E-commerce security

Instructor Serdar CANBAZ*

Abstract

The new economy and information age, which started to change most values in human lives, made it easier to reach and share information.

Through World Wide Web, the internet, having appeared and desired to be used as a means for trade, the term "electronic commerce" has been coined.

The electronic commerce, resulting from development in information and communication technologies, has some problems, both in national and international context. It has brought its own legal, managerial and technical problems stemming from widespread use.

There are numerous problems caused by electronic commerce, both nationwide and worldwide. Especially the mutual trust problem between parties is an important problem. That is, during data exchange in trade there is the risk of third parties to access and misuse that data.

The aim of this paper is to find out problems in secure electronic trade and review the literature on the basis of precautions and reveal the practical side of those precautions.

Key words: E-commerce, Electronic trade, security, information, communication.

Introduction

The internet, with rapidly developing technology and information era, made it easier to reach information with low costs. Fast, easy and cost efficient information sharing has become an inevitable part of daily life and companies made their use of this.

Globalization, information era and developing internet technology has given investors an opportunity for virtual investment. Data sharing through internet has approached further and led to the birth of concepts like e-trade (electronic trade), e-jobs, e-state and e-society.

Those new concepts have come with their own problems. For the participation to e-commerce, security concerns of both parties have formed the most important problem.

In the present paper, information about e-commerce has been given; then security concerns have been analyzed and solutions to those, with recent examples have been proposed and then concluded.

1. The development of information era and the new world with technology

When we look into information and development we see Julius Reuter in 1850 who started his job with information. He succeeded sending information with pidgins and proved that information is a merchandise too[1].

It is accepted that the information era has started in the last quarter of the 20th century and the capital replaced by access to information and communication technologies[2]. The new world, formed by globalising markets, information technologies and computing systems, has given way to new work, life and trade styles. Thus, a new social and economic system "The New Economy" has come to life[3].

Computers, made previously difficult-to-perform processes easier. Therefore, companies are trying to adapt themselves to make use of innovations brought by technology[4].

---

* Kırklareli University, Babaeski Vocational Scholl

[1] http://www.deltur.cec.eu.int/kitap/bilgitop.html, Access Date 15.04.2006

[2] Adem Özbay, Jan Devrim, *E-Ticaret Rehberi*, Bilgi Teknolojileri Dizisi 7, Hayat Yayınları, İstanbul, 2000, s. 20

[3] M. Emre Civelek, Edin Güçlü Sözer, *İnternet Ticareti, Yeni Ekososyal Sistem ve Ticaret Noktaları*, Beta Basım Yayım Dağıtım A.Ş., İstanbul, 203, s. 41-42

[4] Şule Özmen, *Ağ Ekonomisinde Yeni Ticaret Yolu, E-Ticaret*, İstanbul Üniversitesi Yayınları, İstanbul, 2003, s. 5

In old economies, data transfer (cash, cheque, invoice, meeting etc.) was done through physical means; in the new economy, all kinds of data are transferred digitally. Information, stored in computers in 0 and 1 digit system, is transferred in the speed of light[5]. At present, information is transferred so quickly and easily that, although the source and receiver are in different continents, they look as if they are together[6].

In the beginning of the 21st century, mainly in small units and the internet, information economics has come to life. On the base of this economy, there lie knowledge and correspondence instead of natural resources and physical labor[7]. Information technologies, being inevitable in acquiring, processing and managing knowledge, has led the new social stage to be called "information society"[8]. In the industrial society, the strategic source was "capital" but in the information society "knowledge" replaced this main strategic source. Information producers tend to make the main line on society and "information workers" became of an increasing importance. Organizations using knowledge in technology systems extended their life span[9].

Innovations and improvement in technology have become obvious in many fields, especially in economics, and affected economic life, work life, business processes of companies, ways of businesses, business rules, organizational structures, managerial approaches, decision making and many more concepts[10].

Through internet, which formed the basis of new economics coming with information era, many businesses, work styles and concepts were derived. Electronic jobs, electronic commerce, electronic marketing, virtual workplace, virtual teams and virtual organizations can be given as examples[11].

2. Electronic commerce

Including[12] the trade of merchandise and services, promotion, advertising, logistics, electronic customs, insurance, documentation, corporal management; civil purchasing, e-money, stock exchange, e-payment, digital signature and electronic notary, electronic commerce[13] has been defined by international organizations as follows[14]:

According to World Trade Organization (WTO), it is the production, advertising and distribution of merchandise or services through telecommunication networks[15].

According to the Organization for Economic Cooperation and Development (OECD), it is all trade activities, based on processing and spreading digitalized written text, sound and images, relating to people and companies[16].

According to United Nations – Centre for Trade Facilitation and Electronic Business (UN – CEFACT), sharing business information, structured or unstructured, for business, management and consuming activities, among producers, consumers and civil organizations through electronic means (such as e-mail and messages, electronic billboards, world wide web technology, smart cards, electronic funds transfer, electronic data exchange etc.)[17].

---

[5] Don Tapscott, *Dijital Ekonomi*, Koç Sistem Yayınları, İstanbul, 1998, s. 6
[6] Selçuk Burak Hasıloğlu, *Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri*,Türkmen Kitabevi, İstanbul, 1999, s. 21
[7] Özbay v.d., E-Ticaret Rehberi, s. 20
[8] Hasıloğlu, Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri, s. 26-27
[9] Hasıloğlu, Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri, s. 23
[10] Özmen, E-Ticaret, s. 6
[11] Ali Deniz Akkirman, *Sanal İşyerinde Örgütsel Davranış*, Aktüel Yayınları, İstanbul, 2004, s. 36
[12] Umut Mehmet Yürüyen, *Deniz-Ticaretinde Elektronik Satış Yönetimi,* Dokuz Eylül Yayınları, İzmir, 2003, s. 24
[13] Nevzat Erdağ, Emel Batuman, *Elektronik Ticaret El Kitabı*, Bilgi Serisi : 5, Arıkan Basım Yayım Dağıtım Ltd. Şti., Denizli, 2006, s. 27
[14] Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 22-23
[15] Marc Bacchetta, Patrick Low, Aaditya Mattoo, Ludger Schuknecht, Hannu Wagerand Madelon Wehrens, *Electronic Commerce and The Role of The WTO*, WTO Publications, Switzerland, 1998, s. 5
[16] Nusret Ekin, *Bilgi Ekonomisinde E-Ticaret*, İTO Yayınları, Yayın No:1998-61, İstanbul, 1998, s. 77
[17] Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 23

Electronic commerce can be defined as, trading information, product or services through information networks[18].

