digital Signature Algorithm (DSA/DSS) and Lucas Sequences (LUC)[*]. The most common of these is RSA (Appendix B explains the basics of RSA). The main method is so simple. Suppose that there are two people whose names are Bob and Alice. If Bob wants to communicate with Alice he follows the following two steps:

1) Bob signs the message with his private key and sends it to Alice.
2) Alice uses public key of Bob to verify the signature.

This method is very effective for a secure and reliable trust relationship because of the following reasons:

1) Signature is trustworthy because the public key of Bob verifies the signature belongs to Bob and Alice becomes confident that Bob had signed it.
2) Signature can not be duplicated because only Bob knows his private key.

[*] For further information about the subject, please look at "Public Key Algorithms/Cryptosystems" at http://security.ittoolbox.com/topics/t.asp?t=325&p=353&h2=344&h1=325&h3=353, Last Accessed August 13, 2005.

3) Signature can not be used again because it is a part of the message.
4) Signature can not be repudiated because Alice does not need the help of Bob to confirm his signature.

2.8.1. Problems Related with the Approach

Actually, the method explained above can not solve all the security and reliability problems. There are four main concepts which can create problems associated with this approach:

a) **Need for Time Stamps:** Sometimes the signing moment of the document is needed for some kind of electronic transactions. Think the message in above example as an order of payment. If Alice receives a message from Bob to collect money from bank, she may use the document which is signed by Bob for multiple times. The solution of this problem is time stamps. Time stamp means a small data added to electronic signature which includes date and time of the signature created.

b) **Need for a Certification Authority:** In the above example we assumed that there are no problems associated with obtaining public key of Bob. However in reality there some problems related with this. First of all Alice must know the public key of Bob really belongs to Bob. In other words someone may sign a document claiming that he/she is Bob and may send his/her public key to Alice to verify the process. In this type of a situation Alice takes the public key and decrypts the message. There is no problem associated with encryption, decryption or any other process. However the message comes from another person instead of Bob. This requires an authority to prove Bob's public key really belongs to Bob. These authorities are called "Certification Service Providers" or "Certification Authorities". Certification service providers may be governmental or a private institutions. In any case their job is to tie the identities of natural or legal

persons to their public keys. Certification service provider performs this function by issuing digital certificates for the public key of natural or legal persons and signing them with its own digital signature. Other important responsibilities of them can be classified as creating public and private keys for users, storing digital certificates for a long time, updating certificates and preparing list of revoked certificates.

c) **Need for Encryption of Message or Signature:** In the above example any person knowing the public key of Bob can read the message. What must be done if Bob wants only Alice reads the message. This problem can be solved by using two approaches. One of them is encrypting the document with Alice's public key and signing it with Bob's private key. If Bob encrypts the message with Alice's public key and signs it with his own key. No one other than Bob and Alice can read the content of message. If Bob does not want that somebody learn he had signed the document in addition to content confidentiality, he must follow the reverse process. He must firstly sign the document by his private key and than encrypt it with Alice's public key. Other and more suitable one for a faster communication is encrypting the message by using symmetric keys which are defined before the communication.

d) **Need for Hash Functions:** The main disadvantage of public key based algorithms is their slowness. If Bob wants to send a one page document with a relatively small key, there is no problem. But if he wants to send 2000 pages using a bigger key with the aim of increasing security, the algorithm works slower than expected because of the complex encryption mechanism. This problem can be solved by hash functions. Hash functions are used for summarizing messages. They are single dimension functions and they give same results for different messages very rarely. A little change in the document causes a big change in the summary of it so they guarantee that message is not altered. In the above example, if Bob applies a hash function

on the message and signs the summary instead of the message itself and adds this signed summary to the original message, he overcomes the performance problem. Hash algorithms are fundament to many cryptographic applications. Although widely associated with digital signature technology, the hash algorithms have a range of other uses. Secure Hash Algorithm Number 1 (SHA-1) and Message Digest Algorithm Number 5 (MD5) are amongst the most widely known, trusted and used ones. Another widely known hash algorithm is keyed-hash message authentication code (HMAC) which is a more complex algorithm utilized with a password [22]. The Secure Hash Algorithm (SHA) was developed by NIST and is specified in the Secure Hash Standard (SHS, FIPS 180). SHA-1 is a revision to this version and was published in 1994. It is also described in the ANSI X9.30 Standard. SHA-1 produces a 160-bit (20 byte) message digest. Although slower than MD5, this larger digest size makes it stronger against brute force attacks. MD5 was developed by Professor Ronald L. Rivest in 1994 [23]. Its 128 bit (16 byte) message digest makes it faster than SHA-1 in implementation.

A much better method considering the problems stated above is illustrated in the Figure 5.

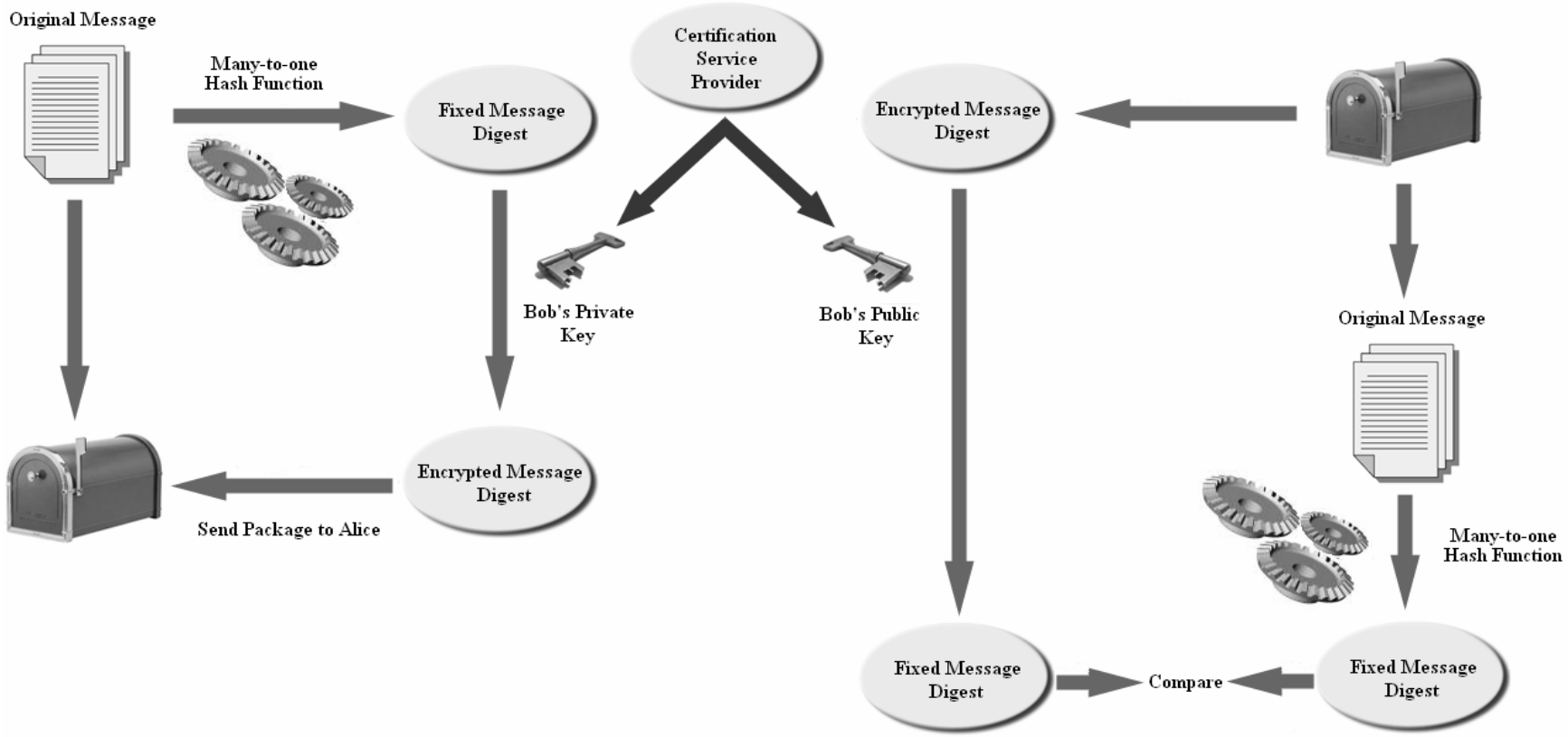


Figure 5: Processes of Electronic Signature

CHAPTER 3

Electronic Signature - Developments and Applications

This chapter reviews the developments and applications about electronic signature concept by giving examples from different parts of the world to analyze the practical implementation of electronic signature concept. The chapter focuses on developments and applications in three main regions which are World, Europe and Turkey.

3.1. Developments and Applications in the World

Developments and applications in the World about electronic signature concept can be classified as below:

3.1.1. Studies in the World

The concept of electronic signature started to be used in 1996 in the world and currently most of the countries defined the legal scope of it. It is expected that global online trade will expand to $12.8 trillion by the end of 2006 [24] and electronic signature is the key factor which makes these applications secure, efficient and effective. The most important developments in the e-signature concept are “Model Law on Electronic Commerce of 1996” [25] and “Model Law on Electronic Signature of 2001” [26] which are designed by United Nations

Commission on International Trade Law (UNCITRAL)[*]. Most of the countries in the world used these two laws to establish their legal base in the electronic signature concept.

European Union published EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures to define the basis of electronic signature. Article 1 of Directive contains the following sentence that defines the purpose of it.

> *The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.* [27]

EU Directive 2000/31/EC of Electronic Commerce of 8 June 2000 which is published to provide free circulation of information system services among member states also defines the electronic agreements and the legal results of them. This situation is stated in the Article 1 of directive as: "This Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States." [28]

The main obstacle in front of the general acceptance and usage of e-signature in the world is the absence of interoperability. Each country follows a different approach and sets up its own certification service providers. If these service providers are not associated with each other by using proper mechanisms like cross certification, the validity of signatures are isolated in geographical boundaries of the countries. Cross certification means "The process undertaken by certification authorities to establish a trust relationship" [29]. When two certification authorities are cross certified, they agree to trust and rely upon each other's public key certificates and keys as if they had issued them themselves. The two certification authorities exchange cross

---

- For further information about the subject, please look at "United Nations Commission on International Trade Law" at http://www.uncitral.org,, Last Accessed October 6, 2005.

certificates, enabling their respective users to interact securely. An additional problem is the cost of e-signature. Obtaining an electronic signature has a cost of approximately 60 Euros in Europe [30]. This cost is 80 US Dollars in US and 200 YTL in Turkey [31, 32].

The dates at when American countries started to use electronic signature can be listed as below [33]:

1999: Bermuda, Peru, Colombia
2000: United States
2001: Canada, Argentina

The dates at when European countries started to use electronic signature can be listed as below:

1997: Italy
1998: Germany
1999: Portugal, Spain
2000: France, Denmark, Luxembourg, England, Ireland, Austria, Czech Republic, Estonia, Lithuania, Slovenia
2001: Belgium, Hungary, Norway, Sweden, Island
2002: Netherlands, Poland
2004: Turkey

The dates at when Asian countries started to use electronic signature can be listed as below:

1995: Russia
1998: India
1999: Singapore
2000: Japan, Hong Kong, Philippines
2002: Thailand

3.1.2. Example Applications in the World

The most common usage area of electronic signature is online banking. Personal online banking is used nearly for a couple of years in the world. Traditionally it is performed by using tokens and one time passwords. Currently electronic signature is mostly used for logging onto the electronic systems but the operations performed by using certificates and electronic signature increases day by day. On the other hand smartcard infrastructure is also used in personal online banking but it is not used as widespread as business to business trade [34]. In other words, the main transaction tool used in business to business trade over electronic networks is smartcard infrastructure. This is because of the need for high level of security.

E-government is on the way of being another usage area of electronic signature. Some countries like United States, Japan, England, Germany, Austria, Finland, Italy, Denmark, Ireland, Sweden, Slovenia, Czech Republic, Poland Romania, Colombia, Singapore and India started applications of e-government while some others like Netherlands, Belgium and Hungary plans to start them [35]. E-government applications mainly depend on electronic identification cards.

In the following, some recent examples of electronic signature applications in the world are briefly explained.

USA - External Certification Authority Program of US Ministry of Defense

External Certification Authority Program (ECA) is designed for increasing the security of online transactions between US Ministry of Defense and suppliers of Ministry. ECA depends on digital certificates provided by VeriSign and it covers three important systems which are “Security Travel System”, “Document Entry System” and “General Business Processes System” [36]. ECA eliminates most of the security risks associated with these systems and increases the speed of business transactions which in turn leads to more efficiency and effectivity. It is thought that

ECA will develop more in the future to cover 350.000 partners of US Ministry of Defense.

USA - FBI Smart IT Security Nationwide

"Smart IT Security Nationwide" system is designed for Federal Bureau of Investigation (FBI) by Northrop Grumman Corporation. It depends on public key infrastructure to provide increased security for FBI's information technology systems. The system contains approximately 35.000 FBI users which have smartcards containing their identification and authentication details. The main aim of system is to ensure that individuals are identified properly prior to granting them access to electronic information and systems. The technology is part of the defense "in depth layered" security for the FBI and protects FBI employees with the ability to encrypt data, digitally sign documents and e-mail, and ensures non-repudiation of these actions [37]. In addition to this, it is flexible enough to cover more workers in the future.

Canada - Canadian Imperial Bank of Commerce

Canadian Imperial Bank of Commerce (CIBC) is one of the leader financial institutions of Canada which has more than 9 million personal and institutional customers in North America. CIBC provides all banking operations in an online environment by using its developed electronic network. The bank also works as the processing center and partner of VeriSign in Canada. CIBC's processing center covers PKI platform of VeriSign in order to provide secure web servers and qualified certificates [38]. The bank also works in the business of marketing, selling, maintaining and managing of these services. CIBC is the first bank in Canada which provides the opportunity to perform all banking operations online by using electronic signature. This opportunity brings CIBC increased customer satisfaction, increased time efficiency and decreased costs.

Australia - Cargo Management Re-engineering Project (CMR)

Cargo Management Re-engineering Project (CMR) is designed for the Australian Customs by SecureNet Company. The system is designed to provide the public key infrastructure (PKI) and services required for government's new online import/export system [39]. The main of the system is to modernize the handling of products coming in and out of Australia. The main functions of system include generating, storing and managing digital certificates and signatures as well as the associated PKI policies and procedures for cryptography.

South Korea - Korea Financial Telecommunications and Clearance Institute

In South Korea, all the Internet based financial transactions require users to possess official cyber certificates and digital signatures. This is because of the need for ensuring security and accountability in cyber exchanges. In May 2003, all of the existing certificates provided to banks and financial institutions were converted into official certificates provided by the Korea Financial Telecommunications and Clearance Institute (KFTC) [40]. KFTC only issues official certificates for financial institutions interested in starting online banking services and covers all of the shareholders who perform online banking operations like internet banking or online stock trading. The certificates issued by KTFC can also be used by people for the operations related with government institutions including complaints and suggestions. The digital certificates can also be used for taking part in government bids.

New Zealand - Secure Electronic Environment Mail

New Zealand government uses Secure Electronic Environment Mail (SEEMail) system to provide secure online communication between governmental institutions. The system is designed to facilitate the exchange of email and attachments in a secure way by using public key cryptography over the Internet [41]. It is capable of

protecting public domain information and information classified in confidence, sensitive and restricted. Nearly 30 governmental institutions use SEEMail system and the number of them increases day by day.

3.2. Electronic Signature in Europe

Developments and applications in Europe about electronic signature concept can be classified as below:

3.2.1. Studies of European Union about Electronic Signature

The Council and the Parliament of European Union published its Framework Directive No: 1999/93/EC about e-signature in the Official Gazette of Europe at 13 December 1999.

As stated in the Article 1 of Directive, two major aims of the Directive are [27]:

- to facilitate the use of electronic signatures and contribute to their legal recognition.
- to establish a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.

This Directive forms a draft for the application of electronic signature in European Union and provides the legal recognition of certificates, electronic signatures, minimum standards of tools used for creating electronic signatures and voluntary accreditation. It also provides new norms on security and international cooperation. Before the Directive some countries were using different special laws for the subject (e.g., Germany, Italy). EU's Directive was prepared to provide harmonization between member states and went into effect in all member states at

17 July 2001. The Directive has four annexes which clarify the practical side of the subject. These four annexes are as follows:

- Annex 1: Requirements for Qualified Certificates
- Annex 2: Requirements for Certificate Service Providers Issuing Qualified Certificates
- Annex 3: Conformity of Secure Signature Creation Devices (SSCDs)
- Annex 4: Secure Signature Verification

Information and Communications Technologies Standards Board (ICTSB) is an organization which was established in the information and communication technologies area in Europe by three standardization institutions which are CEN, CENELEC and ETSI [42].

European standardization institutions established European Electronic Signature Standardization Initiative (EESSI)* program in the custody of ICTSB with the support of European Commission. The main aim of EESSI is to define standardization needs which arise in the practical implementation of E-signature Directive. In the report of EESSI expert team, dated 20 July 1999, new requirements on standards were evaluated from a general point of view and three topics stated below found important for the future of e-signature [43]:

- Quality and operational standards of certification service providers.
- Interoperability standards of e-signature.
- Quality and operational standards of signature creation and verification equipment.

* For further information about the subject, please look at "EESSI Home" at http://www.ict.etsi.org/EESSI_home.htm, Last Accessed October 11, 2005.

EEESSI was focused on Public Key Infrastructure (PKI) to support electronic signature. Main points were defined as follows:

- Security needs for signature products.
- Certification and registration of the suitability of products and services
- Security management and certification policy for certification service providers which provide advanced certificates.
- Creating and verifying signatures.
- Coding scheme and syntax of e-signature and technical side of e-signature policies
- Standard for using X.509* public key certificates as Advanced Certificates.
- Interoperability protocol of cooperation with time stamp authority.

Signature types suggested in this report and attributed to the Directive are classified in Table 1.

3.2.2. Example Applications in Europe

In the following, some recent examples of electronic signature applications in Europe are briefly explained.

Austria - Electronic Health Insurance Card

Electronic Health Insurance Card system is designed for Austrian government by a consortium consisting of Siemens Austria, IBM and Telekom Austria [44]. The main aim of system is replacing Austria's current paper-based healthcare vouchers

* For further information about the subject, please look at "X.509 Information Technology" at http://www.itu.int/rec/T-REC-X.509/en ,Last Accessed October 12, 2005.

and eliminating the need to issue and process an annual volume of more than 40 million vouchers. Personal information of patients like name, title, date of birth, and social insurance number are written on the chip of the card. The card also allows digital signing with the aim of letting card holders use it for electronic transactions with government authorities. The system connects 12.000 doctors to the computing centre network of the Federation of Austrian Social Security Institutions and increase efficiency by balancing the inputs and outputs of the health processes in a secure way.

Germany - Köln City Card Project:

This project contains the adaptation of business processes in the municipality to the secure electronic environment for the use of employees and citizens. It provides a solution to the problems related with electronic communication between citizens and municipality and legality of signatures. The project uses a combined approach which integrates the public key infrastructure with smartcards [45]. As a result of the project, business processes improved with the help of electronic signatures and they are expanded to the areas of education, health and culture by means of smartcards.

Italy - Ministry of Internal Affairs ID Card Project

Italy is the second country which starts to use electronic ID card. Italian Ministry of Internal Affairs designed a new ID card based on smartcard infrastructure to develop the relations between citizens and government authorities on electronic networks instead of governmental buildings. The project uses central PKI management to distribute electronic ID cards from municipalities to perform electronic transactions and it includes 280.000 citizens from 83 municipalities of Milano, Palma and Rome in the pilot study period [46]. Italian government plans to distribute 40 million electronic ID cards in a five year period.