Electronic trade has been defined by Electronic Trade Coordination Committee Legal Working Group Report in May 1998 as: individuals' or organizations', all trade activities aiming to create a value based on processing, transferring and keeping written, audial or visual information through open or closed networks that can be used by limited number of users or fully open networks[19].

Another definition says that, electronic commerce is, all activities, related to individuals and organizations, processing digital data such as sound, video, text etc. through standard communication means without the need for physical exchange where both parties can communicate aiming to create a value[20].

Based on the above definitions, electronic commerce can be defined as, "the production, advertising, trading, paying for and distributing the products trough computer networks"[21].

2.1. Types of electronic commerce

Electronic trade can be classified into the following categories:

- Business to Consumer (B2C) [22]
- Business to Business (B2B) [23]
- Citizen to State Organizations (KPDS, ÜDS, ÖSS etc.) [24]
- Companies to State Organizations (SGK, Civil Entrusting etc.) [25]
- State to State[26].

2.2. Electronic trade tools

There are six tools in electronic trade. These are,

- Telephone
- Fax
- Television
- Electronic payment and money transfers
- Electronic data interchange (EDI)
- Internet[27].

Among the above, internet is considered to be the most efficient tool in electronic commerce, being low-cost, fast and convenient in processing audial, visual and written data[28]. Electronic trade is mostly regarded as done on the internet or other networks, and discussions are mainly in this range[29].

However, it is clear that it would be insufficient to regard electronic commerce as only done on the internet or by a website. In fact internet trade is only a part of electronic trade[30].

A company aiming to trade through internet should first have a web site. To have a web site, the requirements are:

a. Domain name registration,
b. Web site design,
c. Technical basis formation,
d. Payment system formation.

---

[18] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[19] Veysel Bozkurt, *Elektronik Ticaret*, Alfa Yayınları, İstanbul, 2000, s.200
[20] Erdağ vd., Elektronik Ticaret El Kitabı, s. 2
[21] Selda Ene, *Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama*, Pusula Yayıncılık, İstanbul, 2002, s.2
[22] Billur Yaltı, *Elektronik Ticarette Vergilendirme*, Der Yayınları, İstanbul, 2003, s.9
[23] Bozkurt, Elektronik Ticaret, s. 65
[24] Erdağ vd., Elektronik Ticaret El Kitabı, s. 11
[25] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 11
[26] Özbay v.d., E-Ticaret Rehberi, s. 41
[27] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 4
[28] Bozkurt, Elektronik Ticaret, s. 101
[29] Özbay v.d., E-Ticaret Rehberi, s. 20,21,35
[30] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 4

In this process, the organization has to register the company's or the brand's domain name, design its website in a convenient way and form its technical basis and payment system[31].

2.2.1. Electronic payment and money transfer systems

Electronic payment is to pay by phone, computer networks or other digital means. For money transfer, on-site-payment, automated teller machines (ATM), money order etc. were previously used. At present, with the technological developments, various payment tools such as credit cards, debit cards, smart cards, electronic wallet, electronic money (www.cybercash.com and www.digicash.com), electronic cheque (www.fstc.org and www.echeck.org), Electronic Funds Transfer (EFT), Virtual POS, Mail Order, Escrip, IPIN, PCPay, ECharge, My Phone, First Virtual, E-Mobil/M-Pay and PayPal (www.paypal.com) have been formed[32].

Among all means for payment, credit cards, due to their widespread use, high standards and opportunity for on-line use, are the best choice for electronic commerce[33]. Developed as a tool to replace cash payment, credit cards have become the main payment tool for electronic commerce. Credit cards helped electronic trade to develop at least as the internet itself. However, there are criticisms towards paying through credit cards; especially on the basis of security there are heavy criticisms and worries. Carrying the risk of data theft and misuse, electronic commerce is heavily criticized[34].

2.2.2. Electronic data interchange-edi)

Stemming from the need of civil and private sector organizations for effective communication, electronic data interchange is a system for information and document exchange between two organizations, through computer networks without human factor[35]. International traders, carriers, commissioners, banks, insurers, customs managements, trading firms and other related civil organizations join this process[36]. Electronic data interchange, helps all parties reach information, shortens the process and prevents repetition and possible errors[37].

2.2.3. Internet

The word "internet" is the short version of the English origin "Interconnected Network" phrase[38]. Internet is a global network which has no beginning, end, limit or director[39].

The starting point of internet is The US Ministry of Defence's Advanced Research Project Agency (ARPA) founded in 1957, after Russia's sending the Sputnik to space[40]. ARPA[41] was founded to enable US forces to manage war, and before or during war, command ballistic missiles even if all the communication channels destroyed[42].