Table 1: Signature Types

Signature Types	Explanation	Legal Proof Level
Electronic Signatures stated in the Article 5.2 of Directive	Any signature which is not an Advanced Electronic Signature.	Can not be repudiated.
Advanced Electronic Signatures stated in the Article 5.1 and Annexes I, II and III	Signature which requires minimum technical level to be equivalent with handwritten signature.	Have same effects with handwritten signature.
Enhanced Electronic Signatures	Signature which has additional technical data (like time stamp) to increase technical security	Increase the level of technical proof.

Source: Final Report of the EESSI Expert Team [43]

Denmark - EDay1 and EDay2

Denmark is the first country in the world that gives a general right for public authorities to communicate electronically between themselves. The legislation about this right came into force at 1 September 2003 and this day was called EDay1. EDay1 covers all central and local government institutions and provides them the opportunity to send and receive documents electronically to all other public bodies, with the exception of sensitive data and documents. This exception is cancelled by EDay2, which gives all Danish citizens a legal right to communicate electronically with central government bodies at 1 February 2005. EDay2 allows the electronic exchange of sensitive information, including the legitimate sharing of personal data [47]. Public authorities have prepared themselves for EDay1 and EDay2 by establishing secure e-mail solutions depending on digital certificates and by adapting their working practices to the electronic environment. In addition to this, both EDay1 and EDay2 are supported by public campaigns.

It is expected that EDay1 and EDay2 will allow the Danish public sector to save €143 million over 4 years because of the fact that it will be faster and more reliable to exchange information between authorities, citizens and businesses.

Hungary - EBEV Project

The Hungarian Tax and Financial Control Administration (APEH) mandated the 10.000 largest Hungarian taxpayers submit their tax returns online in 2005 using an electronic filling system called EBEV [48]. The system was introduced as a pilot study covering 500 corporate taxpayers in 2003 and it was extended to 3.000 largest taxpayers in 2004. It allows electronic submission of tax returns through the internet by using digital signatures. Although EBEV users represent less than 1% of the total of Hungarian taxpayers it is expected to generate significant savings on the processing of tax returns. This is because of the fact that the amount of tax paid by this little group of taxpayers consists nearly half of the money in circulation.

Hungarian government plans to cover 350.000 taxpayers by EBEV system in 2006 to decrease the costs and the number of errors in the tax collection period.

3.3. Situation in Turkey

In this section developments and applications in Turkey pertaining electronic signature are explained.

3.3.1. Studies of Turkey about Electronic Signature

E-signature concept is under the custody of Telecommunications Authority in Turkey. Telecommunications Authority started to work about the subject in the beginning of March 2004 and formed "National Coordination Committee" whose members are from different organizations including private institutions, governmental institutions and universities. National Coordination Committee was divided into three working groups to focus on different points. These working groups are Infrastructure Working Group, Information Security and Standards Working Group, Legal and Regulatory Working Group. The working calendar of National Coordination Committee is given in Table 2.

This hardworking period was depending on the E-signature Law No: 5070 which was published in the Official Gazette of 23 January 2004 and focusing on preparing an ordinance which was explaining the practical side of articles stated in the Law. This ordinance named, "Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law" was published in the Official Gazette of 6 January 2005. After this date, the legal base continued to grow. New additions to the legal base can be classified as follows:

- Ordinance on Amendment over Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law dated 04.02.2006

- Communiqué on Processes and Technical Criteria Regarding Electronic Signatures dated 06.01.2005
- Communiqué on Amendment over Communiqué on Processes and Technical Criteria Regarding Electronic Signatures dated 18.06.2005
- Communiqué on Amendment over Communiqué on Processes and Technical Criteria Regarding Electronic Signatures dated 21.01.2006
- Ordinance on Insurance of Financial Liabilities in Certification dated 26.08.2004
- General Provisions Related with Mandatory Insurance of Financial Liabilities of Certification dated 27.01.2005
- Tariffs and Instructions Related with Insurance of Financial Liabilities in Certification 27.01.2005
- Circular of Prime Ministry numbered 2004/21 dated 09.06.2004
- Circular of Prime Ministry numbered 2006/13 dated 19.04.2006

Table 2: Calendar of E-Signature National Coordination Committee

E-Signature National Coordination Committee (NCC) Work Plan						
Studies	**2004**					
	March	**April**	**May**	**June**	**July**	**August**
1st NCC Meeting	**19**					
Establishing working groups, defining their functions, principles and draft work plans.	**30**					

Table 2 (continued)

2nd NCC Meeting - Making the work groups and the content of draft work plans definite.		13				
Submitting progress reports to Telecommunications Authority.			31			
Submitting conclusion reports to Telecommunications Authority and taking the opinion of NCC				30		
3rd NCC Meeting - Discussing the conclusion reports of working groups in NCC.					19	
Submitting additional opinions about conclusion reports to Telecommunications Authority.						13

Source: Telecommunications Authority of Turkey [49]

3.3.2. Example Applications in Turkey

There are two projects related with the application of electronic signature in Turkey. These are Public Disclosure Project (KAP) of Capital Markets Boards of Turkey and Inward Process Project (DİP) of Undersecreteriat of The Prime Ministry for Foreign Trade.

In the following these two projects which are related with the application of electronic signature in Turkey are explained briefly.

Public Disclosure Project (KAP)

The main aim of Public Disclosure Project is transferring financial tables, special situation statements and other announcements of publicly held companies and all intermediary institutions over computer networks in a secure way by using electronic signature. The project is designed by the cooperation of two institutions which are İstanbul Stock Exchange (İMKB) and Capital Markets Board (SPK) [50]. All independent auditing companies are also in the scope of Public Disclosure Project when signing the financial tables.

Public Disclosure Project contains all requirements of a full e-government application including government (SPK), firms (KAP companies) and citizens (investors). As a result of this, it is an important information system investment in the process of adopting European Union. KAP covers nearly 530 companies and 2500 users spread all over the Turkey [51].

In the scope of KAP, some software is developed for the companies. Companies use this software to fill out their announcements and these announcements are signed by using electronic signatures in a predetermined hierarchical way. After signing process, the announcements are sent to Capital Markets Board over the Internet. These announcements are saved to the KAP database and they are shared with public instantly. Companies can save their announcements offline by using the software and then they can send them when they are online. In some periods, independent auditing firms sign the documents in a manner that is harmonized with the signing hierarchy to join the announcement process.

KAP is the first institutional application in Turkey which integrates electronic documents with certificates and electronic signatures. It is designed as an open architecture system that can be improved for additional needs which may arise in the future.

Inward Process Project (DİP)

Inward Process Project (DİP) of Undersecreteriat of The Prime Ministry for Foreign Trade is a project that contains 5000 companies which are members of 13 exporter unions, union users, port of entry users and experts of Undersecreteriat of The Prime Ministry for Foreign Trade [52]. Bureaucratic delays in the transportation and permission of inward process authorization documents decreased to minimum with this project. Companies which want to get permission for trade documents can use the Internet for application and for following their permission process by using the system. The Undersecreteriat of Foreign Trade also carries out the inner work flows by using electronic networks. Both the Foreign Trade Experts and company users use electronic smartcards to verify their identity in the electronic environment. In addition to this, electronic signature is also incorporated into the process to provide integrity and non-repudiation. This functionality is ensured by using Zeugma PKI software [53] which is designed by Information Technologies and Electronic Research Institute (BİLTEN) which is a joint subsidiary of The Scientific & Technological Research Council of Turkey (TÜBİTAK) and Middle East Technical University (METU).

Electronic signature application designed by The Undersecreteriat of Foreign Trade is taking electronic signature services from public certification authority which is The Scientific & Technological Research Council of Turkey because of the adaptation process to the legal base.

CHAPTER 4

Legal Analysis of Electronic Signature in Turkey

As electronic signature shall have the same legal effect with that of handwritten one, it is important to analyze the legal side of the subject. This is because of the fact that the same legal effect brings the same legal responsibility. This chapter firstly focuses on Electronic Signature Law No: 5070 in a manner emphasizing the structure, special characteristics and reflections of it and then explains the other related legal base including ordinances, communiqués, provisions and circulars.

4.1. Electronic Signature Law No: 5070

Electronic signature is defined as "data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication" [54]. This definition comes from the Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004 (E-signature Law). This law gives the responsibility to Turkish Telecommunications Authority about the subject.

E-signature Law will perform a critical role in the e-government and e-trade applications if it is explained to the public in a scientific and a proper way. This is because electronic signature is an important tool which is used for authentication of parties in the public networks including the Internet.

4.1.1. Definitions & Concepts According To Electronic Signature Law No: 5070

As electronic signature is a new technological development which includes new technical concepts, the legal base shall define these technical concepts as clear as possible to diminish the number of misunderstandings. Definitions and concepts according to Electronic Signature Law No: 5070 are stated in the following sections.

4.1.1.1. Electronic Data

According to E-signature Law, electronic data means "Records which are created, conveyed and stored by means of electronic, optic and similar ways" [54]. The definition of electronic data does not appear in EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (E-signature Directive) and most of the other foreign electronic signature laws. It appears only in the Irish Law; however, the definition in the Irish Law includes not only digital data but also other types of electronic data which include biometric or photonic properties [55].

4.1.1.2. Electronic Signature

According to E-signature Law, electronic signature means "Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" [54]. This definition is same with the definition which appears in E-signature Directive. The word "authentication" is used in Turkish translation as "authenticating the user" however it means "authenticating the data" in the E-signature Directive. As a result of this, authentication shall not be understood as "approving the identity". It shall rather be understood as an approval mechanism for the data. This point emphasizes another interesting point that e-signature does not have to include the identity of data owner. In other words, any

data which can authenticate another data can be named as e-signature. The phrase "identify" which means "approving the identity" appears in the definition of "Advanced Electronic Signature" in E-signature Directive [2]. As a result of this "authentication" shall not be used as a synonym for "identification" while interpreting the E-signature Law.

4.1.1.3. Signatory - Owner of Electronic Signature

According to E-signature Law, signatory means "A natural person who uses signature-creation device" [54]. This definition looks like the definitions on the E-signature Directive and other foreign e-signature laws. Turkish E-signature Law allows only natural persons to be a signatory but natural persons can create and use e-signature on the behalf of other legal persons if they are clearly authorized in the certificate. This property of law is designed for solving potential problems related with legal persons but it is not sufficient because of the certification service providers. As a natural result of the public key infrastructure (PKI), certification service providers must have certificates and electronic signatures to sign the certificates of their customers and Turkish E-signature Law does not allow them to have electronic signatures. Currently the problem seems to be solved by representative mechanism explained above but it may create more complex problems in the future when the number and customer base of certification service providers increase. The E-signature Laws of Ireland [55] and Austria [56] allow legal persons to have electronic signature to solve these kinds of problems and this is a better approach. The directive also defines signatory as "A person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents" [2].

4.1.1.4. Signature Creation Data

According to E-signature Law, signature creation data means "Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an

electronic signature" [54]. This definition is the same definition which is used in the E-Signature Directive and it is defined same in other foreign legal bases. It indicates the "private key" concept which is used in practice. The main aim of defining this type of data as "signature creation data" instead of "private key" is the need for creating a technology independent law. As the process of creating a law and putting it into practice is a complex and difficult task, the law maker wants to design the regulation technology independent to use it more effectively. In addition to this, technical requirements like key length, hash value or random creation value are regulated by using Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law (Electronic Signature Ordinance) and Communiqué on Processes and Technical Criteria Regarding Electronic Signatures (Electronic Signature Communiqué). In practice signature creation data can be formed by both certification service providers and certificate owner.

4.1.1.5. Signature Verification Data

According to E-signature Law, signature verification data means "Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature" [54]. This definition is also the same definition which is used in the Electronic Signature Directive and other foreign legal bases and it indicates the "public key" concept which is used in practice.

4.1.1.6. Signature Creation Device

According to E-signature Law, signature creation device means "Software or hardware device used to create signature" [54]. This definition is very similar to the ones in Electronic Signature Directive and other foreign legal basis. In reality the directive defines the concept in a more proper way by integrating the "signature creation data" into definition. Electronic Signature Directive defines the signature creation device as "configured software or hardware used to implement the signature creation data" [2]. This is more proper as the signatory creates electronic

signature by using signature creation data. In practice, signature creation devices can be classified as hardware based and software based ones. The hardware based devices include smartcards, USB tokens, computers or personal digital assistants (PDA) while the software based devices include soft certificates, computer software and operating systems.

4.1.1.7. Signature Verification Device

According to E-signature Law, signature verification device means "Software or hardware device used to verify signature" [54]. This definition is also very similar to the ones in Electronic Signature Directive and other foreign legal basis. In reality, the directive defines the concept in a more proper way by integrating the "signature verification data" into definition. Electronic Signature Directive defines the signature verification device as "configured software or hardware used to implement the signature verification data" [2]. This is more proper as the third parties verify electronic signature of signatory by using signature verification data. In practice signature creation devices can also be used signature verification devices. However Turkish E-signature Law defines them in a distinct manner. As a result of this, the law permits standalone creation or verification devices. At first sight, it seems as a good property for obtaining flexibility in legal base; however, it creates additional burden on law maker to define the standards twice for each category.

4.1.1.8. Secure Electronic Signature Creation Devices

According to the Article 6 of E-signature Law [57];

> *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 can not be derived in any means and their secrecy is assured.*

c) *Electronic signature creation data recorded in those devices can not be obtained or used by third parties and electronic signatures are protected against forgery.*
d) *The data to be signed can not be altered by anyone except the signature owner and can be seen by the signature owner before the generation of signature.*

4.1.1.9. Secure Electronic Signature Verification Devices

According to the Article 7 of E-signature Law [58];

> *Secure electronic signature verification devices are signature verification devices which;*
>
> *a) Display the data used for verification of the signature to the person who makes verification without any alteration.*
> *b) Manage the signature verification process in a reliable and accurate way, and display the results of verification to the person who makes verification without any alteration.*
> *c) Ensure that signed data is displayed in reliable manner when necessary.*
> *d) Display its results to the person who makes verification without any alteration detecting the authenticity and validity of the electronic certificate used for the verification of the signature in a reliable manner.*
> *e) Display the identity of the signature owner to the person who makes verification without any alteration.*
> f) *Ensure the detection of any alterations that affect the conditions relevant to the verification of the signature.*

4.1.1.10. Time Stamp

According to E-signature Law, time stamp means "The record that is confirmed by certification service provider with electronic signature for the purpose of verification of the exact time for creation, alteration, sending, receiving and/or recording of an electronic data" [54]. Law maker defines the time stamp but it does not include it to the technical subjects which will be regulated by ordinance as stated in the article 20 of Electronic Signature Law. As a result of this the technical aspects of time stamp concept does not regulated by the ordinance. The ordinance includes two definitions related with time stamping which are Time Stamp Policy (Document containing general rules regarding time stamp and time stamping

services) and Time Stamp Practice Statement (Document describing implementation of the issues laid down in the time stamp policy in detail). But these definitions are related with the managerial side of business which is in the obligations of certification service providers.

4.1.1.11. Electronic Certificate

According to E-signature Law, electronic certificate means "Electronic data binding the signature verification data of the signature owner to identity data of that person" [54]. This definition is the same definition which is used in the Electronic Signature Directive and it is defined same in other foreign legal bases. Electronic certificate is used for the verification of signatory's identity by using a trustworthy third party which is certification service provider.

4.1.1.12. Qualified Electronic Certificate

According to the Article 9 of E-signature Law [59];

> *Qualified electronic certificates shall include the followings:*
>
> *a) An indication that the certificate is "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 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.*

4.1.1.13. Secure Electronic Signature

According to the Article 4 of E-signature Law [60];

> *Secure electronic signature;*
>
> *a) is exclusively assigned to the owner of signature.*
> *b) is generated with the secure electronic signature creation device which is kept under sole control of the signature owner.*

c) *enables the identification of the signature owner based on the qualified electronic certificate.*
d) *enables to detect whether signed electronic data is altered or not subsequently.*

The most important property of secure electronic signature is its legal effect. According to law, secure electronic signature shall have the same legal effect with that of handwritten signature. The concepts universal electronic signature or qualified electronic signature can be used as synonyms for the secure electronic signature in the legal base of other countries. The common property of all of them is that they are created by using qualified certificates and secure electronic signature creation devices.

4.1.2. General Evaluation of Electronic Signature Law No: 5070

E-signature Law No: 5070 is harmonious with EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. When EU and other countries in the world are carefully examined it is seen that electronic signature laws are prepared by using a minimalist and neutral principles. Turkish law also appropriates this approach and states it in its memorandum. However the law focuses on public key infrastructure and digital signature and this causes different comments in the public.

These comments constitute a big obstacle in the realization process of targets. However if the law is explained in a proper and scientific way to the public, it will perform a great mission to create additional value which will accelerate e-government and e-trade applications. Turkish Electronic Signature law takes most of the definitions and articles from Electronic Signature Directive 99/93/EC and this is the most powerful property of it. This property also allows using technical and regulation experience of European countries in the preparation period of E-signature Directive.

If this property of law examined carefully, it can be explained in the light of scientific truths why the name of law is “Electronic Signature Law” instead of

“Digital Signature Law” and why it is focusing on public key infrastructure instead of structure neutrality. Some important clues and some explanatory definitions appear in the general memorandum of law and memorandums of articles. However, this situation shelters in some dangers which may lead to misunderstanding or misinterpretation of Turkish Electronic Signature Law.

When combined with the lack of proper, consistent and reasonable applications, the manner of conduct of law on focusing public key infrastructure and digital signatures may lead to contradictory results.

Electronic Signature Directive 99/93/EC which is the source of Turkish Electronic Signature Law aims to clarify basic legal framework and components of this framework about electronic signatures. Directive also clarifies the law politics of European Union and focuses on a predetermined technology which is followed by the other civil countries in the world. This technology is public key infrastructure technology. European Union decided to give legal validity to applications designed over public key infrastructure because of the public opinion and legal risk assessment. In addition to this, European Union defined electronic signature as flexible as possible as a result of technology neutrality. This property aims to allow the development of other applications on the same infrastructure. This definition is the same in Turkish electronic signature law.

Turkish Electronic Signature Law has four important aims. First of them is defining the concepts related with electronic signature and integrating these concepts into legal base. When the law is examined carefully it is clearly seen that nearly each part begins with framework definitions which are related to that part. In addition to this, the law also contains a general “Purpose, Scope and Definitions” part. The main aim of this definitive approach is to help related parties understand the technologically complex concepts. Turkish electronic signature law is a new law that contains unaccustomed concepts like “Secure Electronic Signature”, “Time Stamp” or “Certification Service Providers” and the parties using this law may

misunderstand these concepts which in consequence may lead to misinterpretations of rights and liabilities. As a result of this law maker wants define the concepts clearly to prevent these potential mistakes and concentrates on definitions in Articles 1, 2, 3, 4, 5, 6 and 7.

Second aim of the law is drawing the boundaries of rights and liabilities. This practice mainly focuses on certification service providers but it also includes rights and liabilities of natural and legal persons. Articles 8, 9, 10, 11, 12, 13 of law focus on rights and liabilities of parties. Article 8 defines certification service providers and bases of establishing them. Article 9 defines qualified electronic certificates which are the main components of secure electronic signatures. Article 10 defines liabilities of certification service providers. Article 11 defines the conditions and methods for the revocation of qualified electronic certificates. Article 12 contains rules of protection of privacy while Article 13 contains legal liabilities of parties.

Third aim of the law is defining supervision and penalties. This aim is mainly related with rights and responsibilities of Turkish Telecommunications Authority (TA). Articles 15, 16, 17, 18 and 19 of law focus on supervision and penalties. Article 15 explains the bases of supervision which will be performed by TA. Article 16 defines the penalties related with use of signature creation data without consent. Article 17 defines the penalties related with forgery in electronic certificates. Article 16 and 17 are general articles which can be applied to natural or legal persons or certification service providers. Article 18 focuses on administrative fines which will be applied on certification service providers and finally Article 19 explains what must be done in case of repetition of forbidden actions.