---

[31] Civelek v.d., İnternet Ticareti, s. 173-178
[32] Civelek v.d., İnternet Ticareti, s. 174-178
Ekin, Bilgi Ekonomisinde E-Ticaret, s. 86
Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 15-16
Erdağ vd., Elektronik Ticaret El Kitabı, s. 70-71
Hasıloğlu, Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri, s. 102-103
Özbay v.d., E-Ticaret Rehberi, s. 52-54
Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 195
http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date: 20.05.2006
http://www.paypal.com, Access Date: 26.06.2010
[33] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date: 20.05.2006
[34] Bozkurt, Elektronik Ticaret, s. 105-106
[35] Bozkurt, Elektronik Ticaret, s. 106
[36] Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 30
[37] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 5-6
[38] Yaltı, Elektronik Ticarette Vergilendirme, s. 40
[39] PC World Dergisi Eki, *İnternet El Kitabı*, Ilıcak Matbaacılık A.Ş., Aralık 1996, İstanbul: s. 5
[40] Robert Spector, *amazon.com Get Big Fast*, HarperCollins Publishers Inc., New York, 2002, s. 2
[41] Hasıloğlu, Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri, s. 44
[42] Spector, amazon.com Get Big Fast, s. 2

In 1969 ARPANET[43] network formed the basis of internet and through time, trading companies discovered that they could use this network for their trading activities. Thanks to trading activities, the INTERNET (network of networks) expanded and became popular all over the world[44].

The internet, got rid of the strictly controlled Pentagon structure and became an open, transparent and plain organization. Internet has no owner; also, there is no authority operating, managing and controlling it. Internet, having been designed as a platform to communicate information freely and continuously, was planned in the form of a general flexible basis on which all kinds of applications could be done[45]. Through the internet[46], allowing millions of interconnected computers transfer files and data, one can do shopping, go through music archives, communicate with people from different countries in written, audial and/or visual forms[47].

To make connection among computers, "a common computing language" named Transmission Control Protocol / Internet Protocol (TCP/IP)[48] is used[49]. Other than TCP/IP, File Transfer Protocol (FTP) is used for transferring files; Hypertext Transmission Protocol (HTTP) is used for written, audial, visual and other graphical content[50]. As long as compatible with TCP/IP, any computer can connect to the internet, and if signals available, it is possible to connect to the internet even from space[51].

Since the early years of internet's birth, e-mails are a widely used service[52]. It allows users to send text, audio, images etc. fast and for low costs[53]. At present, intra-corporal communication, sending meeting records, intra-corporal correspondence, sending data and information is done on the internet[54]. E-mails are one of the most effective ways of reaching the customers and perform sales. It allows reaching to present or potential customers[55]. From this point, internet is an essential element in electronic commerce.

Using the electronic marketing, once a user is signed up to the web site, new products are advertised to that customer or within the announcement activities, advertorial messages can be sent to many e-mail addresses[56].

Making use of the internet tools for internal communication is called "intranet"[57]; and with user identities and passwords given to contacts through companies, using the internet for correspondence and performing trade activities with customers, partners and other parties which are all over the world, is called "extranet"[58].

3. Security concerns in electronic trade

Global information infrastructure should be cleared from all risks and be trusted. If users are not sure that the internet communication is safe for data, internet trade would not be successful[59].

Personal or financial data can be obtained by third parties and both sides may lose control over each other's identities, resulting in many problems. Security concerns stemming from internet trade, come

---

[43] A. Selami Güleç, Azmi Yalçın, *Elektronik İstila*, İstanbul: Nobel Kitabevi, 2003, s. 8
[44] http://www.internetmarketing-tr.com/info/info-0001.htm, Access Date 15.03.2006
[45] http://www.superonline.com/hukuk/hukuk.htm, Access Date 18.05.2006
[46] Allen Douglas, Steve Johnson, *İnternet Öğrenim Kılavuzu*, Alfa Basım Yayın Dağıtım A.Ş., İstanbul, 1998, s. 2
[47] Zülkif Güven, Burhan Deniz, *Bilgisayara Giriş*, Sürat Yayınları, İstanbul, 1998, s. 174
[48] Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 31
[49] Ali İhsan Bülbül, *Bilgisayara Giriş*, Bayrak Matbaacılık, 2. Baskı, İstanbul, 2003, s. 373
[50] Hakkı Öcal, *İnternet Tasarım Rehberi*, Byte Türkiye Dergisi Ekim 1998 Eki, İhlas Matbaacılık, Gazetecilik, Yayıncılık A.Ş., İstanbul, 1998, s. 4
[51] http://www.superonline.com/hukuk/hukuk.htm, Access Date 18.05.2006
[52] Hasıloğlu, Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri, s. 53
[53] Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 41
[54] Akkirman, Sanal İşyerinde Örgütsel Davranış, s. 32
[55] Özmen, E-Ticaret, s. 138
[56] Civelek v.d., İnternet Ticareti, s. 180
[57] Coşkun Dolanbay, *E-Ticaret Strateji ve Yöntemleri*, Meteksan Sistem Yayınları, Ankara, 2000, s. 15
Akkirman, Sanal İşyerinde Örgütsel Davranış, s. 33
[58] Hasıloğlu, Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri, s. 74-75
Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 36
[59] William J. Clinton Albert Gore, *Global Elektronik Ticaret*, Çev: Veysel Bozkurt, Alfa Yayınları, İstanbul, 2000, s.27

from problems caused by the above reasons[60]. In electronic trade, both sides perform activities without seeing each other; so they want to ensure trust, being mutually sure about identities. Stemming from this need, digital signature and digital certificates have come to practice[61].

Another issue which should be taken into consideration is the risk of credit card etc. details obtained by others, and the worry, the customers feel when they have to give their personal details while shopping[62]. The risk of data to be obtained while being transferred by the internet, is not less than the risk on the phone. Ways of shopping such as phone/mail-order, and other internet applications, which do not require the credit card to physically pass through a POS machine, carry the risk of credit card number, expiry date and CV2 obtained by others and used for shopping[63]. Therefore, many card holders are deeply concerned about security and although they need it, they prefer to stay distant to internet operations. To prevent personal data being stolen by others, is of a great importance for internet trade[64]. For ensuring safe data transfer, applications based on encoding information, such as SSL, SET, 3D SET, HALF SET and 3D SECURE have been developed[65].

3.1. Encryption techniques used in electronic trade

Encryption is encoding information to prevent it from being taken before it reaches the actual receiver, using various mathematical algorithms and encoding keys[66]. Encryption techniques widely used on the internet are mainly "public key" which is asymmetrical and "private key" which is symmetrical[67].