Fourth and the last aim of the law is defining the details which will ease the application of law. One of the related articles with this aim is Article 14. Article 14 is related with Foreign Electronic Certificates and states that electronic certificates issued by any electronic certificate service providers established in a foreign country shall be recognized under international agreements. Articles 20, 21, 22, 23,

24, 25 and 26 of law focus on auxiliary subjects including “Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law”, exemptions and additions to other laws.

4.1.3. Special Characteristics of Law

Turkish Electronic Signature Law has some special characteristics and these characteristics can be classified as below:

4.1.3.1. The Same Legal Effect with That of Handwritten Signature

According to E-signature Law, secure electronic signature shall have the same legal effect with that of handwritten signature. This article is appropriate with Article 5/1 of Directive. In the Article 5/1 of Directive, it is stated that legal effect of electronic signatures which depend on qualified certificates and created by using secure electronic signature creation devices are same with those of handwritten signatures and positive evidence attribute of these signatures shall not be denied [61].

4.1.3.2. Positive Evidence Attribute of Electronic Signature

With the Article 23 of Electronic Signature Law, a new Article which is named 295/A is added to the Article 295 of Turkish Law of Civil Procedure. This article states that [62]:

> *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.*

It is stated that secure electronic signature will be accepted as a positive evidence until the contrary is proved and it can be thought that it limits judge's right to exercise judicial discretion. However most of the countries accept secure electronic

signature as positive evidence which is more reliable than the other positive evidences*.

4.1.4. Legal Operations Which Can Not Be Performed By Using Electronic Signature

According to the second paragraph of Article 5 of Electronic Signature Law, "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" [63]. This article covers the operations made by using notaries, operations which must be performed in front of an official position and etc. (buying or selling real estate and motor vehicles or marriage). Defining these operations in a general manner can create some problems for some operations like assurance contracts which have debatable characteristics [64].

4.1.5. Reflection of Electronic Signature Law No: 5070 on Other Laws

Turkish Electronic Signature Law has some reflections on other laws to provide better integrity and to diminish contradictory interpretations. These reflections are explained in the following sections.

4.1.5.1. Turkish Law of Obligations

Article 22 of Electronic Signature Law adds the following sentence to the Article 14 of Turkish Law of Obligations. "Secure electronic signature has the same conclusiveness with handwritten signature" [65]. As a result of this all of the legal operations except the ones stated in the Article 5 of Electronic Signature Law can be performed by using electronic signature. Article 5 of Electronic Signature Law states that, "Secure electronic signature shall not be applicable to legal proceedings

* For further information about the subject, please look at "Electronic Commerce" at http://www.fipr.org/WhoCarriesRiskOfFraud.htm, Last Accessed October 21, 2005.

subject to a special procedure or an official form pursuant to laws and warranty contracts" [63].

4.1.5.2. Turkish Law of Civil Procedure

Article 23 of Electronic Signature Law adds the following paragraphs to the Article 295 of Turkish Law of Civil Procedure [66]:

> *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.*
>
> *In case any party denies the data generated by secure electronic signatures and alleged against himself, Article 308 of this Law shall be imposed through comparison.*

There is an important point in the second paragraph of this addition. Second paragraph states that Article 308 of same law will be used through comparison if any party denies the data generated by secure electronic signature. However according to Article 295 of the law, the thing which is denied is the data created with secure electronic signature and this data is considered as voucher at the first paragraph of the same article. Article 308 of law regulates denial of signature not denial of a voucher. As a result of this some problems may arise in the application through comparison [67].

4.1.5.3. Turkish Law of Debt Collection and Bankruptcy

Article 68 of Turkish Law of Debt Collection and Bankruptcy regulates the confessed signatures on vouchers [68]. However, neither Electronic Signature Law nor Turkish Law of Debt Collection and Bankruptcy states the presentation way of electronically signed documents to the Court of Debt Collection and Bankruptcy. They also do not contain any articles related with whether Court of Debt Collection and Bankruptcy has an authority to inspect these documents or not. As a result of

this, some problems may arise when it is faced with cases including documents with confessed electronic signatures.

4.1.5.4. Turkish Law of Tax Methods

Article 242 of Turkish Law of Tax Methods states that "Ministry of Finance has an authority to define methods and basis of creation, registration, transmission protection and presentation of books and documents including the ones which are kept in electronic networks" [69]. This article gives authority to Ministry of Finance for the adaptation process of the electronic signature in taxation.

4.1.5.5. Turkish Banking Law

Article 42 of Turkish Banking Law states that [70];

> *The original letters received and activity-related documents, or proper copies where the original ones are not available, as well as the photocopies of letters written shall be kept in order of their number and dates for a period of ten years within the body of the relevant bank. It is possible to keep such documents in the form of micro films or in electronic or magnetic environments. The principles and procedures applicable to the implementation of this article shall be determined by the Board.*

This article gives authority to Banking Regulation and Supervision Agency for the adaptation process of the electronic signature in banking.

4.1.5.6. Turkish Consumer Protection Law

According to the Article 3 of Turkish Consumer Protection Law, property means "Portable goods, real estates used for residence or holiday and electronic data including software, images and similar things prepared for using in electronic environments which are subject to trade" [71]. This article helps the application of electronic signature by integrating electronic data into the definition of property.

In addition to this, Article 9/A of law regulates, “Distant Contracts”. Article 9/A defines “Distant Contracts” as “Contracts which are prepared without facing each other by means of written tools, visual tools, telephone, electronic environments and similar ways” [72]. This article helps the application of electronic signature by creating a legal base to the contracts prepared over internet.

4.2. Other Legal Base

Other legal base related with Electronic Signature Law No: 5070 are categorized in the following sections.

4.2.1. Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law

Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law came into force in 01.06.2005. A small grammatical amendment was made in the ordinance by adding “commitment letter” concept into the ordinance in 04.02.2006. This ordinance covers ten important parts which are related with electronic signature. These parts are explained in the following.

4.2.1.1. General Provisions

This part contains, purpose, scope, base, definitions and principles of ordinance. Especially the principles part contains important points in the application process of electronic signature. These points include important actions like equal treatment, protecting consumer rights, providing service quality, providing effective competition and considering international standards.

4.2.1.2. Announcement Process

This part covers the process of announcement, examination and results of announcement and changes in the announcement.

4.2.1.3. Certification Process

This part covers the certification process. It explains application of qualified electronic certificate including creation, publication, renewing and revoking of it.

4.2.1.4. Liabilities

This part includes the liabilities of three parties. First of them is the liabilities of certification service providers. Second of them is the liabilities of the holders of qualified certificates. Third and the last of them is the liabilities of third parties.

4.2.1.5. Technical Matters and Security

This part contains technical requirements related with signature creation data, signature verification data and security criteria.

4.2.1.6. Financial Matters

This part contains the financial matters including managerial fees and the fees of qualified electronic certificates, time stamps and related services

4.2.1.7. Inspection Methods and Bases

This part contains principles of inspection, rights of inspectors, liabilities of inspectors, liabilities related with the inspection process of electronic certificate service providers, submittals of reports and Telecommunications Board's decisions.

4.2.1.8. End of Activity

This part explains how an electronic certificate service provider shall end its activity and what shall be done after the end. This part also explains what must be done if Telecommunications Authority stops the activities of a certificate service provider.

4.2.1.9. Other Provisions:

This part includes time stamping, acceptance of foreign electronic certificates, activity report responsibility of electronic certificate service providers, communiqué related with technical matters and conditions not covered.

4.2.1.10. Information and Documents Submitted in the Announcements Process

This part defines the information and documents which will be submitted in the announcement process. These include communication details of companies, information related with companies, certification principles, certification application bases, time stamp principles, time stamp application bases, financial responsibility insurance of certificates, copy of contract, copy of commitment letter, service contract and information and documents demanded by ordinance.

4.2.2. Communiqué on Processes and Technical Criteria Regarding Electronic Signatures

Communiqué on Processes and Technical Criteria Regarding Electronic Signature came into force in 01.06.2005. This communiqué covers technical Criteria and processes related with electronic signature as explained in its purpose. The communiqué covers standards to be followed in operating electronic certificate providers, creating qualified certificates, selecting algorithms, defining the length of signature creation and verification data, certification principles, certification application bases, security criteria, time stamping and documentation. As the communiqué defines detailed information about keys and key lengths, it is stated in the Article 6 of it that the length of keys will be valid until 31.12.2005 because of the security needs [73]. Indeed, the communiqué was amended at 21.01.2006 and new key lengths are defined which are valid until 31.12.2008[*].

[*] For further information about the subject, please look at "Resmi Gazate Bilgi Merkezi - Tebliğ" at http://rega.basbakanlik.gov.tr/Eskiler/2006/01/20060121-11.htm, Last Accessed February 5, 2006.

4.2.3. Ordinance on Insurance of Financial Liabilities in Certification

As electronic signature legally binds natural and legal persons as handwritten signature, it is important to cover some financial risks related with it. But the scope of this coverage is not related with the holders of certificates. Instead, it is related with certification service providers. In other words certificate holders are not insured for the financial risks which are created by themselves by using their electronic signature. They are insured for the financial risks which can originate from the actions of certification service providers. Article 5 and Article 6 of Ordinance on Insurance of Financial Liabilities in Certification enlightens the situation by obligating certification service providers to insure the certificates before delivering them to the certificate holders, to cover risks arise from not carrying out their responsibilities stemming from the electronic signature law [74, 75]. This insurance covers assurance of legal responsibilities of certification service providers which are related with using secure products, using secure systems and performing the business in a secure way. This ordinance states that insurance branch, general provisions, tariffs and instructions related with electronic certificates will be defined by Undersecreteriat of Treasury [76].

4.2.4. General Provisions Related with Mandatory Insurance of Financial Liabilities of Certification

General Provisions Related with Mandatory Insurance of Financial Liabilities of Certification covers the subject of insurance, scope of it, duration of it and cases not covered by insurance.

4.2.5. Tariffs and Instructions Related with Insurance of Financial Liabilities in Certification

Tariffs and Instructions Related with Insurance of Financial Liabilities in Certification covers the fees related with insurance and instructions related with insurance.

4.2.6. Circular of Prime Ministry Numbered 2004/21

Circular of Prime Ministry Numbered 2004/21 informs the public institutions about the legal framework related with electronic signatures.

4.2.7. Circular of Prime Ministry Numbered 2006/13

Circular of Prime Ministry numbered 2006/13 informs the public institutions about the developments in legal framework related with electronic signatures.

CHAPTER 5

Economic Analysis of Electronic Signature from Multiple Perspectives

Electronic signature has an economic side in addition to its legal side. In this chapter, macro economic effects of electronic signature on different geographical areas in the world, micro economic effects of electronic signature on governmental and private institutions, and micro economic effects of electronic signature on consumers are presented sequentially.

5.1. Macro Economic Effects

Electronic markets had arisen parallel to traditional markets of goods and services and in the light of new technical advances they reshaped trade transactions in all aspects of business including marketing, production, and payment. Electronic commerce (e-commerce) is seen as the key factor of these new markets. It is expected that global online trade will expand to $12.8 trillion by the end of 2006 [24]. Such a number affects all of the related science branches, especially the economy. The estimations for the size of e-commerce market changes from one study to another but there is a total agreement on the subject that legal problems arise because of the open network structure of internet which is the trade area of the global economy. As a result of this, companies are reluctant to make e-commerce and infrastructure investments. This is because of the fact that no legal framework provides full security for online trade.

Security issues must be solved both domestically and internationally to increase the economic return of e-commerce. Natural and legal persons who are not acquainted with each other will perform buying, selling, leasing, consulting, mediation and etc. via e-commerce. As a result of this, it is very important to provide identification, authentication, and security in electronic networks.

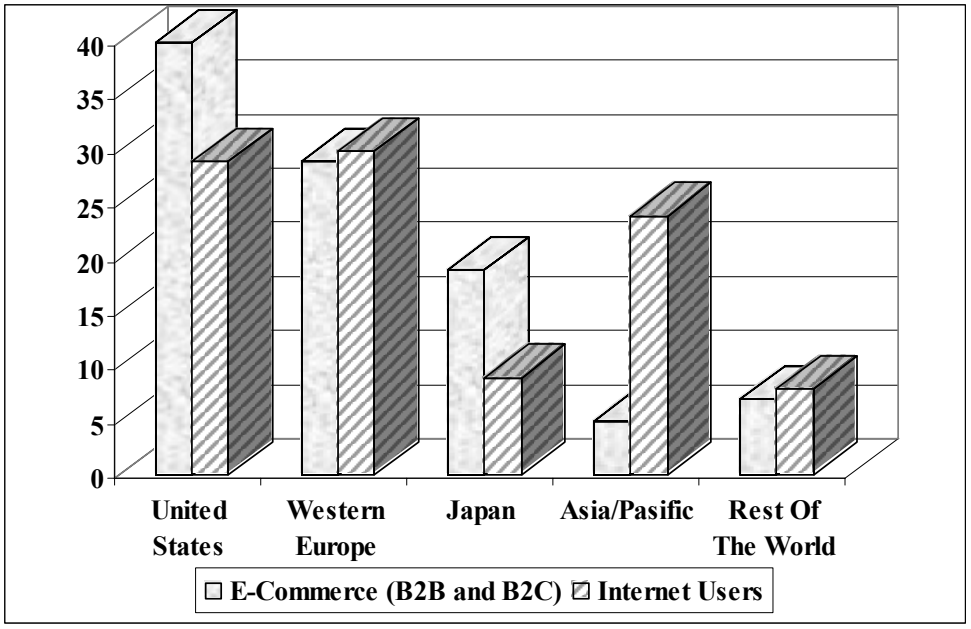
Electronic signature is the trust support and the main infrastructure of electronic commerce and electronic government (e-government) because of the insecure structure of networks, especially the Internet. However, prevalence of electronic signature depends on technological and legal infrastructures which provide security, and efficiency.

When examined globally, it is seen that the level of e-commerce changes from region to region. Figure 6 shows the shares of regions in the global e-commerce business and the Internet penetration in year 2002. This figure shows that United States and Western European countries are the leaders in both internet usage and electronic commerce level. These countries are followed by Japan in the electronic commerce and Asian/Pacific countries in the internet usage. The ratios in United States and Western European countries emphasize a strong positive relation with the level of internet usage and the level of electronic commerce. However the ratios in Japan and Asian/Pacific countries show that this strong positive relation is not the sole factor affecting the countries. There may be some other factors like the cultural perception of people, the scope of legal base or the adequacy of technical infrastructure.

Electronic commerce can be classified into four categories. First one is business to business (B2B), second one is business to consumer (B2C), third one is business to government (B2G), and the last one is government to business (G2B) [78].

B2B e-commerce consists nearly 95% of the total e-commerce [79]. Table 3 shows World E-commerce Revenues and Estimates.

Figure 6: Shares of World Internet Users and E-commerce Revenue (%)



Source: UNCTAD - E-commerce and Development Report 2002 [77]

To understand the importance of the electronic signature, it is important to emphasize that the total revenue gained from all of the products and services globally is $7.43 trillion [77]. According to the forecasts of Forrester Research Company e-commerce will constitute 18% of global trade in 2006 and it is extremely important to provide security and reliability for this huge amount of global transaction.

Table 3: World E-commerce Revenues and Estimates (Billion $)

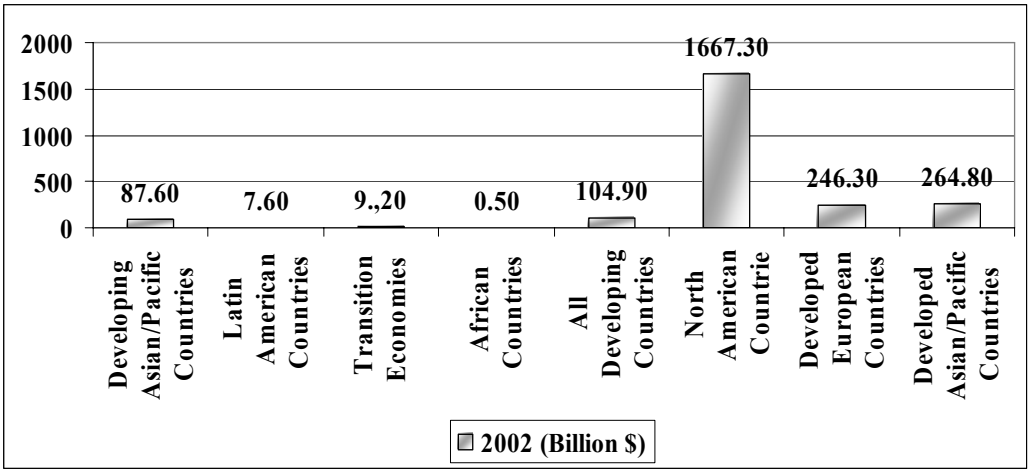
Company	2002	2003*	2004*	2005*	2006*
Forrester	2293.50	3878.80	6201.10	9240.60	12837.30
IDC				4600.00	
eMarketer	823.48	1408.57	2367.47		

Source: UNCTAD - E-commerce and Development Report 2002 [77]

* Estimates

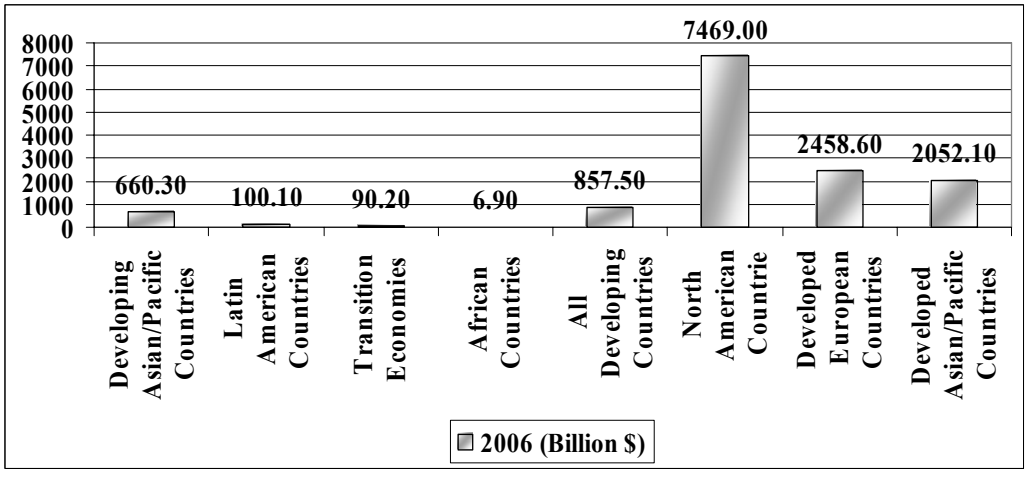
Figures 7 and 8 are drawn to help understanding the regional B2B and B2C e-commerce revenues and estimates more properly. There is correlation between the level of electronic trade and usage of electronic signature. As seen from the Figures 7 and 8, the leading countries in e-commerce area are North American and European countries. As expected, these countries are the initiators of usage of electronic signature (for the dates of electronic signature laws of some countries see Section 3.1).

Figure 7: Regional E-Commerce Revenues of 2002 (Billion $)



Source: Forrester Research - Global Online Trade [24]

Figure 8: Regional E-Commerce Revenue Estimates of 2006 (Billion $)



Source: Forrester Research - Global Online Trade [24]

The general macro economic effects of electronic signature on economy can be derived as:

- Lower expenditures: Expenditures are an important part of an economy. In general it can be said that the lower expenditures, the better economy. Electronic signature will help to diminish total government and private sector expenditures in the economy and this will return to society as an increased welfare in the future.

- Decrease in transaction costs: Transaction costs are the costs incurred in making an economic exchange. Electronic signature diminishes these costs because it makes transactions faster. As a result of this allocation and re-allocation of resources will be faster and this will improve economic efficiency.

- Improved business cycles: Economy gives response to the fluctuations with the speed of its business cycles. Electronic signature will help to improve business cycles and improved business cycles will help economy to be more rapid to changes. This will help governments to cope with inflation and unemployment in addition to increase total economic output.

- Proper use of workforce: Electronic signature will eliminate some human jobs from the economy which are focusing on security of transactions. Some examples of this may include notaries or deeds officials in the future. As a result of this, the workforce focusing on security of transactions may be used in another place more efficiently. This will firstly increase structural unemployment in the short run however it will rise up new employment opportunities in the long run.

- Decrease in electronic burglary: Electronic signature is a very secure system to perform transactions over insecure networks. As it has same legal effects

with that of handwritten signature, it is designed to keep the security as high as possible. As a result of this electronic signature prevents most of the electronic burglaries which are made by using insecure points of technologies. Today financial resources can be transferred from one country to another by a simple click over electronic networks. Securing financial resources by electronic signature will diminish the funds which are transferred to undeserved parties and facilitate more trade which benefits all countries. This in turn will help to balance the internal and external trade in addition to stabilize exchange rates.

- Decrease in speculations. As electronic signature legally binds the identity information of people with their signing function, it limits the speculations which can be performed by anonymous internal and external parties. This will help to stabilize expectations in the economy which in turn help to apply governmental policies more effectively.

- Preventing black market economy: Connecting electronic signature infrastructure with proper financial systems including banking, taxation customs and etc. will help the government to control the flow of total income and total expenditure which will be very beneficial to prevent the black market economy depending on uncontrolled leakages and injections. This will increase the total tax revenue which in turn will help to improve the budget.

- Increasing efficiency and effectiveness: With the widespread use of electronic signature, the efficiency and effectiveness in the economic processes will increase and this will help to obtain more proper results from fiscal and monetary policies. In other words, economic policies can be applied effectively and the results of them will be obtained more efficiently.

5.2. Micro Economic Effects

While the usage of electronic signature affects macro economy it also effects institutions and consumers in a micro perspective.

5.2.1. Micro Economic Effects on Institutions

As an estimation, nearly 90% of institutions work with paper documents today and the number of misallocated documents can not be ignored. These misallocated documents probably can not be found when needed and users loose minimally 8 hours for the document processes in a week on an average [80]. In addition to this, there are many copies of documents and users' efforts on document management are doubled or perhaps tripled because of this factor. These losses increase when the governmental institutions are inspected. As a result of this, electronic signature provides great amount of savings on efficiency and time.

With the secure infrastructure of electronic signature, security of information and documents can be guaranteed and there will be no need for additional physical procedures focusing on security concept. In addition to this, electronic signature will bring space savings as the documents are kept in electronic networks in a secure way.

In conclusion document management will be more effective when compared with the one performed in paper environment. Efficiency will increase when time, space and paper savings are achieved.

The general micro economic effects of electronic signature on private and governmental institutions can be derived as:

- Decrease in documentation costs: Electronic signature does not require paper. As a result of this, it will bring great savings on paper based

businesses. In addition to this, mistakes made on documents can be corrected in the digital media so it prevents additional costs generated from these types of documents. This will help to achieve economies of scale in documentation and achieving economies of scale in documentation means allocating scarce resources to the other areas more efficiently.

- Decrease in managerial costs: As electronic signature brings the ability to operate reciprocally inside and between institutions in a secure way and as it legally binds the identity information of people with their signing function, it helps to decrease the costs that arise from managerial monitoring activities.

- Decrease variable costs: If electronic signature is used, the need for physical transportation of documents from one institution to another will disappear. Documents will be transported via electronic networks under the custody of parties and this will reduce the time of transportation and speed up the processes. This increase in the speed of business processes will help to decrease variable costs which are affected by transaction costs in the production stage and decrease in variable costs means lower prices and more competitive markets.

- Decrease in fixed costs: There is a sunk cost related with the establishment of electronic signature infrastructure and it can be thought that establishing this infrastructure brings additional fixed costs to the institutions in the short run. However this infrastructure removes storage, maintenance and security costs related with the documents. As a result of this the total effect of electronic signature on fixed costs remains in a decreasing manner in the long run. Decrease in fixed costs also means lower prices and more competitive markets.

5.2.2. Micro Economic Effects on Consumers

Electronic signature also affects the consumers in the micro perspective. As the main aim of the technology is to accelerate the electronic business processes which are performed over online environments, especially over the Internet in a secure way, it helps to increase usage level of information technologies by providing secure solutions. People who do not use information technologies are always confronted with some costs which arise from not using the technology. These costs include actual costs and risk based costs. The total of all these costs is called by some researchers as cost of misinformatics. Cost of misinformatics can be defined as "Sum of direct and indirect costs originating from not using information technologies or using them in an inefficient and ineffective way" [81].

To analyze the subject from this perspective let us think two cases one of which depends on performing banking operations manually while the other depends on performing banking operations online by using electronic signatures. An important point to consider here is integrating electronic signature concept into the online banking application. Personal and institutional online banking without using electronic signature have already been performed for a couple of years in the world. However the risks associated with this kind of online banking are always high as the main infrastructure used for transactions is an insecure one which is the Internet. Electronic signature provides a very secure communication opportunity in the insecure networks like the Internet. As a result of this, it is used to eliminate risk based costs arising from security vulnerabilities as much as possible.

Think of a case that a person for instance Bob wants to transfer a huge amount of money from his bank account to another bank account for instance Alice's bank account with the aim of performing business. Let us assume that, this business is buying or leasing a real estate. If Bob wants to perform this operation manually, he will pass through some steps like going to bank, drawing the money, transferring the money to Alice's bank and depositing the money to the account of Alice. On the

other hand if Bob performs the banking operation online by using a secure electronic signature he will pass through some steps like switching on his computer, connecting to bank's website, preparing the order of payment, signing it with his electronic signature and approving the transfer.

The most important question when analyzing these two cases is "Which case creates more cost on Bob?" The answer to this question leads us to the concept of opportunity cost.[*] Bob spends more time when he performs the banking operation manually and this extra time has a cost. If all the other conditions are same, we can say it is less costly for Bob to perform banking operation online by using electronic signature instead of performing it manually because of the opportunity cost. This expression is not sufficient to obtain a definite result as it is impossible to calculate and stabilize all the other variables affecting the cases. As a result of this, we shall prepare some assumptions to clarify this expression. These basic assumptions for both cases are stated below:

- Bob knows how to perform banking operation manually and online: If we don't use this assumption it can be claimed that Bob has costs like learning how to fill the documents, how to use computer, how to use the Internet or how to use electronic signature.

- Bob has suitable infrastructure to perform banking operation manually and online: If we don't use this assumption it can be claimed that Bob has costs like buying a secure bag to transport money, buying a computer to perform online banking, subscribing to an internet service provider for the Internet service or obtaining electronic signature.

- In both of the cases Bob's income is same, Bob is responsive to costs at the same level and he perceives costs as an important piece of operation. If we

[*] For further information about the subject, please look at "Opportunity Cost" at http://www.econ.iastate.edu/classes/econ301/Bunzel/documents/Education.pdf, Last Accessed February 9, 2005.

don't use this assumption it can be claimed that Bob's income or perceptions may lead to biased results.

- The comparison is performed only on opportunity cost and other costs are not included in the analysis.

Under these assumptions we can generalize our expression as using information technologies is more cost effective than not using them for consumers ceteris paribus*.

This cost effectiveness increases the demand of consumers to the products and services. Increased demand forces institutions to produce more goods and services and achieving economies of scale. As the number of institutions achieving economies of scale increases the competition increases and increased competition means products and services with less prices and more quality.

If we do not consider these assumptions, we will be faced with two important questions one which are "Is it profitable to obtain electronic signature which has a cost of nearly 200 YTL?" and the other is "What will be the cost of teaching to use electronic signature to the society and who will incur it?" Obviously, the answer to the second question depends on the governmental policies which aim to increase the educational level of society. At first sight it seems it is a very costly processes but the cost is incurred by government with the aim of increasing the quality of human

* Ceteris paribus is a Latin phrase, literally translated as "with other things [being] the same," and usually rendered in English as "all other things being equal." A prediction, or a statement about causal or logical connections between two states of affairs, is qualified by ceteris paribus in order to acknowledge, and to rule out, the possibility of other factors which could override the relationship between the antecedent and the consequent.

A ceteris paribus assumption is often essential in all predictive sciences - in order to evaluate scientific laws it is usually necessary to rule out some unspecified set of relevant factors which could interfere with the effect of some causal factor. Experimentally, the ceteris paribus assumption is realized when a scientist controls for all of the independent variables other than the one under study, so that the effect of a single independent variable on the dependent variable can be separated out. By holding all the other relevant factors constant, a scientist is able to focus on the unique effects of a given factor in a complex causal situation. [82]

capital and increased quality of human capital means lower costs and efficient business processes in the future.

The answer to first question is a debatable one. When examined carefully it is seen that the price of obtaining electronic signature is nearly the same in the World (See section 3.1.1). As a result of this, it may be claimed that obtaining electronic signature is not expensive in Turkey. However the economic conditions of countries are different from each other and Turkey seems not so bright in this perspective. As a result of this, the price of obtaining electronic signature remains very high in Turkey when compared with different economies and this limits the diffusion rate of technology. To overcome this problem, the local parties in the electronic signature business including the certification service providers and infrastructure providers shall be supported in the short run and the economy shall be strengthened in the long run.

CHAPTER 6

Awareness Level of Electronic Signature in Turkey

In biological psychology, awareness describes a human or animal's perception and cognitive reaction to a condition or event. Awareness is an ability to be conscious of, feel or perceive something. [84] This chapter focuses on awareness level of electronic signature in Turkey. The chapter starts with the importance of subject and continues with two analyses one of which reviews the institutional awareness level while the other reviews the personal one. The chapter ends with the reflection of awareness level on the practical implementation of subject. Analyses performed in this chapter are not based on any predefined statistical techniques. They are wholly created by analytical thinking and logical inferences. As a result of this statistical reliability of the calculations are not certain. They are only projected logical results of the study to the calculations which are made by other studies. In literature there are some methods like verbal reports, subjective tests, forced-choice tests, objective tests, behavioral methods, physiological methods and imaging methods to calculate the awareness level. [85] Although the design of the questionnaire which aims to measure awareness level of people resembles forced-choice tests which require subjects to judge some sequences, it is not designed by any method related with forced-choice tests. In this study we define awareness levels of people as percentages. The percentages calculated show the ratio of people in the society who are aware of their legal responsibilities related with electronic signature. The awareness levels of institutions are not determined as percentages; instead general evaluations are made using the data obtained from another study which is performed by Telecommunications Authority of Turkey.

6.1. Importance of Awareness Level: A Social View

The most important social problem of information era is “digital divide” which means the perceived growing gap between those who have access to and the skills to use Information and Communication Technologies (ICT) and those who, for socio-economic and/or geographical reasons, have limited or no access [86].

United Nations Development Program (UNDP) states in its Human Development Reports that there is a new kind of poverty named “information poverty” because of the increasing gap between the ones who have ability to access opportunities of the information and communication technologies and the ones who do not have. United Nations states that the differences in the information area between developed, developing and underdeveloped countries increase day by day. This view is also stated by other organizations like G8 and OECD; however the main problem is how the cost will be paid to cover the differences [86]. Electronic signature is not a solution to the information poverty problem, but if the accessibility of electronic signature increases it may help to lower the gap by making it easier to conduct online transactions. Governments’ policies to cover some parts of costs which are associated with digitally divided last users will be helpful to balance the social structure.

In addition to digital divide problem, another important problem of information era is information overflow faced by the parties which have a chance to access information. These parties including natural and legal persons are faced with information bombardment. Information shall be used for the benefit, wealth and happiness of people; however fast improvements in the information technology combined with legal and technical inadequacy brings opposite effects like electronic forgery, vandalism, obscenity, and attacks to private life. These crimes are taking on a shape on the information infrastructure. Uncontrolled flow of each type of text, picture, data and information; the inadequacy in the usage of prevention mechanisms; and the lack of dissuasive laws and regulations create serious social

problems among the members of society who have access to information infrastructure. It is not possible to say that, people are accessing true and beneficial information. This is because of the fact that people are facing information contamination. Electronic signature can reduce electronic crimes and information overflow because of the security, reliability, and non-repudiation it brings.

The most important inheritance to the future society is clean information sources. As the information is a strategic source and the basic value of information society, it is mandatory to keep this source in a clean and effective manner. As a result of this, electronic signature can be named as the powerful guardian of information society. Technology brings new methods, new energy sources, new production methods, new powers and all these lead to rapid and deep changes on the foundations of the society. If these rapid and deep changes can not be managed effectively their negative effects can overweigh their positive effects. Technological changes can be beneficial if they are integrated to the values of social life. The most important result of a proper integration is shaping the structure of the society towards a more mature civilization.

In the economic systems of today, information is a key input in addition to the traditional factors of production. If this factor can be merged into the traditional factors effectively, all of them create a synergy which leads to new type of jobs, new type of workers, new type of laws and new type of economy which in turn help to create a more developed country. According to Castells “The power wars of information are cultural wars. Power as the source of capital and culture as the source of power creates the social hierarchy of information era” [87].

On the other hand, with the diffusion of information technologies to the social layers of society, democracies will be more participative. This is because of the fact that individuals will find more opportunities to convey their ideas and thoughts to other individuals in the society in a fast and secure way. Today’s prototype concepts like e-government, e-election and e-democracy will be the future ways of governing

the society. As a result of this, it is clearly seen that holders of the information sources will be the most powerful ones of the future. Understanding e-signature concept clearly can be an important step towards a powerful information society.

6.2. Institutional Awareness Level in Turkey

In June 2004, Telecommunications Authority of Turkey performed an institutional survey with the aim of providing information for The Infrastructure Working Group of Electronic Signature National Coordination Committee to determine the expectations of governmental institutions from the electronic signature concept. The survey is carried on eighteen governmental institutions including the Ministry of Justice, Ministry of Finance, Turkish Notary Union, Turkish State Meteorological Service, State Statistics Institute, The Pension Fund for Civil Servants, Capital Markets Board of Turkey, Central Bank of Turkey, Undersecreteriat of The Prime Ministry for Foreign Trade, Undersecreteriat of Maritime, Turkish Republic State Railways, Turkish Standardization Institute, Turkish Cooperation and Development Administration, Undersecreteriat of Customs, Public Registration Office, The Scientific & Technological Research Council of Turkey (TÜBİTAK) - Information Technologies and Electronics Research Institute (BİLTEN), Ankara Metropolitan Municipality and İstanbul Metropolitan Municipality by the experts of Telecommunications Authority. The surveys are filled by IT departments, law departments and related managers of institutions. The results obtained from this survey can be found in Appendix C [88].

According to the results of this survey, it is clearly seen that, some governmental institutions in Turkey have not adapted electronic signature to their work processes yet. Another important result of survey shows that governmental institutions which adapted electronic signature to their processes mainly use electronic signature for their security needs inside their institutions instead of performing institution to institution, institution to citizen or citizen to institution operations. This limits the speed of penetration of electronic signature in the country. However this negative

effect is balanced with the willingness of institutions to adopt electronic signatures. All of the governmental institutions which attend the survey, state that they are currently using electronic signature or they plan to use it at most in 24 months and this is a positive factor which increase the expectations on electronic signature penetration.

This survey also points out possible interoperability problems. The governmental institutions prefer different infrastructures to use with electronic signature. Some of them prefer to use soft digital certificates while some others prefer to use smartcards or USB tokens. In addition to this, some of them use foreign PKI software while others use local ones developed by Turkish Institutions. These two main groups also have other subgroups. For instance the choices of foreign software include VeriSign CA, GlobalSign CA and Microsoft CA. On the other hand, the choices of local software include TÜBİTAK - BİLTEN - ZEUGMA and TÜBİTAK - UEKAE - ASYA. In the short run, these preferences may not create problems on the processes performed inside institutions; however, when the integration of e-government requires governmental institutions to communicate with each other they may create additional burden on the government to standardize the processes.

The survey results show that, each institution targets a closed subset of related institutions in the integration processes according to its functions. At first sight, integrating the systems to related institutions by using electronic signature seems as a good starting step. However, full integration to e-government is not stated in the answers of institutions although full integration is very important to harmonize the governmental processes to gain efficiency and effectiveness from the technology. Most of the institutions state that they will adapt their software to the new technology and neither of them states that they will change their technology in a standard way which is harmonious with other ones.

Another important result of the survey is the unsatisfactory answers to the questions related with continuity, method of use, and up-to-dateness of systems. Nearly none

of the institutions have an idea about how to provide these important requirements. In addition to this most of the institutions can not determine the number of inside and outside users who will use their electronic networks via electronic signature. The numbers range from 50 to unlimited and this limits capacity planning.

As the survey gathers general information about electronic signature from governmental institutions, it will be more suitable to infer a general awareness level instead of relying on percentages. For the awareness level of electronic signature, perhaps the most significant and most important answers are the answers to questions 13, 14, 15, 16 and 17 because these questions are examining the type of users and the institutional processes related with the electronic signature. The answers emphasize confidentiality and authentication more than the other functions of electronic signature. Focusing on authentication is beneficial but not sufficient. Neither of the institutions underlines integrity or non-repudiation functions. On the other hand, it seems that they are focusing on confidentiality more than needed. Although the confidentiality is one of the functions of electronic signature, it is not necessary to sustain confidentiality by using mechanisms provided by electronic signature. At this point there is a great confusion. Most of the governmental institutions think that they will sustain confidentiality by using electronic signatures; however, the main aim of electronic signature shall be sustaining security and reliability which are basic components of trust relationships. As a result of this, we can infer from the information at our hand that most of the governmental institutions misunderstand the electronic signature subject. This points out to a low level of institutional awareness level. This proposition about the low level of awareness can be supported with the answers to the last two questions of the survey. These two questions examine the purposes of using electronic signature and problems faced with when integrating it to the real life. These parts state that infrastructure and know-how is not sufficient for integrating electronic signature to the current governmental system and this insufficiency becomes more complex as the human resources and other resources of institutions differ from each other.

6.3. Awareness Level of People in Turkey

For determining the awareness level of people, we designed a 19 questions survey which aims to gather data like the Internet usage habits, incomes, ages and jobs of participants. We applied the survey both offline and online for a period of 4 months. The main aim of applying both online and offline surveys is to reach maximum participants as much as possible. The total number of completed surveys was 1014. These 1014 surveys were gathered in the same database and were reviewed with the aim of eliminating empty and erroneous ones. The final number was 907, which means we eliminated 107 participants because of inconsistencies and no answers. When analyzed, it was seen that 441 of them were completed offline while 465 of them were completed online.

In the offline surveys 9 big cities were selected to cover the whole country and at least 20 surveys were sent to each of them. These cities were Ankara, Antalya, Erzurum, Gaziantep, İstanbul, İzmir, Konya, Trabzon and Zonguldak and each of them is the biggest city in its geographical region. These surveys are performed by students who are advised to gather data from different parts of cities as random as possible with the aim of obtaining heterogeneity. The survey uses cluster sampling method* accepting the cities as clusters. The survey was gathered data from nearly 70 cities in total and it can be found in Appendix D. The question by question results of survey can be found in Appendix E.

The answers given to the first six questions of the survey shows that 600 out of 907 participants use the Internet which consists 66.2% of the total sample and 307 out of 907 participants do not use the Internet which consists the remaining 33.8% part. These 600 people mostly connect to the Internet from their homes and their workplaces with the ratios of 32.8% and 30.0% respectively, and 32.2% of them connect to the Internet between 10 hours and 30 hours in a week. Another important

* For further information about the subject, please look at "Cluster Sampling" at http://en.wikipedia.org/wiki/Cluster_sampling, Last Accessed October 21, 2005.

result gathered from this part is that more than half of the participants use online banking and trade services in addition to online governmental services but they are mostly indecisive about the level of security for the operations performed over internet.