3.1.1. Public and private key cryptography

Private key cryptography is a technique based on a single key which is used between the user and internet site owner.

In SET protocol, known as Asymmetric Cryptography, public key encryption is used and data can only be read by the receiver. In this cryptography, both public and private key cryptography can be used. Derived by a public key, this cryptography can only be decoded with the private key. On the other hand, a cryptogram derived by a private key can be decoded by all public keys. Public key encryption ensures the keeping of data and proves the correctness of it to both sides[68].

3.1.2. Des and rsa

Data Encryption Standard (DES) is a widely used way of encryption. In DES method, 72 quadrillion encryption keys are used. In this method, for each encryption, a single key is randomly selected and the code can be decoded only by the receiver holding the same private key.

Another internet encryption technique is RSA, which was developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. In this technique, there is an algorithm, making calculations among great prime numbers producing public and private keys[69].

3.1.3. Biometrics

With the improvement in the science of analyzing human's biologic characteristics, identifying people's identity has become possible[70]. Here, in the field of internet security, computers analyze those characteristics and identify users. Biometrics technique is based on identifying human's fingerprints, voice, eyes, hand and body shapes and other typical physical characteristics[71].

---

[60] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[61] http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
[62] E.W.T. Ngai, F.K.T. Wat, "A literature review and classification of electronic commerce research,", *Information & Management, Elsevier Science B.V.*, n: 39, 2002, s. 418
[63] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[64] http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
[65] Özbay v.d., E-Ticaret Rehberi, s. 52
[66] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[67] Yürüyen, Deniz-Ticaretinde Elektronik Satış Yönetimi, s. 44
[68] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[69] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[70] Civelek v.d., İnternet Ticareti, s. 229
[71] http://bm-dergi.emo.org.tr/index.php?option=com_content&task=view&id=32&Itemid=74, Access Date 15.03.2006

A computer company, HP, has mounted a fingerprint reader to its lap-top computers and made it possible for the computers to identify users[72]. Vakıfbank BioŞifre (Vakıfbank BioCode) and İş Bankası Biyokimlik (İş Bankası BioIdentity) are two of those techniques used by those banks in some of their ATMs[73]. Although biometrics is a high-cost technique, it is assumed that it will be widely used in the future[74].

3.2. Digital signature

It is possible to secure data by "digitally signing" it. Thus, it aims to prevent any other parties to reach data, which is subject to internet operations. This helps identity, confidentiality, content of message kept in secret and avoids refusability. Any record attached to an electronic data and has a logical relation to it, is called electronic signature. It can be derived electronically, optically etc., and can be carried or kept, being used for identity verification[75].

Electronic signature's legal basis and technical specifications have been defined in the Electronic Signature Law dated 15.01.2004, with entry 5070. For overcoming limitations, ensuring the raising volume of trade and its security, electronic signature is an important development. By ensuring secure trade medium, participation to electronic trade will increase[76].

Through recent legislations, electronic signature has gained equal status with the real signature and became legally accepted. However, in formal and specially performed legal operations and in back bonds electronic signature is not valid. Electronic data formed with electronic signature is considered a bill and unless otherwise proved it is accepted as a legal proof[77]. Moreover, electronic signature falsification and using it without legal permission results in fine or imprisonment[78].

Turkish Science Foundation started the e-Trust project based on mobile electronic signature, with the aim of making electronic signature use easier and widespread. By the help of mobile electronic signature, GSM users will be able to perform e-state, e-jobs, e-trade and m-trade operations. On the computer, with a single password, mobile electronic signature can be safely and conveniently used for identification in banking, applications, and public applications[79].

3.3. Digital certificate

Like the real signatures in daily life, digital signatures are used for identification of the sender of any data. To form and verify a digital signature, digital certificates are used. For signing a received data, a digital certificate by the sender is needed.

Digital certificate or digital identity, electronically correspond to passport, driving license or identity cards used in daily life. Digital certificate is developed to be submitted electronically for proving the right to reach the identity of a person or an on-line service. Digital certificates connect an electronic key and identity information used for encoding or decoding digital information. Digital certificate ensures users' or organizations' information to be circulated through the communication channels safely[80].

From the internet banking to on-line shopping, security has become an increasingly important concern. Passwords are not any more sufficient to control access, and digital certificates provide a more secure way to do so. In a digital certificate there is a key belonging to the certificate owner, username, expiry date, a serial number and the organization from which the certificate was taken[81].

---

[72] Aydın Türkmen, "*Sahibini Tanıyan Laptop Üretildi*" Güneş Gazetesi 26 Şubat 2006, s. 16
[73] http://www.vakifbank.com.tr/biosifre.aspx, Access Date 15.08.2010
http://www.isbank.com.tr/content/TR/Guvenlik/Biyokimlik-987-292.aspx, Access Date 15.08.2010
[74] http://www.activefinans.com/activeline/sayi8/biometri.html, Access Date 18.06.2006
[75] Bozkurt, Elektronik Ticaret, s. 200
[76] http://www.ymm.net/e-ticaret/e-imza.htm, Access Date 12.04.2006
[77] http://www.ymm.net/e-ticaret/elektronik_imza_kanunu.htm, Access Date 12.04.2006
[78] http://www.ymm.net/e-ticaret/e-imza.htm, Access Date 12.04.2006
[79] http://www.e-guven.com/default.asp, Access Date 15.08.2010
[80] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[81] http://www.globalsign.com.tr/destek/dijital_sertifika_body.asp, Access Date 20.02.2006

Organizations giving and managing certificates are called certification organizations. Digital certificates are signed by those organizations' secret keys. Digital certificates can be obtained from organizations such as GlobalSign and VeriSign. Once the information about the certificate applier reaches the providing organization, application is automatically put into process and certificates are transmitted electronically[82].

3.4. Security standards in e-commerce

Security standards, based on encoding information during data flow between the user, company and bank, ensure safety and scrutiny even if the data is obtained by others[83].