The answers given to the seventh question, show that 308 out of 907 have heard the electronic signature concept while the remaining 599 did not. This question provides simple statistical information when evaluated alone. However it gives us an important result when it is evaluated along with the first question. If we search for a correlation between answers of "No" to the first question and answers of "No" to the seventh question, we obtain the table below:

Table 4: Relation of Question 1 and Question 7

		Answers of "No" to Question 1	Answers of "No" to Question 7
Question 1	Pearson Correlation	1	1
	N	307	307
Question 7	Pearson Correlation	1	1
	N	307	307

** Correlation is perfect at the 0.01 level (2-tailed).

This table shows us that there is a perfect correlation between answers of "No" to the first question and answers of "No" to the seventh question. This means that neither of 307 people who do not connect to the Internet heard electronic signature concept. In other words, in our survey, people who do not connect to the Internet also did not hear anything about the electronic signature concept. In bigger samples, there may be participants who do not connect the Internet but heard the electronic signature concept. However we will eliminate this group from our analyses by generalizing this result to the whole country and state that "People who do not use the Internet in Turkey have most probably not heard electronic signature concept".

The answers given to the questions 8, 9, 10, 11 and 12 show that only 30 of 308 people who heard electronic signature have electronic certificates which consists 9.7% of heard ones and 3.3% of the total sample. 10 of these 30 people state that they obtained their electronic certificates from foreign firms over internet with the aim of trying, one of them states that he/she obtained the certificate personally without using the Internet and another one states that he/she developed it for him/herself. The remaining 18, state that their certificates are given from the institutes or the universities in which they work. This means most of the people obtain electronic certificates without demanding it. It is an important clue for the diffusion rate of electronic signature which shows that electronic signature is in the early stages of adaptation. The most important tool for using electronic signature is soft certificate and it is followed by smartcard, USB token is the third with a ratio of 20%. People use electronic signature mostly for electronic mail and for the operations performed inside their institution or university. The ratio of using it in online banking and trade is 16.7% while the ratio of using it in official works is 13.3%. When this result is evaluated, where of 9 out of 30 participants have qualified electronic certificate, it is clearly seen that people do not use their electronic signature in an interoperable manner. There are two sources of this problem. First one is the lack of awareness level and the other one is the inadequacy of the infrastructure.

Thirteenth question is designed as containing 20 true-false sub-questions which aim to analyze the awareness level of people who heard the electronic signature concept. These 20 sub-questions are designed by considering the legal prerequisites and experiences of certification service providers. The main of selecting number 20 for the true-false questions is not to depress participants with a lot of questions. These questions are designed as simple as possible to eliminate potential misunderstandings. The answers given to the sub-questions show that on the average, only 5.83 out of 20 are answered correctly by 308 people who heard electronic signature concept. This constitutes a ratio of 29.15%. The average number of wrong answers is 3.25 and this constitutes a ratio of 16.25%. It is a good

result to see that correct answers are more than incorrect ones. However the most important result obtained from question 13 is the remaining part which determines the number of unknown questions. On the average 10.92 of 20 true-false questions are answered as "Not Known". This means that, people don't know 51.6% of 20 sub-questions which are designed considering the legal responsibilities of electronic signature owners. The standard deviation of correct answers is 4.022 which means most of the correct answers fall between a range of 1 to 10 questions while standard deviation of incorrect ones is 2.6 which means most of the incorrect answers fall between a rage of 0 to 6 questions. The value of standard deviation for unknown answers is 5.46. An interesting result that can be obtained from this question is that maximum number of correct answers is 20 while the maximum number of incorrect ones is 12. This shows us that most of the people who are not confident about their answers choose "Not Known" option instead of answering the questions.

Question 14 is designed to measure the beliefs of people about the security level of electronic signature. This question is similar to question 7 which is designed to measure the beliefs of people about the security level of the Internet. When analyzed from a unified perspective it is seen that not only the questions but also the results are very similar to each other. Most of the people answering question 14 are indecisive about the security of electronic signature like the ones that are answering question 7. If we look at the correlation between answers to 7 and answers to 14 for 308 participants who heard about electronic signature we obtain Table 5.

Table 5: Relation of Question 7 and Question 14 for 308 People Who Heard Electronic Signature Concept

		Answers to Question 7	Answers to Question 14
Question 7	Pearson Correlation	1	0.249(**)
	N	308	308
Question 14	Pearson Correlation	0.249(**)	1
	N	308	308

** Correlation is significant at the 0.01 level (2-tailed).

The correlation between answers to the seventh and the fourteenth questions is a significantly positive one. We can infer from this table that people who heard about electronic signature answered both questions in a similar way.

Question 15 gathers data about the ages of participants while question 16 gathers data about the gender of participants. The average of ages is 33.68 while the standard deviation of it 10.974 for the whole population. The oldest participant of survey is 79 years old while the youngest one is 18 years old and our survey covers 583 males and 324 females.

At this point correlation between answers to question 13 and question 15 can be analyzed to infer some results about age - awareness level relation. Table 6 shows that there is significant negative correlation between the age and awareness level for the whole population.

Table 6: Relation of Question 13 and Question 15 for 907 People Who Attended to the Survey

		Correct Answers to Question 13	Answers to Question 15
Question 13	Pearson Correlation	1	-.0117(**)
	N	907	907
Question 15	Pearson Correlation	-0.117(**)	1
	N	907	907

** Correlation is significant at the 0.01 level (2-tailed).

This means that awareness level of people decreases as their ages increase.

Another analysis depends on the correlation between answers to question 13 and question 16 which aim to infer some results about awareness level - gender relation. Table 7 shows that there is not a significant correlation between the gender and awareness level for the whole population. This means that awareness level is not related to gender.

Table 7: Relation of Question 13 and Question 16 for 907 People Who Attended to the Survey

		Correct Answers to Question 13	Answers to Question 15
Question 13	Pearson Correlation	1	-0.0003(**)
	N	907	907
Question 16	Pearson Correlation	-0.0003(**)	1
	N	907	907

** Correlation is not significant at the 0.01 level (2-tailed).

Questions 17, 18 and 19, aim to measure income, occupation and residence data. It is seen clearly from the results that the incomes of participants are mostly between 1000 and 2000 YTL and most of them are government officials. Our survey spans nearly 70 cities.

Perhaps the most important result which can be gathered from the answers to these questions is that there is a significant positive correlation between the income level and awareness level for 308 people who heard electronic signature. This correlation can be found in Table 8.

Table 8: Relation of Question 13 and Question 17 for 308 People Who Heard Electronic Signature Concept

		Correct Answers to Question 13	Answers to Question 17
Question 13	Pearson Correlation	1	0.234(**)
	N	907	907
Question 15	Pearson Correlation	0.234(**)	1
	N	308	308

** Correlation is significant at the 0.01 level (2-tailed).

This means that awareness level of people increase when the incomes of them increase.

The questions focusing on occupation and residence data are not evaluated in the analyses. They are put into the survey with aim of checking the level of intended heterogeneity. However, any further research on the area may use the answers to these questions to analyze the relation between the awareness level and occupation or residence data.

So far we evaluated the results and correlations between results in our survey. But the question is "What is awareness level of people about electronic signature in Turkey" and "How will it be calculated?" In the following we have developed a model to compute the awareness level of electronic signature in Turkey.

In the evaluation of answers to questions we found a perfect correlation between answers of "No" to the first question and answers of "No" to the seventh question and stated that people who do not connect to the internet also did not hear anything about the electronic signature concept in our survey. In addition to this we generalized this result to the whole country and state that "People who do not use the Internet in Turkey most probably did not hear electronic signature concept". If we stay loyal to this generalization, we can eliminate the ones who do not use the Internet from our awareness level analysis and calculate the awareness level in the country by projecting our analysis to other analyses which define the Internet usage level of the country. The most important and the recent analysis about the Internet usage levels in Turkey, is made by State Statistical Institute at the end of 2005. This is a survey named "Household Information Technology Usage Research". According to this survey internet usage level is 23.06% in urban areas while 8.19% in rural ones and urban areas consists nearly 62.9% of Turkey while the rural ones consists 37.1% of it [89]. If we can find the awareness level of our participants who use the Internet in our survey, we can project our results to the whole country over the statistics of State Statistics Institute by using this information and our generalization together. In our survey, the ratio of internet users who heard electronic signature is:

Equation 1: The Ratio of Internet Users Who Heard Electronic Signature

$$308/600 = 0.513333333$$

These 308 people answered our 20 sub-questions located under the question 13 and they give 5.831168831 correct answers on the average as we calculated in our analyses stated above. In the light of this result, the ratio of correct answers in the sub-questions of question 13 can be calculated as:

Equation 2: The Ratio of Correct Answers in the Sub-Questions of Question 13

$$5.831168831/20 = 0.291558441$$

The awareness level of 600 internet users can be calculated as:

Equation 3: The Awareness Level of 600 Internet Users

$$0.513333333 * 0.291558441 = 0.149666666$$

If we project this result to the results of "Household Information Technology Usage Research", we can calculate the awareness level in Turkey as below:

Equation 4: The Projected Awareness Level of Electronic Signature in Turkey

The Projected Awareness Level of Electronic Signature in Urban Areas of Turkey

$$0.149666666 * 23.06\% \approx 3.45\%$$

+

The Projected Awareness Level of Electronic Signature in Rural Areas of Turkey

$$0.149666666 * 8.19\% \approx 1.23\%$$

=

$$\mathbf{(3.45\% * 0.629) + (1.23\% * 0.371) \approx 2.63\%}$$

It can be seen from above calculations that the awareness level of electronic signature in Turkey is 2.63%. However this result is not definite result. This result is only the combination of the results of "Household Information Technology Usage Research" and our survey. Our survey contains nearly all cities in Turkey with each type of job and income. In other words our survey provides the needed heterogeneity to measure the awareness level of country. In addition to this, the numbers of our offline and online surveys are nearly equal to each other and means, medians, modes and standard deviations of our answers are logical and balanced. In total, all our results depending on this structure do not show any inconsistency.

6.4. Reflection of Awareness on Practical Implementations

According to the electronic government study performed by Taylor Nelson Sofres in 27 countries in 2004, Turkey appeared in the last three countries with Indonesia and Russia. The study showed that, on the average the usage ratio of electronic government in those 27 countries was 26% while the ratio in Turkey was only 3% in 2004. The results of this study can be found in Table 9 [90].

Table 9: Usage Ratios of Electronic Government

Usage of Electronic Government		
High	**Medium**	**Low**
Norway (53%)	Estonia (25%)	England (11%)
Denmark (47%)	India (22%)	Malaysia (11%)
Canada (46%)	France (18%)	Latvia (8%)
Finland (45%)	Hungary (18%)	Slovakia (8%)
USA (34%)	Spain (17%)	Lithuania (5%)
Hong Kong (31%)	Czech Rep. (17%)	Poland (5%)
Australia (31%)	Germany (17%)	**Turkey (3%)**
Holland (31%)	South Korea (17%)	Indonesia (3%)
Taiwan (26%)	Japan (16%)	Russia (3%)

Source: Taylor Nelson Sofres [90]

Today, this ratio can be calculated by using the same approach we have used in the awareness level. It is obvious that people who do not connect to the Internet also do not use electronic government as the Internet is the primary tool needed to use electronic government. As a result of this, our 307 participants who do not connect to the Internet shall be eliminated from our analyses. The projection of remaining 600 participants can be used to estimate the usage ratio of electronic government. By combining the data gathered from Household Information Technology Usage Research of State Statistical Institute with the data gathered from the answers to question 5 of Survey on the Awareness Level of Electronic Signature the usage ratio of electronic government in Turkey can be calculated as:

Equation 5: The Usage Ratio of Electronic Government in Turkey

$$[(23.06\%) * (0.629) + (8.19\%) * (0.371)] * 337 / 600 \approx 9.85\%$$

By using this information, the usage ratios in urban and rural areas can also be calculated as:

Equation 6: The Usage Ratio of Electronic Government in Urban Areas of Turkey

$$(23.06\%) * 337 / 600 \approx 12.95\%$$

Equation 7: The Usage Ratio of Electronic Government in Rural Areas of Turkey

$$(8.19\%) * 337 / 600 \approx 4.6\%$$

With the same approach we used in usage ratio of electronic government we can also calculate the usage ratios of online banking and trade by combining the data gathered from Household Information Technology Usage Research of State Statistical Institute with the data gathered from the answers to question 4 instead of question 5.

Equation 8: The Usage Ratio of Online Banking and Trade in Turkey

$$[(23.06\%) * (0.629) + (8.19\%) * (0.371)] * 385 / 600 \approx 11.26\%$$

By using this information, the usage ratios in urban and rural areas can be calculated as:

Equation 9: The Usage Ratio of Online Banking and Trade in Urban Areas of Turkey

$$(23.06\%) * 385 / 600 \approx 14.80\%$$

Equation 10: The Usage Ratio of Online Banking and Trade in Rural Areas of Turkey

$$(8.19\%) * 385 / 600 \approx 5.26\%$$

Our results show that the usage ratio of electronic government is multiplied by more then three times which accounts to nearly 9.85% within two years. When this ratio examined with the ratio of using online banking and online trade which is nearly 11.26%, it is seen that Turkey performed an accelerated increase in integrating information technologies to governmental and business related processes. Although this accelerated increase is an important step for full integration, it is not sufficient alone because the ratios of today are still below the world averages of 2004. To overcome this problem and to accelerate the integration, all the steps shall be taken in a coordinated manner. In other words if an effective full integration is wanted all the perspectives of electronic signature including technical, legal and economic sides shall be considered together.

CHAPTER 7

Conclusion and Future Work

In conclusion, the results obtained from our analyses in preceding chapters can be summarized as below:

On the technical side of electronic signature, there is no problem for the governmental and private institutions which are not using electronic signature currently because all the standards and related institutions are defined very clearly and they can integrate information technologies to their processes simply by accepting predefined rules. This kind of a practice will help to prevent unnecessary potential costs and interoperability problems. On the other hand there are three problems related with governmental and private institutions which are using electronic signature currently. First of them is the potential sunk cost problem which means the costs associated with establishing, using and maintaining systems which are not appropriate with current standards. Second is the adaptation cost problem which means the cost which must be incurred to adapt the non-standard systems to the standard ones. Third and the last of them is the interoperability problem which means adapting business processes to the other institutions' processes using electronic signature. To overcome these problems, both the government and the private sector are continuing to adapt their infrastructure to the standardized electronic processes. On the government side The National Research Institute of Electronics and Cryptology (UEKAE) which is a subsidiary of The Scientific & Technological Research Council of Turkey (TÜBİTAK) is assigned responsible for meeting the certification needs of governmental institutions while in

the private sector side two certification service providers are authorized to meet the certification needs of non-governmental natural or legal persons.

The legal side of electronic signature seems containing fewer problems then the technical side at first sight because legal base including Electronic Signature Law, The Ordinance on the Procedures and Principles Pertaining to the Implementation of Electronic Signature Law and Communiqué on Processes and Technical Criteria Regarding Electronic Signatures are prepared fully compatible with European Union's Directives and Regulations. However there is an important point in the discussion that fully compatible does not mean covering all the required provisions. The legal base contains some ambiguous issues which can be interpreted differently by different parties. In addition to this, there are some uncovered important issues like the lack of giving a right to legal persons, especially certification service providers to obtain electronic certificates and these uncovered issues may create additional problems when the number of practices increases. The reflection of legal base of electronic signature to the other legal bases including the laws like Turkish Law of Obligations or Turkish Law of Civil Procedure is also insufficient and contains ambiguous provisions too. As the electronic signature concept is an evolving concept which creates new standards and applications day by day. The gaps in the legal base shall be closed as fast as possible while the ambiguities shall be clarified to provide wider application of the subject.

Economic side of electronic signature seems having some problems in the short run arising from facing with increased unemployment or high infrastructure costs. However, it is clearly understandable from our analyses in Chapter 5 that performing processes by information systems is more profitable then performing them manually and positive effects outweigh the negative ones in the long run. The reflections of this result to the macro economy are increased welfare, improved economic efficiency, better and faster allocation and re-allocation of resources, flexibility to cope with inflation and unemployment, increased total economic output, balanced internal and external trade, proper use of workforce, more effective

governmental policies, increased total tax revenue, and improved budget while the reflections of this result to the micro economy are economies of scale in documentation and managerial activities, better allocation of scarce resources, lower prices depending on lower costs, more competitive markets depending on lower prices, and more efficient time usage depending on decreased opportunity costs. However, in the economic sense there are two problems limiting wider application of electronic signature one of which is the cost of electronic signature and the other is the cost of teaching people how to use electronic signature.

Our analyses on both institutional and personal surveys have shown that both institutions and people are oriented to use information technologies including the electronic signature but the coordination and interoperability are not considered sufficiently. In addition to this, the level of awareness is very low for the electronic signature concept which has been in the agenda of governmental and private institutions for nearly five years and this low level of awareness limits the diffusion rate of technology.

Although the analyses performed in this study form a starting point for evaluating legal base, economic applications and awareness level of electronic signature in Turkey, there is still much to do. Any future research extending beyond this study shall consider two important points related with this study.

One point is related with the methods used for legal analyses. Legal analyses in the study focus on two perspectives one of which is the determination of gaps inside Turkish legal base while the other is the determination of differences between Turkish legal base and other countries' legal bases. For the first perspective, any gap found in the analyses can be interpreted by other researchers as not being a gap as the legal analyses depends on comments instead of universal truths. For the second perspective, as the results obtained from the implementation of legal bases vary from country to country, it is not possible to say that a law, an ordinance or a communiqué working very well in some country will work well in other countries

too. Perhaps a study containing the results obtained from practical implementation of legal base can be developed in the future which will support or refute the analyses in this study.

The other point is related with the calculations performed over surveys. Calculations in this study are based on analytical thinking and logical inferences instead of using predefined modeling methods and statistical techniques and the statistical reliability of surveys are not considered. As a result of this, reliability of the results may be debatable. In addition to this, the study combines and compares its results with the results of other studies to obtain final calculations. This means that, any deviation or wrong calculation in the results of other studies also affects the reliabilities of the results of this study. Perhaps a study using predefined modeling methods and statistical techniques with a bigger and a more heterogeneous statistically reliable survey can be developed in the future which will obtain more definite calculations than the ones in this study.

BIBLIOGRAPHY

[1] Article 14 of *Turkish Law of Obligations Numbered 818 of 1926.*

[2] Article 2 of *EU Directive 1999/93 of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.*

[3] *Kamu Bilişim Platformu VII, E-imza'nın Toplumsal Boyutu, 2. Çalışma Grubu Raporu,* pp: 14-15, 2005.

[4] Menezes A., Van Oorschot P. and Vanstone S., *Handbook of Applied Cryptography,* pp:1.2, CRC Press, 1996.

[5] *Introduction to History,* Retrieved August 12, 2005, from http://www.nsa.gov/history/index.cfm

[6] *General Information,* Retrieved August 12, 2005, from http://www.nist.gov/public_affairs/general2.htm

[7] *CISSP Study Notes from CISSP Prep Guide,* Retrieved August 12, 2005, from http://www.braindumps.com/dls/11298.doc

[8] *Açık Anahtarlı Kriptografi,* Retrieved August 12, 2005, from http://www.enderunix.org/docs/pkc.html

[9] *Digital Signature,* Retrieved August 13, 2005, from http://europa.eu.int/ISPO/ecommerce/issues/digisig/digisign3.htm

[10] Brickell E., Pointcheval D., Vaudenay S. and Yung M., *Design Validations For Discrete Logarithm Based Signature Schemes,* Lecture Notes in Computer Science 1751, pp:276-292, 2000.

[11] *Risks of Relying on Cryptography Discussion,* Retrieved August 14, 2005, from http://www.ciphersbyritter.com/NEWS5/RISKRELY.HTM

[12] *Wikipedia - Key space,* Retrieved August 14, 2005, from http://en.wikipedia.org/wiki/Keyspace

[13] Schneir B., *Applied Cryptography,* pp:191-210, John Wiley & Sons Inc., 1996

[14] Singh S., *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography,* pp:264, Anchorbooks, 2005.

[15] *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1,* RSA Security Inc., 2000.

[16] *Identification and Authentication,* NIST Computer Security Handbook, Retrieved August 14, 2005, from http://niatec.info/pdf/nistiadraft.pdf

[17] *RSA Security - 2.2.5 What is Identification?,* Retrieved August 14, 2005, from http://www.rsasecurity.com/rsalabs/node.asp?id=2185

[18] *RSA Security - 2.1.9 What are Secret Sharing Schemes?,* Retrieved August 14, 2005, from http://www.rsasecurity.com/rsalabs/node.asp?id=2179

[19] Alkan M., Sağıroğlu Ş., *Her Yönüyle Elektronik İmza,* pp:3, Grafiker Yayınları, 2005.

[20] *US Department of Commerce, IT Security,* Retrieved August 14, 2005, from http://www.osec.doc.gov/cio/ITSIT/DOC_IT_Security_Program_Policy_Final_2003.htm

[21] Sections 201, 202, 203 of *Cyberspace Electronic Security Act (CESA) of 1999.*

[22] *HMAC,* Retrieved August 20, 2005, from http://en.wikipedia.org/wiki/HMAC

[23] *Secure Hash Algorithm Directory,* Retrieved August 20, 2005, from http://www.secure-hash-algorithm-md5-sha-1.co.uk/

[24] *Forrester Research - Global Online Trade,* Retrieved August 21, 2005, from http://www.forrester.com/ER/Research/Brief/Excerpt/0,1317,13720,FF.html

[25] *UNCITRAL - Model Law on Electronic Commerce with Guide to Enactment with Additional Article 5 as Adopted in 1998,* 1996.

[26] *UNCITRAL - Model Law on Electronic Signatures with Guide to Enactment,* 2001.

[27] Article 1 of *EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.*

[28] Article 1 of *EU Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market.*

[29] *Glossary,* Retrieved October 8, 2005, from http://www.pki.vt.edu/help/glossary.html

[30] *Products and Downloads,* Retrieved May 6, 2006, from http://www.signature-perfect.com/english/products_en/products_en.html

[31] *E-signature Resource Center,* Retrieved May 6, 2006, from http://www.silanis.com/site/resource_center/

[32] *Nitelikli Elektronik Sertifika Fiyatları,* Retrieved May 6, 2006, from http://www.turktrust.com.tr/statics/niteliklielektroniksertifikafiyatlari.jsp

[33] *PKI Uygulamalarındaki Gelişmeler ve Dünyadan Örnekler,* Siemens Business Services Sistem Hizmetleri A.Ş. Stratejik Planlama ve Pazarlama Grubu, pp:15-17, 2004

[34] *The Legal And Market Aspects of Electronic Signatures, Study for The European Commission - DG Information Society,* pp:68-69, 2003.

[35] *WMRC Global E-Government Survey 2001,* Retrieved October 6, 2005, from http://www.insidepolitics.org/egovt01int.html.

[36] *FECC DOD - Industry Working Group Final Report,* pp:10-14, 2000

[37] *Northrop Grumman Successfully Deploys Smart IT Security Nationwide,* Retrieved October 10, 2005, from http://www.primezone.com/newsroom/?d=74275

[38] *CIBC - Quick Facts,* Retrieved October 10, 2005, from http://www.cibc.com/ca/inside-cibc/quick-facts.html

[39] *Securenet,* Retrieved October 11, 2005, from http://www.securenet.com.au/investor/p_investor.asp?navid=180

[40] *PKI International Scan,* Retrieved October 11, 2005, from http://www.solutions.gc.ca/pki-icp/pki-in-practice/efforts/2002-07/scan-analyse04_e.asp#_Toc19584695

[41] *SEEMail - New Zealand E-government Programme,* Retrieved October 10, 2005, from http://www.e.govt.nz/services/see

[42] *ICTSB Homepage,* Retrieved October 11, 2005, from http://www.ict.etsi.org

[43] *Final Report of the EESSI Expert Team,* pp:32-66, 1999, Retrieved October 11, 2005, from http://www.ictsb.org/EESSI/Documents/Final-Report.pdf

[44] *EUROPEA - IDABC, Austria Launches Electronic Health Insurance Card Pilot,* Retrieved October 11, 2005, from http://europa.eu.int/idabc/jsps/documents/dsp_showPrinterDocument.jsp?docID=3691&lg=en

[45] *PKI Uygulamalarındaki Gelişmeler ve Dünyadan Örnekler,* Siemens Business Services Sistem Hizmetleri A.Ş. Stratejik Planlama ve Pazarlama Grubu, pp:6-8, 2004.

[46] *PKI Uygulamalarındaki Gelişmeler ve Dünyadan Örnekler,* Siemens Business Services Sistem Hizmetleri A.Ş. Stratejik Planlama ve Pazarlama Grubu, pp:9-12, 2004.

[47] *EUROPEA - IDABC, EDay2 Marks New E-Government Milestone In Denmark,* Retrieved October 11, 2005, from http://europa.eu.int/idabc/en/document/3835/194

[48] *EUROPEA - IDABC, Hungarian Government Extends Mandatory e-Filing of Tax Returns,* Retrieved October 11, 2005, from http://europa.eu.int/idabc/jsps/documents/dsp_showPrinterDocument.jsp?docID=3694&lg=en

[49] *Elektronik İmza Ulusal Koordinasyon Kurulu Hazırlık Raporu,* p:32-33, Telekomünikasyon Kurumu, 2004.

[50] *Kamuyu Aydınlatma Platformu,* Retrieved October 12, 2005, from http://www.spk.gov.tr/kap/eisis_genel_bilgi.html

[51] *KAP Şirketler,* Retrieved October 12, 2005, from http://kap.gov.tr/Yay/Sirket/sirketListe.aspx

[52] *Inward Processıng Regime,* Retrieved October 12, 2005, from http://www.dtm.gov.tr/ihr/mevzu/dahhar/dir%20ingilizce%20Not-WEB-190905.doc

[53] *DTM E-imza Uygulamaları,* Retrieved October 12, 2005, from http://dir.dtm.gov.tr/basvuru/giris.jsp#

[54] Article 3 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[55] Article 2 of *Ireland Electronic Commerce Act of 2000.*

[56] Article 2/2 of *Austrian Electronic Signature Law SigG of 2000.*

[57] Article 6 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[58] Article 7 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[59] Article 9 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[60] Article 4 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[61] Article 5 of *EU Directive 1999/93 of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures.*

[62] Article 295 of *Turkish Law of Civil Procedure of 1927.*

[63] Article 5 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[64] Keser L., *Elektronik İmza Ulusal Koordinasyon Kurulu, Hukuk Çalışma Grubu İlerleme ve Sonuç Raporu,* pp:23-27, Temmuz 2004.

[65] Article 22 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[66] Article 23 of *Electronic Signature Law No: 5070 which was published in the Official Gazette of 23 January 2004.*

[67] Article 308 of *Turkish Law of Civil Procedure of 1927.*

[68] Article 68 of *Turkish Law of Debt Collection and Bankruptcy of 1932.*

[69] Article 242 of *Turkish Law of Tax Methods of 1961.*

[70] Article 42 of *Turkish Banking Law of 2005.*

[71] Article 3 of *Turkish Consumer Protection Law of 1995.*

[72] Article 9/A of *Turkish Consumer Protection Law of 1995.*

[73] Article 6 of *Communiqué on Processes and Technical Criteria Regarding Electronic Signatures.*

[74] Article 5 of *Ordinance on Insurance of Financial Liabilities in Certification of 2005.*

[75] Article 6 of *Ordinance on Insurance of Financial Liabilities in Certification of 2005.*

[76] Article 8 of *Ordinance on Insurance of Financial Liabilities in Certification of 2005.*

[77] *UNCTAD - E-commerce and Development Report 2002,* Retrieved August 28, 2005, from http://www.unctad.org/en/docs/ecdr2002_en.pdf

[78] Bozkurt V., *Elektronik Ticaretin Ekonomik ve Sosyal Boyutu,* p:66, Alfa Yayınları, 2000.

[79] İnalöz A., *Research on Electronic Commerce In The Framework of Telecommunications Regulatory Issues,* Expertise Thesis, pp:15-16, 2003.

[80] Ertuğrul Z., *Kamuda E-İmza Uygulamalarının İsrafi Önlemeye ve Verimliliğe Etkileri,* pp:17-18, 2004

[81] *Türkiye Bilişim Derneği, E-Toplum Çalışma Grubu, E-Birey Alt Çalışma Grubu, Sonuç Raporu,* p:15, 2004

[82] *Ceteris Paribus,* Retrieved September 12, 2005, from http://en.wikipedia.org/wiki/Ceteris_paribus

[83] *The Digital Strategy,* Retrieved October 16, 2005, from http://www.digitalstrategy.govt.nz/templates/Page____60.aspx

[84] *Awareness, Saivite Virtue*, Retrieved June 18, 2006, from www.himalayanacademy.com/resources/books/virtue/SVGlossary.html

[85] *Being Conscious,* Retrieved June 18, 2006, from http://srsc.ulb.ac.be/AI/lectures06/DEA06-ApReC-03.pdf

[86] *United Nations Development Program, Human Development Report,* pp:18-22, 2005.

[87] Castells M., *End of Millennium,* pp:21-22, Oxford Press, 1996.

[88] *E-imza Ulusal Koordinasyon Kurulu, Altyapı Çalışma Grubu, İlerleme Raporu,* pp:15-38, Retrieved October 26, 2005, from http://www.tk.gov.tr/eimza/doc/diger/altyapi.pdf

[89] *Hanehalkı Bilişim Teknolojileri Kullanımı,* Retrieved February 23, 2006, from http://www.tuik.gov.tr/PreHaberBultenleri.do?id=1

[90] Dalziel D., *Government Online, A Multi-Country Study Of E-Government Usage,* pp: 5-10, Taylor Nelson Sofres, 2004.

APPENDICES

APPENDIX A - STANDARDS OF CRYPTOGRAPHY

International Standards Organization (ISO)

- ISO/IEC 9798-1: Part 1: General Model
- ISO/IEC 9798-2: Part 2: Mechanisms Using Symmetric Encipherment Algorithms
- ISO/IEC 9798-3: Part 3: Entity Authentication Using A Public Key Algorithm
- ISO/IEC 9798-4: Part 4: Mechanisms Using A Cryptographic Check Function
- ISO/IEC 9797: Data Integrity Mechanism Using A Cryptographic Check Function Employing A Block Cipher Algorithm
- ISO/IEC 9796: Digital Signature Schemes Giving Message Recovery
- ISO/IEC 8372: Modes Of Operation For A 64-Bit Block Cipher Algorithm
- ISO/IEC 9160: Physical Layer Interoperability Requirements
- ISO/IEC 9979: Procedures For The Registration Of Cryptographic Algorithms
- ISO/IEC 10116: Modes Of Operation For An N-Bit Block Cipher Algorithm
- ISO/IEC 10118-1: Hash-Functions - Part 1: General
- ISO/IEC 10118-2: Hash-Functions - Part 2: Hash-Functions Using An N-Bit Block Cipher Algorithm

- ISO/IEC DIS 11770-2: Key Management - Part 2: Mechanisms Using Symmetric Techniques

International Telecommunications Union (ITU)

- [X.273] Information Technology - Open Systems Interconnection - Network Layer Security Protocol
- [X.274] Information Technology - Telecommunication And Information Exchange Between Systems - Transport Layer Security Protocol
- [X.509] Information Technology - Open Systems Interconnection - The Directory: Authentication Framework
- [X.736] Information Technology - Open Systems Interconnection - Systems Management: Security Alarm Reporting Function
- [X.736 Summary] Summary Of Recommendation X.736
- [X.740] Information Technology - Open Systems Interconnection - Systems Management: Security Audit Trail Function
- [X.800] Security Architecture For Open Systems Interconnection For Ccitt Applications
- [X.800 SUMMARY] Summary of Recommendation X.800
- [X.802] Information Technology - Lower Layers Security Model
- [X.803] Information Technology - Open Systems Interconnection - Upper Layers Security Model

National Institute of Standards and Technology (NIST)

- X3: Information Processing Systems
- X9.9: Existing Wholesale DES MAC Standard
- X9.19: Existing Retail DES MAC Standard
- X9.23: Existing Wholesale Encryption Standard
- X9.17: Existing, Recently Updated Wholesale DES Key Management Standard

- X9.24: Existing retail DES key management standard
- X9.30: Part 1: Digital Signature Algorithm
- X9.30: Part 2: Secure Hash Algorithm
- X9.30: Part 3: Certificate Management For DSA
- X9.31: Part 1: RSA Signature Standard
- X9.31: Part 2: MD2, MD5, SHA, MDC-2
- X9.31: Part 3: Certificate Management
- X9.42: Diffie-Hellman Key Agreement
- X9.44: Transport Of Keys Using RSA
- X9.45: Attribute Certificates
- X9.41: Mechanisms To Manage Security Services
- X12.58 (Version 2): EDI Security Structures

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 1363-2000: Standard Specifications For Public Key Cryptography IEEE 1363a-2004: Standard Specifications For Public Key Cryptography - Amendment 1: Additional Techniques
- IEEE P1363.1: Public-Key Cryptographic Techniques Based On Hard Problems Over Lattices
- IEEE P1363.2: Password-Based Public-Key Cryptography
- IEEE P1363.3: Identity-Based Public Key Cryptography

Internet Engineering Task Force (IETF) -Working Groups In The Security Area

- An Open Specification for Pretty Good Privacy (openpgp)
- Authenticated Firewall Traversal (aft)
- Common Authentication Technology (cat)
- IP Security Policy (ipsp)
- IP Security Protocol (ipsec)
- IP Security Remote Access (ipsra)
- Intrusion Detection Exchange Format (idwg)

- Kerberized Internet Negotiation of Keys (kink)
- Kerberos WG (krb-wg)
- One Time Password Authentication (otp)
- Public-Key Infrastructure (X.509) (pkix)
- S/MIME Mail Security (smime)
- Secure Network Time Protocol (stime)
- Secure Shell (secsh)
- Securely Available Credentials (sacred)
- Security Issues in Network Event Logging (syslog)
- Simple Public Key Infrastructure (spki)
- Transport Layer Security (tls)
- Web Transaction Security (wts)
- XML Digital Signatures (xmldsig)

RSA Security

- PKCS # 1 The RSA encryption standard.
- PKCS # 3 The Diffie-Hellman key-agreement standard.
- PKCS # 5 The password-based encryption standard (PBE).
- PKCS # 6 The extended-certificate syntax standard.
- PKCS # 7 The cryptographic message syntax standard.
- PKCS # 8 The private-key information syntax standard.
- PKCS # 9 This defines selected attribute types for use in other PKCS standards.
- PKCS # 10 The certification request syntax standard.
- PKCS # 11 The cryptographic token interface standard.
- PKCS # 12 The personal information exchange syntax standard.
- PKCS # 13 The elliptic curve cryptography standard.
- PKCS # 14 This covers pseudo random number generation (PRNG).
- PKCS # 15 The cryptographic token information format standard.

Note: PKCS #2 and #4 do not exist anymore because they have been incorporated into PKCS #1.

APPENDIX B - MATHEMATICAL BASICS OF RSA

A. Initializing RSA

1. Pick two large primes, P and Q.
2. Find N = P * Q. N is the RSA modulus.
3. Let E be a number relatively prime to (P-1) * (Q-1).
4. Find D, so that D * E = 1 mod (P-1) * (Q-1).
5. The set (E, N) is the public key.
6. The set (D, N) is the private key.

B. Encrypting Message

1. Let M be the message.
2. Make sure M < N, otherwise split M in suitably small pieces and perform RSA on each individual piece.
3. Compute $C = M^E \bmod N$.
4. C is the encrypted message.

C. Decrypting Message

1. Let C be the encrypted message.
2. Compute $M = C^D \bmod N$.
3. M is the original message.

D. Signing Message

1. Let M be the message.
2. Compute $S = M^D \bmod N$.
3. S is the digital signature. Send it with message M.

E. Verifying Message

1. Let S be the signed message
2. Compute $M_c = S^E \bmod N$
3. Check if $M_c = M$.

APPENDIX C - INSTITUTIONAL SURVEY OF TELECOMMUNICATIONS AUTHORITY ON ELECTRONIC SIGNATURE

Retrieved From Telecommunications Authority 2005 [88]

Unofficial Translation of Institutional Survey of Telecommunications Authority on Electronic Signature.

Important Notice: In case of divergent interpretation, the original Turkish text shall prevail.

1- Do you use electronic signature in your institution? If your answer is "No" then when do you plan to use it?

Ministry of Justice	Yes.
Turkish Notary Union	Yes.
Ankara Metropolitan Municipality	No. In 12-24 months.
TÜBİTAK - BİLTEN	No. In 12-24 months.
Undersecreteriat of Maritime	No. In 12-24 months.
Turkish State Meteorological Service	No. In 12-24 months.
State Statistics Institute	No. In 12-24 months.
Undersecreteriat of the Prime Ministry for Foreign Trade	No. In 0-6 months.
The Pension Fund for Civil Servants	No. In 12-24 months.

Question 1 (continued)

Undersecreteriat of Customs	No. In 6-12 months.
İstanbul Metropolitan Municipality	No. In 12-24 months.
Ministry of Finance	No. In 12-24 months.
Central Bank of Turkey	Yes.
Public Registration Office	No. In 6-12 months.
Turkish Republic State Railways	No. In 12-24 months.
Turkish Cooperation and Development Administration	No. In 0-6 months.
Turkish Standardization Institute	No. In 6-12 months.
Capital Markets Board of Turkey	Yes.

2- Which Public Key Infrastructure (PKI) technology do you (plan to) use in your infrastructure?

Ministry of Justice	USB Token.
Turkish Notary Union	USB Token.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	Soft Certificate, Smartcard, USB Token.
Turkish State Meteorological Service	USB Token, One Time Password Creator.
State Statistics Institute	Smartcard, USB Token.

Question 2 (continued)

Undersecreteriat of the Prime Ministry for Foreign Trade	Smartcard.
The Pension Fund for Civil Servants	Soft Certificate, Smartcard, USB Token.
Undersecreteriat of Customs	Not decided yet.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	Soft Certificate.
Central Bank of Turkey	Soft Certificate.
Public Registration Office	Not decided yet.
Turkish Republic State Railways	USB Token.
Turkish Cooperation and Development Administration	Soft Certificate.
Turkish Standardization Institute	Soft Certificate.
Capital Markets Board of Turkey	Smartcard.

3- Which certification authority software do you (plan to) use for electronic signature?

Ministry of Justice	Microsoft CA.
Turkish Notary Union	A pilot study developed by TNU which started in December 2001.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	TÜBİTAK - BİLTEN - ZEUGMA.

Question 3 (continued)

Undersecreteriat of Maritime	TÜBİTAK - UEKAE - ASYA.
Turkish State Meteorological Service	TÜBİTAK - UEKAE - ASYA.
State Statistics Institute	TÜBİTAK - UEKAE - ASYA, Verisign CA
Undersecreteriat of the Prime Ministry for Foreign Trade	TÜBİTAK - BİLTEN - ZEUGMA.
The Pension Fund for Civil Servants	TÜBİTAK - UEKAE - ASYA, GlobalSign CA.
Undersecreteriat of Customs	TÜBİTAK - UEKAE - ASYA.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	Not decided yet.
Central Bank of Turkey	GlobalSign CA, Microsoft CA.
Public Registration Office	Will be defined according to the result of tender.
Turkish Republic State Railways	Not decided yet.
Turkish Cooperation and Development Administration	GlobalSign CA.
Turkish Standardization Institute	Not decided yet.
Capital Markets Board of Turkey	TÜBİTAK - BİLTEN - ZEUGMA.

4- Did you perform any research on the electronic signature subject other than present solutions? If your answer is “Yes” with which institution did you work together?