To ensure security for transmitted data between the user and receiver, SSL (Secure Socket Layer), SET (Secure Electronic Transaction), PAP/CHAP (Password Authentication Protocol/Challenge Handshake Authentication Protocol), PCT (The Private Communications Technology), S/MIME (The Secure Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy) are used. SSL and SET are most widely used safety standards[84].

3.4.1. Ssl (secure socket layer) protocol

SSL[85], having an important role in today's electronic trade and business applications, was developed by Netscape Communications in 1995 to ensure safety in data transfer; working on the TCP/IP protocol, it is a programme layer protecting the data transfer between web browser and server[86].

It ensures the sent data be decoded only at the right address. The data is encoded automatically before being sent and can be decoded by the receiver only. If the data is damaged by third parties before it reaches the receiver, both the sender and receiver are informed of this damage[87]. Both parties verify the data and thus keep the security and scrutiny. SSL, uses digitally signed certificates[88].

When shopping from virtual shop using SSL security protocol, there is no need to apply for certificate. Most web browsers use SSL[89]. If desired to trade through internet, to make the internet site secure for access, one should apply to verisign.com for SSL Security Certificate and load the site to the web server as a module[90].

For a web server to make SSL connection with its users, an e-identity is needed. A user signing in to a secure site, sees that the URL starts with "https:" and makes sure that the site is secured with SSL[91]. The server introduces itself through sending its e-identity to the user. If the e-identity of the server is valid and the e-identity of the certification organization, which certifies the user's browser, is recognized, the browser informs the user about connecting to a secure site. All data between the server and the browser is encoded to prevent third parties read the message. To prevent possible alteration while transmitted, encoded message is digitally signed and sent or received with this signature. SSL/Server Identity Verification aims to prove the user that s/he is connected to the right site and that the data sent can be read only by the server[92]. SSL uses a mechanism where both the sender and the receiver recognize each other. Thus, it is ensured that the data is sent by the right server and received by the right user[93].

The mutual identification between computers is ensured by a technique based on public – private key encryption[94]. In this system, there is a couple of keys. The public key can be seen by everyone and is

---

[82] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[83] http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
[84] Abhijit Chaudhury, Kuıboer Jean-Pierre, *E-Business and ECommerce Infrastucture: Technologies Supporting The e-Business Initisative*, McGraw-Hill Higher Education, U.S.A., 2002, s. 161-165
[85] Özmen, E-Ticaret, s. 217
[86] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 57
[87] http://sertifika.bilten.tubitak.gov.tr/net/teknik/SSL.jsp, Access Date 04.02.2006
[88] http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
[89] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[90] Özmen, E-Ticaret, s. 217
[91] Özbay v.d., E-Ticaret Rehberi, s. 57
[92] http://sertifika.bilten.tubitak.gov.tr/net/teknik/SSL.jsp, Access Date 04.02.2006
[93] Özbay v.d., E-Ticaret Rehberi, s. 56
[94] Bozkurt, Elektronik Ticaret, s. 200

used for encoding the sent message (Indeed, here, they key is an algorithm of encryption and encoding. This algorithm encodes the message to be sent.). The message encoded by the public key can only be opened (decoded) by the paired private key. Thus, with the private key, being known only by you, security is ensured. For instance, you send your own public key to someone who wants to send you a message. That person encodes his message with that key and sends it (the message) to you. The sent message can only be decoded with a second key (private key) and you are the only one who knows it[95].

During SSL connection, in all pages, all data coming from the server should be checked for security. Web sites' security information gives the opportunity to control server's e-identity. If another server's identity is found, the connected server is not the desired one and the security is under threat[96].

Another opportunity that SSL gives, is the sending of the user's e-identity to the server and introducing it. In SSL/User Identity Verification process, server introduces itself to the user and wants the user to introduce himself. For this, the user needs to have an e-identity. Some settings on the server side can help select who of the e-identity holders can access the site[97].

The effectiveness of encoding data flow depends on key length. Key length is of a great importance to protect data. For instance, 8 bit transmission is very easy. Bit means a number in dual numbering system[98]. One bit can represent two values, which are "0" or "1". 8 bits contain 256 different keys. A computer can analyze 256 possibilities in a linear order and solve the key. In SSL protocol, 40 bit, 56 bit and 128 bit encoding is used. In 128 bit encoding there are 2128 different keys and solving this key needs long time and high cost[99]. Moreover, a key is used only once and then disposed. Even if a code is broken during a session, for the next session a new key will be used; so the one who breaks a single code, cannot see another session[100]. Because of this, 128 bits SSL encoding provides a high level of security[101].

In web servers where SSL traffic is dense, additional applications are needed to speed up the SSL connections one of which is Luna SA[102]. Capable of distant management and external identity management, Luna SA provides servers scaled hardware accelerating digital signing performance. It is a flexible Ethernet attached hardware security module providing strong cryptographic acceleration and ensuring hardware key management and multiple configuration profiles[103].

3.4.2. Set (secure electronic transfer) protocol

Developed by a consortium consisting of Visa, Mastercard, Microsoft, Netscape, GTE, IBM, SAIC, Terisa Systems and Verisign, SET has become an industrial standard for data safety for banking cards and payments[104]. The first SET compatible shopping was performed in 1997 in San Francisco, USA. In Turkey, in 1997, Garanti Bank used the first SET compatible protocol in shopping[105].

SET protocol uses a set of public key, DES, RSA encryption methods[106]. Moreover, virtual portfolio and certificate make on-line shopping more secure. SET guarantees the scrutiny of payment and that the card holder is authorized for use and the seller has an agreement with the bank[107].

In set system, provision starts with customer's shopping selection. Then, customer's virtual portfolio and seller's virtual POS (V-POS) are controlled. After this, the virtual POS transmits shopping amount and credit card certification data to the bank. The bank gives provision without seeing the content

---

[95] Özbay v.d., E-Ticaret Rehberi, s. 56-57
[96] http://sertifika.bilten.tubitak.gov.tr/net/teknik/SSL.jsp, Access Date 04.02.2006
[97] http://sertifika.bilten.tubitak.gov.tr/net/teknik/SSL.jsp, Access Date 04.02.2006
[98] http://www.e-cicek.net/guvenlik.asp, Access Date 21.04.2006
[99] Özmen, E-Ticaret, s. 217-218
[100] http://www.e-cicek.net/guvenlik.asp, Access Date 21.04.2006
[101] http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
[102] http://www.gestocomm.cz/data/datasheets/Luna_CA3.pdf, Access Date 12.05.2006
[103] http://www.infonet.com.tr/tr/products/Rainbow/lunasa.htm, Access Date 12.05.2006
[104] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[105] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[106] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 59
[107] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006

(What is bought? How many/much bought? etc.). The virtual seller waits for provision from the bank without seeing the credit card information of the customer and after receiving provision, sends the merchandise[108].

All parties subject to SET system (customer, seller, credit card company) know each other and this can be proved. The identification process is done through a digital certificate as in SSL. All sides in the payment process use their own digital certificates[109].

Together with the card holder and the seller, SET, involves the issuer bank, acquirer bank, and is accepted as a broad payment protocol which proves all parties participating in the on-line shopping process. Also it prevents credit card information be seen by the seller[110].

SET system, as in SSL, is based on encoding and sending data between seller and bank. For using this system, a SET compatible card is required. Card holders who want to use SET protocol have to meet two prerequisites; first they must have certificates given by Certificate Authority for each card. Then they must take a "virtual portfolio" programme from the bank and install it to their computer. After the installation they must sign up their cards to the programme. SET compatible shopping can be done on a computer in which the virtual portfolio is installed and from the sellers within the SET protocol. Although SET protocol is more secure than SSL, it is not as widely used as SSL because it needs a special software. Virtual shops, on the other hand, can start safe trading after installing V-POS and taking digital certificate (from www.verisign.com or www.gte.com) [111].

3.5. 3d set and half set

3D SET is based on a structure known as Three Domain Model[112]. These domains are called Acquirer Domain (the authenticity of the shop), Issuer Domain (card holder and card authenticity) and the Interoperability Domain (interchange of process information using a common protocol) [113].

The main difference of this from SET is that the software and certificate of the card holder is stored by the issuer bank; and the seller software and certificate is stored by the POS owner bank[114].

Half SET on the other hand, is a payment system where data between card owner and seller is submitted through SSL and the data between seller and bank is submitted through SET protocol[115].

3.6. Security examples in e-commerce in Turkey

In Turkey, at present, in addition to the above measures, additional precautions are taken. These are Virtual Credit Card, 3D Secure and CodeSure.

3.6.1. Virtual credit card

Banks succeeded in developing a virtual credit card which enabled secure shopping and prevented unauthorized shopping, thus, solved the objection problem with traders. The credit limit of the virtual card is "zero". Before shopping with the virtual card, one has to set a limit equal to the sum of shopping. During shopping the set amount of money is withdrawn and there is no limit left and the card is of no use any more. Enabling the customer set the card limit, avoids the risk of security concern[116]. In Turkey, starting with Garanti Bank, other banks use the virtual credit car system, too.

3.6.2. International security platform (3d security)

Developed by VISA and approved by Matercard, 3D Secure protocol was brought by a security prerequisite and put into practice by Garanti Bank with the name of National Security Platform (3-D Secure).

---

[108] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[109] http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
[110] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[111] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006
[112] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 61
[113] http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
[114] Ene, Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama, s. 61
[115] Özmen, E-Ticaret, s. 221
[116] http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006

International Security Platform is not an approval or technological platform but a model which regulates the payment process between trader, bank and card holder. Application prepared for VISA is called "Verified by VISA" and the one prepared for MasterCard is called "SecureCode".

In accordance with 3D Secure System, a payment code is sent to the customer and the identity of the user is verified. Thus, unauthorized use is avoided[117].

On 31 March 2006, with the use of chip cards within Chip&Pin a new era has started in shopping. The chip on credit cards reduced the risk of copying the card and in case of loss or theft, the 4 digit password reduced the unauthorized use to a great extent[118].

The code or password required for payment in 3D Secure, can either be a 4 digit password or a verification code sent to the user by SMS.

3.6.3. Smart sms

Another example of 3D Secure is the "Smart SMS" system of Yapı Kredi Bank. It is similar to the compulsory, single use SMS verification code for internet (on-line) banking. Yapı Kredi Bank sends a single use verification code to the customer's mobile phone for verifying and securing on-line money transfers and credit cards. Thus, the trade makes sure that there is the real card holder. Smart SMS makes on-line shopping impossible without the verification code and undesirable outcomes are avoided[119].

3.6.4. Codesure

VISA developed a new level of security with a new credit card to be used for on-line shopping. Aiming make on-line shopping more secure and to prevent swindling, this new credit card is similar to other cards in size and shape but has an eight digit screen, twelve button keyboard and 3 years durable batteries. It is technologically capable of creating a dynamic secure code.

Chip&Pin has brought security to shopping where cards are physically used; even is stolen, unless the card holder tells the password, it is impossible to shop with a credit card. However, in virtual use, credit cards are less safe. Anyone who gains card information can use it without password. Visa CodeSure provides additional security for virtual use, where cards are not physically used[120].

Someone who wishes to shop on-line with CodeSure, should first hit the button "Verified by VISA". Then the card signals when it gets ready for use and the customer enters the usual password using the ATM keyboard. After that, a single use password, to shop on the internet, appears on card screen. Thus, the card holder performs the action securely with a code which nobody knows and cannot be used in any other way. VISA, uses its trial CodeSure cards in Turkey, UK, Italy, Israel, Switzerland and Germany[121].

4. E-commerce data and trader distribution in Turkey

E-trade volumes in Turkey per year are as follows.