Ministry of Justice	To use in daily processes, a one month study was conducted with HAVELSAN A.Ş.
Turkish Notary Union	1 year of research (2001) and 3 years of production and pilot study exist.
Ankara Metropolitan Municipality	No.
TÜBİTAK - BİLTEN	No.
Undersecreteriat of Maritime	No.
Turkish State Meteorological Service	No.
State Statistics Institute	No.
Undersecreteriat of the Prime Ministry for Foreign Trade	A study was conducted with other institutions for an 8 months period with the aim of increasing integration, efficiency and effectivity.
The Pension Fund for Civil Servants	No.
Undersecreteriat of Customs	No.
İstanbul Metropolitan Municipality	No.
Ministry of Finance	No.
Central Bank of Turkey	A study was conducted to integrate the system into the inside processes of institution.
Public Registration Office	No.
Turkish Republic State Railways	No.
Turkish Cooperation and Development Administration	A 3 months study was conducted with Ministry of Foreign Affairs to integrate the system into inside processes of institution.

Question 4 (continued)

Turkish Standardization Institute	No study was performed but meetings were performed for using electronic signature in documentation system
Capital Markets Board of Turkey	Experiences of TÜBİTAK - BİLTEN was used.

5- Which method is /will be used for running and operating the system?

Ministry of Justice	Will be performed by institution's own resources.
Turkish Notary Union	Will be performed by institution's own resources.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	Will be performed by institution's own resources. Support from related companies will be demanded.
Turkish State Meteorological Service	Not decided yet.
State Statistics Institute	Will be performed in the scope of EU projects.
Undersecreteriat of the Prime Ministry for Foreign Trade	Will be performed by institution's own resources.
The Pension Fund for Civil Servants	Not decided yet.
Undersecreteriat of Customs	Not decided yet.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	Not decided yet.
Central Bank of Turkey	Will be performed by institution's own resources.
Public Registration Office	Not decided yet.
Turkish Republic State Railways	Not decided yet.

Question 5 (continued)

Turkish Cooperation and Development Administration	Will be performed by institution's own resources.
Turkish Standardization Institute	Support from related companies will be demanded.
Capital Markets Board of Turkey	Will be performed by institution's own resources. Software will be managed from SPK and TÜBİTAK - BİLTEN will be certificate authority

6- What kinds of measures are taken to provide continuity of system when it is faced with new technologies and standards?

Ministry of Justice	No measures.
Turkish Notary Union	A complete integration exists so the applications can be updated by changing only one DLL.
Ankara Metropolitan Municipality	No measures.
TÜBİTAK - BİLTEN	As BİLTEN is a research and development institute of TÜBİTAK, continuity can be obtained spontaneously.
Undersecreteriat of Maritime	No measures.
Turkish State Meteorological Service	No measures.
State Statistics Institute	It is planned to acquire suitable software and hardware for the upgrade.
Undersecreteriat of the Prime Ministry for Foreign Trade	Current structure will be adapted to changing technologies and standards. In addition to this specific personnel will be trained related with the subject in the long run. Project is designed on a wide scope considering the possible developments in the long run. It is not expected that it will be hard to adopt changes.
The Pension Fund for Civil Servants	No measures.
Undersecreteriat of Customs	No measures.
İstanbul Metropolitan Municipality	No measures.
Ministry of Finance	No measures.

Question 6 (continued)

Central Bank of Turkey	Widely accepted standards allowing transfers between different technologies are taken into consideration.
Public Registration Office	No measures.
Turkish Republic State Railways	This subject will be added to list of specifications designed for documentation automation system.
Turkish Cooperation and Development Administration	Database is designed in a flexible manner. Java programming language and Oracle database system is preferred to provide platform independency.
Turkish Standardization Institute	No measures.
Capital Markets Board of Turkey	Specific personnel will be trained related with the subject in the long run and the developments will be followed by these personnel.

7- How did you start to/plan to use the electronic signature?

Ministry of Justice	Not decided yet.
Turkish Notary Union	By research and development performed in partnership with Israeli Companies on e-management and e-cashier programs.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	By using institution's own resources.
Undersecreteriat of Maritime	By using the resources of other institutions working on the subject and by local companies which provide solution.
Turkish State Meteorological Service	By local companies which provide solution.
State Statistics Institute	Other.

Question 7 (continued)

Undersecreteriat of the Prime Ministry for Foreign Trade	By using institution's own resources and by local companies which provide solution.
The Pension Fund for Civil Servants	By local companies which provide solution.
Undersecreteriat of Customs	By using institution's own resources.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	By using the resources of other institutions working on the subject.
Central Bank of Turkey	By using institution's own resources.
Public Registration Office	Other.
Turkish Republic State Railways	By local companies which provide solution.
Turkish Cooperation and Development Administration	By using institution's own resources.
Turkish Standardization Institute	By local companies which provide solution.
Capital Markets Board of Turkey	By local companies which provide solution. (The project is developed in coordination with İstanbul Stock Exchange (IMKB). Financial resources are provided by İMKB.

8- Which institutions and which applications are chosen for integration?

Ministry of Justice	It is thought to integrate the system with Mernis, Takbis, Judical Record, Polnet and Say200 projects in the scope of National Judgment Network Project (UYAP). This integration aims to send and receive electronically signed documents over electronic networks.

Question 8 (continued)

Turkish Notary Union	It is thought to integrate the system with Mernis, Takbis, Polnet, UYAP and Social Security Institution (SSK). This integration aims to send and receive XML based electronically signed documents which are stored on Oracle databases.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	Not decided yet.
Turkish State Meteorological Service	It is thought to integrate the system with General Directorate of State Hydraulic Works (DSİ), Universities and member media enterprises in the scope of e-government and e-Turkey.
State Statistics Institute	It is thought to integrate the system with Prime Ministry, Other Ministries and State Planning Institute.
Undersecreteriat of the Prime Ministry for Foreign Trade	It is thought to integrate the system with Ministry of Trade, Exporter Unions, Undersecreteriat of Customs, Union of Chambers and Commodity Exchanges of Turkey (TOBB)
The Pension Fund for Civil Servants	Not decided yet.
Undersecreteriat of Customs	It is thought to integrate the system with electronic data interchange (EDI) of Customs Automation project. This integration aims to cover importers, exporters and transporters.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	Not decided yet.
Central Bank of Turkey	It is thought to integrate the system with banks and accountancy.

Question 8 (continued)

Public Registration Office	Not decided yet.
Turkish Republic State Railways	Not decided yet.
Turkish Cooperation and Development Administration	Not decided yet.
Turkish Standardization Institute	It is thought to integrate the system with related institutions like Ministry of Trade and TOBB
Capital Markets Board of Turkey	It is thought to integrate the system with related institutions like İMKB, TAKASBANK, Central Registration Institution, Union of Turkish Capital Markets Agents.

9- Which methods are preferred in the integration process with other institutions?

Ministry of Justice	No answer.
Turkish Notary Union	Direct access to TNU website based on XML is planned.
Ankara Metropolitan Municipality	No answer.
TÜBİTAK - BİLTEN	No answer.
Undersecreteriat of Maritime	No answer.
Turkish State Meteorological Service	It is planned to integrate data transmission property to institution's own software by using development tools. Data transmission will be provided over web-based pages.
State Statistics Institute	Data transmission will be provided over web-based pages.
Undersecreteriat of the Prime Ministry for Foreign Trade	Direct data transmission. It is planned to integrate data transmission property to institution's own software by using development tools. Data transmission will be provided over web-based pages.

Question 9 (continued)

The Pension Fund for Civil Servants	Direct data transmission. It is planned to integrate data transmission property to institution's own software by using development tools.
Undersecreteriat of Customs	Direct data transmission.
İstanbul Metropolitan Municipality	No answer.
Ministry of Finance	No answer.
Central Bank of Turkey	Under evaluation.
Public Registration Office	Usage of all explained methods.
Turkish Republic State Railways	No answer.
Turkish Cooperation and Development Administration	No integration.
Turkish Standardization Institute	Under evaluation.
Capital Markets Board of Turkey	No answer.

10- What kinds of measures are taken to block repetition of transmission of information between institutions? If repetition is necessary, how up-to-dateness of information is provided?

Ministry of Justice	The main aim of UYAP is to prevent repetition. As a result of this, it is integrated with Polnet
Turkish Notary Union	It is planned to synchronize databases of related institutions.
Ankara Metropolitan Municipality	No answer.
TÜBİTAK - BİLTEN	No answer.
Undersecreteriat of Maritime	No answer.

Question 10 (continued)

Turkish State Meteorological Service	No answer.
State Statistics Institute	With the construction of database, repetition will be prevented.
Undersecreteriat of the Prime Ministry for Foreign Trade	Exporter unions will be integrated into system. As a result of this, repetition will be minimal. However integration with other institutions has not been provided yet.
The Pension Fund for Civil Servants	No answer.
Undersecreteriat of Customs	No answer.
İstanbul Metropolitan Municipality	No answer.
Ministry of Finance	No answer.
Central Bank of Turkey	Data gathered from different institutions is processed and transferred to the related institutions.
Public Registration Office	No answer.
Turkish Republic State Railways	No answer.
Turkish Cooperation and Development Administration	Integration with other institutions has not been provided yet.
Turkish Standardization Institute	It is planned to use all of information related resources from one central point to prevent repetition.
Capital Markets Board of Turkey	No answer.

11- What is/will be the number of users using electronic signature public key infrastructure in your institution?

Ministry of Justice	10.001 and more users.
Turkish Notary Union	5.001- 10.000 users.

Question 11 (continued)

Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	501 - 1.000 users.
Undersecreteriat of Maritime	1.001 - 5.000 users.
Turkish State Meteorological Service	501 - 1.000 users.
State Statistics Institute	1.001 - 5.000 users.
Undersecreteriat of the Prime Ministry for Foreign Trade	5.001 - 10.000 users.
The Pension Fund for Civil Servants	5.001 - 10.000 users.
Undersecreteriat of Customs	5.001 - 10.000 users.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	1.001 - 5.000 users.
Central Bank of Turkey	Not decided yet.
Public Registration Office	1.001 - 5.000 users.
Turkish Republic State Railways	501 - 1.000 users.
Turkish Cooperation and Development Administration	10.001 and more users.
Turkish Standardization Institute	51 - 100 users.
Capital Markets Board of Turkey	1.001 - 5.000 users.

12- What is/will be the number of active users using electronic signature and public key infrastructure in your institution?

Ministry of Justice	10.001 and more users.
Turkish Notary Union	Currently 1.000 users use electronic signature and it is planned to reach 5.000 users in the future.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	101 - 500 users.
Undersecreteriat of Maritime	501 - 1.000 users.
Turkish State Meteorological Service	501 - 1.000 users.
State Statistics Institute	1.001 - 5.000 users.
Undersecreteriat of the Prime Ministry for Foreign Trade	5.001 - 10.000 users.
The Pension Fund for Civil Servants	0 - 50 users.
Undersecreteriat of Customs	5.001 - 10.000 users.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	Not decided yet.
Central Bank of Turkey	1001 - 5000 users.
Public Registration Office	10.001 and more users.
Turkish Republic State Railways	Not decided yet.
Turkish Cooperation and Development Administration	10.001 and more users.
Turkish Standardization Institute	51 - 100 users.
Capital Markets Board of Turkey	1.001 - 5.000 users.

13- For which kind of business processes and for how many people do you (plan to) use electronic signature?

Ministry of Justice	Inside our institution. Between our institution and other public institutions. Between our institution and citizens.
Turkish Notary Union	Inside our institution: 150 users. Between notaries: 5.000 users. Between our institution and other public institutions.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	Inside our institution. Between our institution and other public institutions. Between our institution and other private institutions. Between our institution and citizens.
Turkish State Meteorological Service	Inside our institution: 500 users. Between our institution and other public institutions: 50 users. Between our institution and other private institutions: 100 users. Between our institution and citizens: 25 users. Between our institution and other international institutions like WMO, EUMETSAT, ECMWF or NATO
State Statistics Institute	Inside our institution: 2.500 users. Between our institution and other public institutions: 2.500 users. Between our institution and other private institutions.
Undersecreteriat of the Prime Ministry for Foreign Trade	Inside our institution: 300 - 500 users. Between our institution and other public institutions: 100 users. Between our institution and exporter institutions: More than 5.000 users.

Question 13 (continued)

The Pension Fund for Civil Servants	Inside our institution: 200 users. Between our institution and other public institutions: 50 users. Between our institution and other private institutions: 50 users. Between our institution and citizens: 5.000.000 users.
Undersecreteriat of Customs	Not decided yet.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	Not decided yet.
Central Bank of Turkey	Inside our institution: 4.500 users. Between our institution and other public institutions: 300 users. Between our institution and other private institutions: 1.000 users.
Public Registration Office	Inside our institution: 5.000 users. Between our institution and other public institutions: 3.000 users. Between our institution and citizens Between our institution and international institutions.
Turkish Republic State Railways	Inside our institution: 1.500 users.
Turkish Cooperation and Development Administration	Inside our institution: Unlimited users. Between international coordinators: Unlimited users.
Turkish Standardization Institute	Inside our institution. Between our institution and other public institutions. Between our institution and other private institutions. Between our institution and citizens.
Capital Markets Board of Turkey	Between our institution and other private institutions. SPK, İMKB, TAKASBANK, MKK, TSPAKB, Institutions operate in İMKB (299 Companies, 117 Agents and 71 Independent Auditors)

14- If you prefer to use electronic signature inside your institution for which processes do you (plan to) use it?

Ministry of Justice	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.
Turkish Notary Union	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment. For decision/support processes and managerial activities. For auditing distant projects from center in a secure way.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	For system login and access. For electronically signing documents and data in computer environment.
Turkish State Meteorological Service	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.
State Statistics Institute	For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.
Undersecreteriat of the Prime Ministry for Foreign Trade	For system login and access. For electronically signing documents and data in computer environment. Other: For accessing to projects and providing document flows.

Question 14 (continued)

The Pension Fund for Civil Servants	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.
Undersecreteriat of Customs	For electronically signing documents and data in computer environment.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	For electronically signing documents and data in computer environment.
Central Bank of Turkey	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.
Public Registration Office	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.
Turkish Republic State Railways	For system login and access. For electronically signing documents and data in computer environment.
Turkish Cooperation and Development Administration	For electronically signing documents and data in computer environment.
Turkish Standardization Institute	For electronically signing documents and data in computer environment.
Capital Markets Board of Turkey	For system login and access. For electronically signing documents and data in computer environment. For electronically encrypting documents and data in computer environment.

15- If you prefer to use electronic signature for communicating with other public institutions, for which processes do you (plan to) use it?

Ministry of Justice	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.
Turkish Notary Union	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions.
Turkish State Meteorological Service	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.
State Statistics Institute	For electronically signing documents and data in computer environment between institutions.
Undersecreteriat of the Prime Ministry for Foreign Trade	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions.

Question 15 (continued)

The Pension Fund for Civil Servants	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.
Undersecreteriat of Customs	Not decided yet.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	For electronically signing documents and data in computer environment between institutions.
Central Bank of Turkey	For system login and access between institutions. For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.
Public Registration Office	For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.
Turkish Republic State Railways	Not decided yet.
Turkish Cooperation and Development Administration	It is not planned to be used between our institution and other public institutions.
Turkish Standardization Institute	For electronically signing documents and data in computer environment between institutions.
Capital Markets Board of Turkey	For electronically signing documents and data in computer environment between institutions. For electronically encrypting documents and data in computer environment between institutions.

16- If you prefer to use electronic signature for communicating with other private institutions, for which processes do you (plan to) use it?

Ministry of Justice	Not decided yet.
Turkish Notary Union	Not decided yet.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.
Undersecreteriat of Maritime	For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions.
Turkish State Meteorological Service	For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions.
State Statistics Institute	For electronically signing documents and data in computer environment between our institution and other private institutions. For electronically encrypting documents and data in computer environment between our institution and other private institutions.
Undersecreteriat of the Prime Ministry for Foreign Trade	For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions.

Question 16 (continued)

The Pension Fund for Civil Servants	For providing our institution the opportunity of logging in and accessing to other private institutions' systems. For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions. For electronically encrypting documents and data in computer environment between our institution and other private institutions.
Undersecreteriat of Customs	For electronically signing documents and data in computer environment between our institution and other private institutions.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions.
Central Bank of Turkey	For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions. For electronically encrypting documents and data in computer environment between our institution and other private institutions.

Question 16 (continued)

Public Registration Office	For providing our institution the opportunity of logging in and accessing to other private institutions' systems. For providing private institutions the opportunity of logging in and accessing to our institution's systems. For electronically signing documents and data in computer environment between our institution and other private institutions. For electronically encrypting documents and data in computer environment between our institution and other private institutions.
Turkish Republic State Railways	Not decided yet.
Turkish Cooperation and Development Administration	Not decided yet.
Turkish Standardization Institute	For electronically signing documents and data in computer environment between our institution and other private institutions.
Capital Markets Board of Turkey	For electronically signing documents and data in computer environment between our institution and other private institutions.

17- If you prefer to use electronic signature for communicating with citizens, for which processes do you (plan to) use it?

Ministry of Justice	For providing the citizens the opportunity of electronically signing documents when applying to our institution.
Turkish Notary Union	Not decided yet.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	Not decided yet.

Question 17 (continued)

Undersecreteriat of Maritime	For providing the citizens the opportunity of electronically signing documents when applying to our institution. For providing the citizens the opportunity of electronically encrypting documents when applying to our institution.
Turkish State Meteorological Service	For providing the citizens the opportunity of electronically signing documents when applying to our institution.
State Statistics Institute	Not decided yet.
Undersecreteriat of the Prime Ministry for Foreign Trade	For providing the citizens the opportunity of logging in and accessing to our institution's systems. For providing the citizens the opportunity of electronically signing documents when applying to our institution.
The Pension Fund for Civil Servants	For providing the citizens the opportunity of logging in and accessing to our institution's systems. For providing the citizens the opportunity of electronically signing documents when applying to our institution. For providing the citizens the opportunity of electronically encrypting documents when applying to our institution.
Undersecreteriat of Customs	Not decided yet.
İstanbul Metropolitan Municipality	Not decided yet.
Ministry of Finance	For providing the citizens the opportunity of logging in and accessing to our institution's systems. For providing the citizens the opportunity of electronically signing documents when applying to our institution.

Question 17 (continued)

Central Bank of Turkey	Not decided yet.
Public Registration Office	For providing the citizens the opportunity of electronically signing documents when applying to our institution. For providing the citizens the opportunity of electronically encrypting documents when applying to our institution.
Turkish Republic State Railways	Not decided yet.
Turkish Cooperation and Development Administration	Not decided yet.
Turkish Standardization Institute	For providing the citizens the opportunity of electronically signing documents when applying to our institution.
Capital Markets Board of Turkey	Not decided yet.

18- With which purposes do you (plan to) use electronic signature?

Ministry of Justice	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable.
Turkish Notary Union	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To provide secure document flow.
Ankara Metropolitan Municipality	Not decided yet.
TÜBİTAK - BİLTEN	To diminish processes which depend on handwritten signatures and paper stock.

Question 18 (continued)

Undersecreteriat of Maritime	To increase the speed and security of business processes. To provide legal base to electronic business processes.
Turkish State Meteorological Service	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To provide public employees and citizens the opportunity of accessing products and services. To provide legal base to electronic business processes.
State Statistics Institute	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To adopt developments. To provide legal base to electronic business processes.
Undersecreteriat of the Prime Ministry for Foreign Trade	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To provide public employees and citizens the opportunity of accessing products and services.