Table 1: E-commerce volumes in Turkey

Years	Trade volume. Domestic and Foreign Credit Cards	Trade volume. Mail / Phone and E-trade
2005	1.388.390.000 Tl	6.059.790.000 Tl
2006	2.412.680.000 Tl	7.525.000.000 Tl
2007	5.537.170.000 Tl	11.763.590.000 Tl
2008	9.088.680.000 Tl	15.725.380.000 Tl
2009	10.273.680.000 Tl	18.987.810.000 Tl
2010 (Including July)	8.470.480.000 Tl	13.724.140.000 Tl

Source: www.bkm.com.tr, Acces Date : 10.08.2010

[117] http://eticaret.garanti.com.tr/Uluslararasi-Guvenlik-Platformu-3D-Secure.aspx, Access Date 26.06.2010

[118] http://www.cardfinans.com.tr/kampanyalar/chipnpin.jsp, Access Date 06.05.2006

[119] http://www.yapikredi.com.tr/tr-TR/sinirsiz_bankacilik/internet_bankaciligi/guvenlik/bireysel_guvenlik/akilli_sms.aspx, Access Date 15.08.2010
http://www.worldcard.com.tr/worldu-taniyin/world-ile-guvenli-alisveris/default.aspx#uc-boyutlu-guvenlik, Access Date 15.08.2010

[120] http://www.visaeurope.com/en/about_us/innovation/visa_codesure.aspx, Access Date 15.08.2010

[121] http://kredikartim.org/klavyeli-ve-ekranli-kredi-karti/, Access Date 15.08.2010
http://www.radikal.com.tr, "Klavyeli, ekranlı kredi kartı!", Access Date 18.07.2010

When we analyze Table 1, we see that the trade volume of credit cards is 1.388.390.000 Tl in 2005, 2.412.680.000 Tl in 2006, 5.537.170.000 Tl in 2007, 9.088.680.000 Tl in 2008, 10.273.680.000 Tl in 2009 and 8.470.480.000 Tl by the end of July in 2010. It is obviously seen that the volume is increasing every year.

Despite all precautions, unauthorized shopping makes more than 600.000.000 Tl each year. In 2009, unauthorized expenditures make up more than 138.000.000 Tl. This number is 14% higher than of 2008 numbers.

Table 2: E-traders per Regions

Regions	Number of Traders	Percentage %
Marmara Region	11.134	47
Central Anatolia Region	3.991	17
Aegean Region	3.598	15
Mediterranean Region	2.024	8
Black Sea Region	1.738	7
Southeast Anatolia Region	700	3
East Anatolia Region	626	3
Cyprus	148	1
Total	23.959	100

Source: www.bkm.com.tr, Acces Date : 10.08.2010

As seen on Table 2, most of 23.959 traders are in Marmara Region with 47%; then in linear order in Central Anatolia with 17%, Aegean Region with 15%, Mediterranean Region with 8%, Black Sea Region with 7%, Southeast Anatolia Region and East Anatolia Region with 3%, and Cyprus with 1%.

According to data obtained from the Credit Cards Centre of Banks, Istanbul (8.650 - 36%), Ankara (2.543 – 11%) and İzmir (1.557 – 6%) have the most e-traders[122]. In Kırklareli there are 94 traders, 7 of which are 3D Secure. The total number of 3D Secure traders in Turkey is 5.058[123].

Conclusion

With the development of information technology, and with the new type of trade, e-commerce facilities are increasing in our country each year. To protect this increasing trend, security for both parties in this process, should be ensured. Great effort is done to provide security and avoid all treats to increasingly dense participants.

Continuous efforts are done on the basis of legislations, technical base, taxing and security for e-commerce. E-signature, SSL, 3D Secure etc. encryption/verification techniques mentioned in the present paper, help to a great extend to provide security and overcome all kinds of criticism towards credit cards, forming the basis of payment.

As a result, it is obvious that, investors on e-commerce should be aware of all risks on e-commerce and use the most efficient encryption methods to minimize those risks to ensure a secure basis for protection of their customers' personal data and payment basis.

On the other hand, to increase security, e-commerce customers should be informed to use efficient and up-to-date antivirus programmes, firewalls; to keep their e-mails safe through not opening and deleting unknown or doubted mails; to keep their operating system and internet browsers up-to-date and use a password difficult to decode; to stay away, not register and shop from sites which do not use encryption techniques such as SSL; to prefer e-traders with strong security measures such as 3D Secure; to prefer to use e-keyboard against common phishing and worms.

[122] http://www.referansgazetesi.com/haber.aspx?HBR_KOD=137826, Access Date 26.06.2010
[123] http://www.bkm.com.tr/3d-secure-arama.aspx, Access Date 10.08.2010

References

Akkirman, Ali Deniz, *Sanal İşyerinde Örgütsel Davranış*, Aktüel Yayınları, İstanbul, 2004.

Bacchetta Marc, Patrick Low, Aaditya Mattoo, Ludger Schuknecht, Hannu Wagerand Madelon Wehrens, *Electronic Commerce and The Role of The WTO*, WTO Publications, Switzerland,1998.

Bülbül, Ali İhsan, *Bilgisayara Giriş*, Bayrak Matbaacılık, 2. Baskı, İstanbul, 2003.

Bozkurt, Veysel, *Elektronik Ticaret*, Alfa Yayınları, İstanbul, 2000.

Civelek, M. Emre, Edin Güçlü Sözer, *İnternet Ticareti, Yeni Ekososyal Sistem ve Ticaret Noktaları*, Beta Basım Yayım Dağıtım A.Ş., İstanbul, 2003.

Clinton, W.J.- Gore, A., Çev.: Veysel BOZKURT, *Global Elektronik Ticaret*, Alfa Basım Dağıtım Ltd. Şti., İstanbul, 2000.

Chaudhury Abhijit, Kuıboer Jean-Pierre, *E-Business and ECommerce Infrastucture: Technologies Supporting The e-Business Initisative*, McGraw-Hill Higher Education, U.S.A., 2002.

Dolanbay, Coşkun, *E-Ticaret Strateji ve Yöntemleri*, Meteksan Sitem Yayınları, Ankara, 2000.

Douglas, Allen, Steve Johnson, *İnternet Öğrenim Kılavuzu*, Alfa Basım Yayın Dağıtım A.Ş., İstanbul, 1998.

Ekin, Nusret, *Bilgi Ekonomisinde E-Ticaret*, İTO Yayınları, Yayın No:1998-61, İstanbul, 1998.

Ene, Selda, *Elektronik Ticarette Tüketicinin Korunması ve Bir Uygulama*, İstanbul: Pusula Yayıncılık, İstanbul, 2002.

Erdağ, Nevzat, Emel Batuman, *Elektronik Ticaret El Kitabı*, Arıkan Basım Yayım Dağıtım Ltd. Şti., Bilgi Serisi,Denizli, 2006.

Güven, Zülkif, Burhan Deniz, *Bilgisayara Giriş*, Sürat Yayınları, İstanbul, 1998.

Güleç, A. Selami, Azmi Yalçın, *Elektronik İstila*, Nobel Kitabevi, İstanbul, 2003.

Hasıloğlu, Selçuk Burak, *Enformasyon Toplumunda Elektronik Ticaret ve Stratejileri*, Türkmen Kitabevi, İstanbul, 1999.

Ngai E.W.T., F.K.T. Wat, "A literature review and classification of electronic commerce research", *Information & Management, Elsevier Science B.V.*,n: 39, 2002, s. 415–429

Öcal, Hakkı, *İnternet Tasarım Rehberi*, Byte Türkiye Dergisi Ekim 1998 Eki, İhlas Matbaacılık, Gazetecilik, Yayıncılık A.Ş., İstanbul, 1998.

Özbay, Adem, Jan Devrim, *E-Ticaret Rehberi*, Hayat Yayınları Bilgi Teknolojileri Dizisi 7., İstanbul, 2000.

Özmen, Şule, *Ağ Ekonomisinde Yeni Ticaret Yolu E-Ticaret*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2003.

PC World Dergisi Eki, *İnternet El Kitabı*, Ilıcak Matbaacılık A.Ş., PC World Dergisi, İstanbul, 1996.

Spector, Robert, *amazon.com Get Big Fast*, HarperCollins Publishers Inc., New York, 2002.

Tapscott, Don, *Dijital Ekonomi*, Koç Sistem Yayınları, İstanbul, 1998.

Türkmen, Aydın, "*Sahibini Tanıyan Laptop Üretildi*" Güneş Gazetesi 26 Şubat 2006.

Yatlı, Billur, *Elektronik Ticarette Vergilendirme*, Der Yayınları, İstanbul, 2003.

Yürüyen, Umut Mehmet, *Deniz-Ticaretinde Elektronik Satış Yönetimi,* Dokuz Eylül Yayınları, İzmir, 2003.

http://bm-dergi.emo.org.tr/index.php?option=com_content&task=view&id=32&Itemid=74, Access Date 15.03.2006

http://eticaret.garanti.com.tr/icerik/goster.asp, Access Date 20.05.2006

http://eticaret.garanti.com.tr/Uluslararasi-Guvenlik-Platformu-3D-Secure.aspx, Access Date 26.06.2010

http://kredikartim.org/klavyeli-ve-ekranli-kredi-karti/, Access Date 15.08.2010

http://sertifika.bilten.tubitak.gov.tr/net/teknik/SSL.jsp, Access Date 04.02.2006

http://www.activefinans.com/activeline/sayi8/biometri.html, Access Date 18.06.2006

http://www.bkm.com.tr/3d-secure-arama.aspx, Access Date: 10.08.2010
http://www.cardfinans.com.tr/kampanyalar/chipnpin.jsp, Access Date: 06.05.2006
http://www.deltur.cec.eu.int/kitap/bilgitop.html, Access Date 15.04.2006
http://www.e-cicek.net/guvenlik.asp, Access Date 21.04.2006
http://www.e-guven.com/default.asp, Access Date 15.08.2010
http://www.gestocomm.cz/data/datasheets/Luna_CA3.pdf, Access Date 12.05.2006
http://www.globalsign.com.tr/destek/dijital_sertifika_body.asp, Access Date 20.02.2006
http://www.infonet.com.tr/tr/products/Rainbow/lunasa.htm, Access Date 12.05.2006
http://www.insankaynaklari.gokceada.com/konu3_1.html, Access Date 18.04.2006
http://www.internetmarketing-tr.com/info/info-0001.htm, Access Date 15.03.2006
http://www.isbank.com.tr/content/TR/Guvenlik/Biyokimlik-987-292.aspx, Access Date 15.08.2010
http://www.paypal.com, Access Date, 26.06.2010
http://www.radikal.com.tr, "Klavyeli, ekranlı kredi kartı!", Access Date 18.07.2010
http://www.referansgazetesi.com/haber.aspx?HBR_KOD=137826, Access Date 26.06.2010
http://www.superonline.com/hukuk/hukuk.htm, Access Date 18.05.2006
http://www.vakifbank.com.tr/biosifre.aspx, Access Date 15.08.2010
http://www.visaeurope.com/en/about_us/innovation/visa_codesure.aspx, Access Date 15.08.2010
http://www.yapikredi.com.tr/tr-TR/sinirsiz_bankacilik/internet_bankaciligi/guvenlik/bireysel_guvenlik/akilli_sms.aspx, Access Date 15.08.2010
http://www.ykb.com/tr/sss/eticaret.shtml, Access Date 16.05.2006
http://www.ymm.net/e-ticaret/e-imza.htm, Access Date 12.04.2006
http://www.ymm.net/e-ticaret/elektronik_imza_kanunu.htm, Access Date 12.04.2006
http://www.worldcard.com.tr/worldu-taniyin/world-ile-guvenli-alisveris/default.aspx#uc-boyutlu-guvenlik, Access Date 15.08.2010