Question 18 (continued)

The Pension Fund for Civil Servants	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To provide public employees and citizens the opportunity of accessing products and services. To provide legal base to electronic business processes.
Undersecreteriat of Customs	To diminish processes which depend on handwritten signatures and paper stock. To provide legal base to electronic business processes.
İstanbul Metropolitan Municipality	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To provide public employees and citizens the opportunity of accessing products and services. To adopt developments. To provide legal base to electronic business processes.
Ministry of Finance	To increase the speed and security of business processes. To make electronic business processes storable and traceable.
Central Bank of Turkey	To increase the speed and security of business processes. To adopt developments. To provide legal base to electronic business processes.

Question 18 (continued)

Public Registration Office	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To provide public employees and citizens the opportunity of accessing products and services. To adopt developments. To provide legal base to electronic business processes.
Turkish Republic State Railways	To diminish processes which depend on handwritten signatures and paper stock.
Turkish Cooperation and Development Administration	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable.
Turkish Standardization Institute	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To adopt developments. To provide legal base to electronic business processes.
Capital Markets Board of Turkey	To increase the speed and security of business processes. To diminish processes which depend on handwritten signatures and paper stock. To make electronic business processes storable and traceable. To provide public employees and citizens the opportunity of accessing products and services.

19- What kinds of problems did you face with when adapting electronic signature applications to real life?

Ministry of Justice	Continuity of obligation to use handwritten signature. Users' insufficiency to adapt themselves to the applications.
Turkish Notary Union	No answer.
Ankara Metropolitan Municipality	No answer.
TÜBİTAK - BİLTEN	No answer.
Undersecreteriat of Maritime	No answer.
Turkish State Meteorological Service	Continuity of obligation to use handwritten signature. Users' insufficiency to adapt themselves to the applications. Inadequate internet infrastructure in Turkey. Presence of exceptional cases in the institution which are not suitable for electronic signature. To provide legal base to electronic business processes.
State Statistics Institute	No answer.
Undersecreteriat of the Prime Ministry for Foreign Trade	Continuity of obligation to use handwritten signature. Users' insufficiency to adapt themselves to the applications. Infrastructural and technical insufficiency in institution to adapt the applications. Presence of exceptional cases in the institution which are not suitable for electronic signature.

Question 19 (continued)

The Pension Fund for Civil Servants	Continuity of obligation to use handwritten signature. Users' insufficiency to adapt themselves to the applications. Infrastructural and technical insufficiency in institution to adapt the applications.
Undersecreteriat of Customs	No answer.
İstanbul Metropolitan Municipality	No answer.
Ministry of Finance	No answer.
Central Bank of Turkey	Users' insufficiency to adapt themselves to the applications.
Public Registration Office	Continuity of obligation to use handwritten signature. Infrastructural and technical insufficiency in institution to adopt the applications. To provide legal base to electronic business processes.
Turkish Republic State Railways	No answer.
Turkish Cooperation and Development Administration	No answer.
Turkish Standardization Institute	No answer.
Capital Markets Board of Turkey	Users' insufficiency to adapt themselves to the applications. Inadequate internet infrastructure in Turkey.

APPENDIX D - SURVEY ON THE AWARENESS LEVEL OF ELECTRONIC SIGNATURE

Statement of Purpose

A master's thesis with a caption of "Analysis of Electronic Signature in Turkey from the Economic and Legal Perspectives and the Awareness Level in the Country" is prepared about the electronic signature concept which is the main tool for providing security and authentication in the electronic networks. This survey is prepared to provide information to the writer of thesis about the awareness level of subject in different parts of our country.

Method

Please answer questions as clear as possible. **Having no information about the subject is not a prerequisite when filling the survey.** The structure of survey is designed to cover all the parties including the ones having no information about the subject. You can add your views and your information related with the purpose stated above to the **Views** and **Additional Information** fields which are located at the end of survey.

Survey focuses on Turkish citizens who are coming from different backgrounds and who are older than 18 years and it is designed as to be completed in **5 to 10** minutes. **In the survey there is no question about defining the identities of participants.** Demographic information about age, income and job will be used anonymously for statistical purposes.

The richness and accuracy of information we requested from you will not only help to the success of master's thesis but also create a reference for other academic studies related with the usage and awareness level of electronic signature in our country in the future. We are grateful in advance for your participation and help.

Completing Survey and Submission

If you complete the survey on paper, please return it to the person who is in charge of survey. If you complete the survey in computer environment please send it to the e-mail address stated below. If you complete the survey from the webpage, no additional action is needed.

Gökhan İskender: eimza.anketi@gmail.com

1- Do you connect to the internet? ***(If your answer is "No" please continue from question 7.)***

[ ] Yes
[ ] No

2- How do you connect to the internet? (You can give multiple answers.)

[ ] From home
[ ] From workplace
[ ] From school
[ ] From internet cafes
[ ] From free access points like parks, shopping malls, etc.
[ ] From cellular phone
[ ] Other (Please explain) _____

3- What is your frequency of connecting to the internet?

[ ] Less than 1 hour in a week
[ ] Between 1 hour and 10 hours in a week
[ ] Between 10 hours and 30 hours in a week
[ ] Between 30 hours and 60 hours in a week
[ ] More than 60 hour in a week

4- Do you use online banking and trade services?

[ ] Yes
[ ] No

5- Do you use online governmental services? (like tax, examination, passport, and other applications.)

[ ] Yes
[ ] No

6- According to you, what is the level of security for the operations performed over internet?

[ ] Very secure
[ ] Secure
[ ] Indecisive
[ ] Insecure
[ ] Very insecure

7- Did you hear electronic signature concept? ***(If your answer is "No" please continue from question 15.)***

[ ] Yes
[ ] No

8- Do you have electronic certificate? ***(If your answer is "No" please continue from question 13.)***

[ ] Yes
[ ] No

9- How did you obtain electronic certificate?

[ ] Obtained from outside Turkey over internet to try
[ ] Obtained from inside Turkey over internet to try
[ ] Obtained personally without using internet
[ ] Given from institute/university in which I'm working
[ ] I developed for myself
[ ] Other (Please explain) _____

10- How do you create your electronic signature? (You can give multiple answers.)

[ ] By USB token
[ ] By smartcard
[ ] By software
[ ] Other (Please explain) _____

11- For what kind of services do you use your electronic signature? (You can give multiple answers.)

[ ] Electronic mail
[ ] Banking and online trade
[ ] Official works (like tax, examination, passport, and other applications.)
[ ] Inside organization
[ ] Other (Please explain) _____

12- Does your electronic signature contain secure electronic signature properties?

[ ] Yes
[ ] No

13- Please answer the questions below as TRUE, FALSE or NOT KNOWN. Use “T” for TRUE “F” for FALSE and “N” for NOT KNOWN.

Computer and similar tools are needed to create electronic signature.	[T]	[F]	[N]
Internet is needed to use electronic signature.	[T]	[F]	[N]
Electronic signature is used to encrypt sent messages.	[T]	[F]	[N]
Electronically signed documents can only be accessed by signatory.	[T]	[F]	[N]
Currently there is no electronic signature law in Turkey.	[T]	[F]	[N]
Changes in documents after they are electronically signed are noticed.	[T]	[F]	[N]
Time stamp clarifies validity period of electronic signature.	[T]	[F]	[N]
Representatives of legal persons can not sign documents electronically in the name of legal persons.	[T]	[F]	[N]
Electronic certificate connects identity information with signature verification data.	[T]	[F]	[N]
Only natural persons can obtain electronic certificates.	[T]	[F]	[N]
Electronic certificates are given by government.	[T]	[F]	[N]
Electronic certificates have validity periods.	[T]	[F]	[N]
Electronic certificates are free.	[T]	[F]	[N]
Electronic certificates can be obtained from certificate service providers.	[T]	[F]	[N]
Electronic certificates can not be revoked.	[T]	[F]	[N]
The legal results of secure electronic signature are same with those of handwritten signature.	[T]	[F]	[N]
All kinds of operations which can be performed by using handwritten signature can also be performed by using secure electronic signature.	[T]	[F]	[N]
Holders of secure electronic signatures shall not let third parties use their signature.	[T]	[F]	[N]
Secure electronic signature depends open public key infrastructure.	[T]	[F]	[N]
According to laws, secure electronic signature is a definite positive evidence.	[T]	[F]	[N]

14- According to you, what is the level of security for the operations performed by using electronic signature?

[ ] Very secure
[ ] Secure
[ ] Indecisive
[ ] Insecure
[ ] Very insecure

15- What is your age? ____

16- What is your gender? [M] [F]

17- What is your monthly average income?

[ ] Less than 380 YTL
[ ] Between 380 YTL and 500 YTL
[ ] Between 500 YTL and 1000 YTL
[ ] Between 1000 YTL and 2000 YTL
[ ] More than 2000 YTL

18- What is your occupation?

[ ] Government official
[ ] Private sector worker
[ ] Employee
[ ] Self-employed
[ ] Academician
[ ] Student
[ ] Retired
[ ] Unemployed
[ ] Other (Please explain) _____

19- Where do you live? _____

VIEWS

Additional views to add about subject

ADDITIONAL INFORMATION

Question Number	Additional information and explanations

Thank you for your participation.

APPENDIX E - QUESTION BY QUESTION RESULTS OF SURVEY ON THE AWARENESS LEVEL OF ELECTRONIC SIGNATURE

1. Do you connect to the internet? ***(If your answer is "No" please continue from question 7.)***

	Frequency	*Percent*	*Cumulative Percent*
Yes	600	66.2	66.2
No	307	33.8	100.0
Total	907	100.0	

2. How do you connect to the internet? (You can give multiple answers.)

From Home	*Frequency*	*Percent*	*Cumulative Percent*
No	197	32.8	32.8
Yes	403	67.2	100.0
Total	600	100.0	
From Workplace	*Frequency*	*Percent*	*Cumulative Percent*
No	180	30.0	30.0
Yes	420	70.0	100.0
Total	600	100.0	

Question 2 (continued)

From School	*Frequency*	*Percent*	*Cumulative Percent*
No	431	71.8	71.8
Yes	169	28.2	100.0
Total	600	100.0	
From Internet Cafes	*Frequency*	*Percent*	*Cumulative Percent*
No	472	78.7	78.7
Yes	128	21.3	100.0
Total	600	100.0	
From Free Access Points	*Frequency*	*Percent*	*Cumulative Percent*
No	556	92.7	92.7
Yes	44	7.3	100.0
Total	600	100.0	
From Cellular Phone	*Frequency*	*Percent*	*Cumulative Percent*
No	518	86.3	86.3
Yes	82	13.7	100.0
Total	600	100.0	
Other	*Frequency*	*Percent*	*Cumulative Percent*
No	585	97.5	97.5
Yes	15	2.5	100.0
Total	600	100.0	

3. What is your frequency of connecting to the internet?

	Frequency	*Percent*	*Cumulative Percent*
Less than 1 hour in a week	17	2.8	2.8
Between 1 hour and 10 hours in a week	114	19.0	21.8
Between 10 hours and 30 hours in a week	193	32.2	54.0
Between 30 hours and 60 hours in a week	133	22.2	76.2
More than 60 hour in a week	143	23.8	100.0
Total	600	100.0	

4. Do you use online banking and trade services?

	Frequency	*Percent*	*Cumulative Percent*
Yes	385	64.2	64.2
No	215	35.8	100.0
Total	600	100.0	

5. Do you use online governmental services? (like tax, examination, passport, and other applications.)

	Frequency	*Percent*	*Cumulative Percent*
Yes	337	56.2	56.2
No	263	43.8	100.0
Total	600	100.0	

6. According to you, what is the level of security for the operations performed over internet?

	Frequency	*Percent*	*Cumulative Percent*
Very secure	11	1.8	1.8
Secure	197	32.8	34.7
Indecisive	213	35.5	70.2
Insecure	150	25.0	95.2
Very insecure	29	4.8	100.0
Total	600	100.0	

7. Did you hear electronic signature concept? ***(If your answer is "No" please continue from question 15.)***

	Frequency	*Percent*	*Cumulative Percent*
Yes	308	34.0	34.0
No	599	66.0	100.0
Total	907	100.0	

8. Do you have electronic certificate? ***(If your answer is "No" please continue from question 13.)***

	Frequency	*Percent*	*Cumulative Percent*
Yes	30	9.7	9.7
No	278	90.3	100.0
Total	308	100.0	

9. How did you obtain electronic certificate?

	Frequency	*Percent*	*Cumulative Percent*
Obtained from outside Turkey over internet to try	10	33.3	33.3
Obtained from inside Turkey over internet to try	0	0	33.3
Obtained personally without using internet	1	3.3	36.7
Given from institute/university in which the user works	18	60.0	96.7
Developed by the user	1	3.3	100.0
Other	0	0	100.0
Total	30	100.0	

10. How do you create your electronic signature? (You can give multiple answers.)

USB Token	*Frequency*	*Percent*	*Cumulative Percent*
No	24	80.0	80.0
Yes	6	20.0	100.0
Total	30	100.0	
Smartcard	*Frequency*	*Percent*	*Cumulative Percent*
No	15	50.0	50.0
Yes	15	50.0	100.0
Total	30	100.0	
Software	*Frequency*	*Percent*	*Cumulative Percent*
No	13	43.3	43.3
Yes	17	56.7	100.0

Question 10 (continued)

Total	30	100.0	
Other	*Frequency*	*Percent*	*Cumulative Percent*
No	30	100.0	100.0
Yes	0	0	0
Total	30	100.0	

11. For what kind of services do you use your electronic signature? (You can give multiple answers.)

Electronic Mail	*Frequency*	*Percent*	*Cumulative Percent*
No	13	43.3	43.3
Yes	17	56.7	100.0
Total	30	100.0	
Banking and online trade	*Frequency*	*Percent*	*Cumulative Percent*
No	25	83.3	83.3
Yes	5	16.7	100.0
Total	30	100.0	
Official works	*Frequency*	*Percent*	*Cumulative Percent*
No	26	86.7	86.7
Yes	4	13.3	100.0
Total	30	100.0	
Inside organization	*Frequency*	*Percent*	*Cumulative Percent*
No	17	56.7	56.7

Question 11 (continued)

Yes	13	43.3	100.0
Total	30	100.0	
Other	*Frequency*	*Percent*	*Cumulative Percent*
No	27	90.0	90.0
Yes	3	10.0	100.0
Total	30	100.0	

12. Does your electronic signature contain secure electronic signature properties?

	Frequency	*Percent*	*Cumulative Percent*
Yes	9	30.0	30.0
No	21	70.0	100.0
Total	30	100.0	

13. Please answer the questions below as True, False or Not Know.

N = 308	*True*	*False*	*Not Know*
Mean	5.83	3.25	10.92
Median	5.00	3.00	11.00
Mode	7	2	12
Std. Dev.	4.022	2.609	5.462
Variance	16.173	6.809	29.836
Range	20	12	20

Question 13 (continued)

Minimum	0	0	0
Maximum	20	12	20

14. According to you, what is the level of security for the operations performed by using electronic signature?

	Frequency	*Percent*	*Cumulative Percent*
Very secure	29	9.4	9.4
Secure	102	33.1	42.5
Indecisive	160	51.9	94.5
Insecure	17	5.5	100.0
Very insecure	0	0	100.0
Total	308	100.0	

15. What is your age?

N = 907		**N = 600**		**N = 308**	
Mean	33.68	Mean	31.16	Mean	30.65
Median	32.00	Median	28.00	Median	28.00
Mode	28	Mode	28	Mode	26
Std. Dev.	10.974	Std. Dev.	9.007	Std. Dev.	8.449
Variance	120.426	Variance	81.127	Variance	71.389
Range	61	Range	47	Range	40
Minimum	18	Minimum	18	Minimum	18
Maximum	79	Maximum	65	Maximum	58

16. What is your gender?

Gender	*Frequency*	*Percent*	*Cumulative Percent*
Male	583	64.3	64.3
Female	324	35.7	100.0
Total	907	100.0	

17. What is your monthly average income?

Income (Whole Population)	*Frequency*	*Percent*	*Cumulative Percent*
Less than 380 YTL	120	13.2	13.2
Between 380 YTL and 500 YTL	108	11.9	25.1
Between 500 YTL and 1000 YTL	238	26.2	51.4
Between 1000 YTL and 2000 YTL	246	27.1	78.5
More than 2000 YTL	195	21.5	100.0
Total	907	100.0	

Income (308 People Who Heard Electronic Signature Concept)	*Frequency*	*Percent*	*Cumulative Percent*
Less than 380 YTL	28	9.1	9.1
Between 380 YTL and 500 YTL	38	12.3	21.4
Between 500 YTL and 1000 YTL	62	20.1	41.6
Between 1000 YTL and 2000 YTL	116	37.7	79.2
More than 2000 YTL	64	20.8	100.0
Total	308	100.0	

18. What is your occupation?

Job	*Frequency*	*Percent*	*Cumulative Percent*
Government Official	192	21.2	21.6
Private Sector Worker	173	19.1	40.7
Employee	53	5.8	46.5
Self-employed	110	12.1	58.7
Academician	54	6.0	64.6
Student	142	15.7	80.3
Retired	41	4.5	84.8
Unemployed	62	6.8	91.6
Other	76	8.4	100.0
Total	907	100.0	

19. Where do you live?

City	*Frequency*	*Percent*	*Cumulative Percent*
Adana	9	1.0	1.0
Adıyaman	1	0.1	1.1
Afyon	6	0.7	1.8
Ağrı	4	0.4	2.2
Amasya	6	0.7	2.9
Ankara	302	33.3	36.2
Antakya	1	0.1	36.3

Question 19 (continued)

Antalya	31	3.4	39.7
Artvin	1	0.1	39.8
Aydın	7	0.8	40.6
Balıkesir	3	0.3	40.9
Bandırma	1	0.1	41.0
Bartın	1	0.1	41.1
Batman	4	0.4	41.6
Bayburt	2	0.2	41.8
Bilecik	1	0.1	41.9
Bolu	8	0.9	42.8
Burdur	2	0.2	43.0
Bursa	15	1.7	44.7
Çanakkale	6	0.7	45.3
Çankırı	8	0.9	46.2
Çorum	7	0.8	47.0
Denizli	7	0.8	47.7
Düzce	1	0.1	47.9
Edirne	5	0.6	48.4
Erzurum	25	2.8	51.2
Eskişehir	15	1.7	52.8
Gaziantep	25	2.8	55.6

Question 19 (continued)

Gümüşhane	1	0.1	55.7
Hakkari	5	0.6	56.2
Hatay	4	0.4	56.7
Isparta	1	0.1	56.8
İstanbul	130	14.3	71.1
İzmir	49	5.4	76.5
İzmit	3	0.3	76.8
Kahramanmaraş	4	0.4	77.3
Karabük	4	0.4	77.7
Kars	5	0.6	78.3
Kayseri	3	0.3	78.6
Kilis	3	0.3	78.9
Kırıkkale	8	0.9	79.8
Kırklareli	1	0.1	79.9
Kırşehir	3	0.3	80.3
Kocaeli	5	0.6	80.8
Konya	30	3.3	84.1
Kütahya	1	0.1	84.2
Lüleburgaz	1	0.1	84.3
Malatya	2	0.2	84.6
Manisa	5	0.6	85.1

Question 19 (continued)

Mardin	3	0.3	85.4
Mersin	12	1.3	86.8
Muğla	3	0.3	87.1
Muş	3	0.3	87.4
Nevşehir	3	0.3	87.8
Niğde	6	0.7	88.4
Ordu	7	0.8	89.2
Osmaniye	1	0.1	89.3
Sakarya	5	0.6	89.9
Samsun	5	0.6	90.4
Siirt	3	0.3	90.7
Sinop	1	0.1	90.8
Sivas	6	0.7	91.5
Şanlıurfa	2	0.2	91.7
Şırnak	2	0.2	92.0
Tekirdağ	5	0.6	92.5
Tokat	6	0.7	93.2
Trabzon	23	2.5	95.7
Uşak	1	0.1	95.8
Van	5	0.6	96.4
Yalova	3	0.3	96.7

Question 19 (continued)

Yozgat	2	0.2	96.9
Zonguldak	28	3.1	100.0
Total	907	100.0	