INTERNATIONAL JOURNAL OF ELECTRONICS; MECHANICAL and MECHATRONICS ENGINEERING Vol.2 Num.2 pp.(172-179)

DIGITAL SIGNATURE IN THE WAY OF LAW

Ruya Samlı

Istanbul University, Computer Engineering Department
Avcılar, İstanbul, Turkey
ruyasamli@istanbul.edu.tr

Abstract *: Signature can be defined as a person's name or special signs that he/she writes when he/she wants to indicate he/she wrote or confirm that writing. A person signs many times in his/her life. A person's signature that is used for thousands of times for many things from formal documents to exams has importance for that person. Especially, signing in legal operations is an operation that can build important results. If a person's signature is imitated by another person, he/she can become beholden, donate his/her whole wealth, commits offences or do some judicial operations. Today, because many operations can be done with digital environments and internet, signature operation that provides identity validation must also be carried to digital environment. In this paper digital signature concept that is approved for this reason and its situation in international areas and Turkish laws are investigated.*

Keywords *: Digital Signature, Digital Law*

1. INTRODUCTION

Today, many operations that are done with paper can also be made in digital world in many countries. Banking operations, password applications, insurance operations, vehicle (bus train, plain) and organization (cinema, theatre, concert) ticket reservations, tax, bill operations, exam applications, lesson choices of students are some of e-commerce operations. In the operations that are done by internet, identity validation is done with a user name and password. But this validation process is not a very suitable process for the processes that identity information carries vital importance. Because the person can forget the password, or someone else can learn it by anyway. If something occurs like that the person will be in a hard position. So, a concept named digital signature appeared to prevent that situations. Digital signatures are used to show the identity of the person who sent the information or email using electronic environment like original signatures [1]. Electronic signature (or e-signature) which is a concept that contains digital signature can be defined as "the technique of people they use while they are proving that he/she is himself/herself". Validation of people are proved with e-signature in electronic environment while it is proved with original signature, seal at in paper world [2]. E-signature is a very large concept. The biometric security methods which are like people's eye retina, fingerprint or digitalized signatures of people which are made by scanning the original signatures can be shown as examples of e-signatures.

Digital signature is a part of electronic signature and is a signature type that is based on as unique because its content is changed with mathematical functions. Digital certificates are used in building and validating digital signatures.

A person who wants to sign a data digitally must have a personal digital certificate.

2. DIGITAL SIGNATURE

Many definitions can be made about digital signature. Some of them are like that :

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit. Digital signatures are commonly used for software

distribution, financial transactions, and in other cases where it is important to detect forgery or tampering [3].
The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation [4].
A digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turn it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds both of them together. The digital signature ensures the authenticity of the signer. Any changes made to the document after it is signed invalidate the signature, thereby protecting against signature forgery and information tampering. E-signatures help organizations sustain signer authenticity, accountability, data integrity and non-repudiation of electronic documents and forms [5].
A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later [6].

2.1. Properties and Benefits of Digital Signature

Digital signature guarantees the information come from the right user, server or host that claim it sent the information because it is unique. Digital signature protects the datas' content during data flow. It prevents the information from being obtained by another person and also being changed. Also it guarantees the information is sent to and read by the right receiver. It provides stigmatizing and archiving the sent datas. It provides savings of paper, mail, press costs and speed. Digital signature enables to prove who sends and receives the information. The person/server etc who sends a signed document can't deny he/she/it sent the document. This situation is also valid for receivers [7].

2.2. How is a Digital Signature Built and Validated?

Digital siganture is build by doing an operation not in the sent message but over the hash message of it.
Hash message means the message summary but it is not a classical summary that can be differ from person to person, it is obtained by shorten the original message uniquely by some functions.
To obtain the whole original message is not possible from hash message. In other words, hash function is an irreversible function. After obtaining hash message this message is coded by using private key. This coded hash message is used as digital signature. Digital signature is attached to original message and sent to the receiver. Buiding a digital signature is shown in Figure 1.

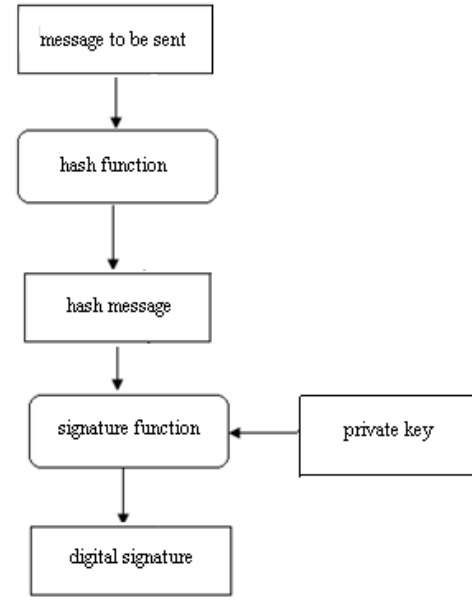

Figure 1 Building a Digital Signature

When a digital signature is built it can be used in many different operations as shown in Figure 2.

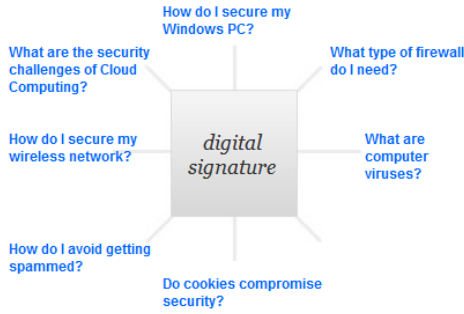

Figure 2 Digital Signature [8]

Receiver decrypts the message by using sender's public key. After this operation, receiver receives a hash message. If two has messages are the same, this message is validated to be come from the right sender. It is guaranteed because if message is changed while it is being sent, the hash message that receiver receives must be different from the first hash message. So, it can be obviously seen that digital signature is incidental to message and the public key of message sender. Validating a digital signature is shown in Figure 3.

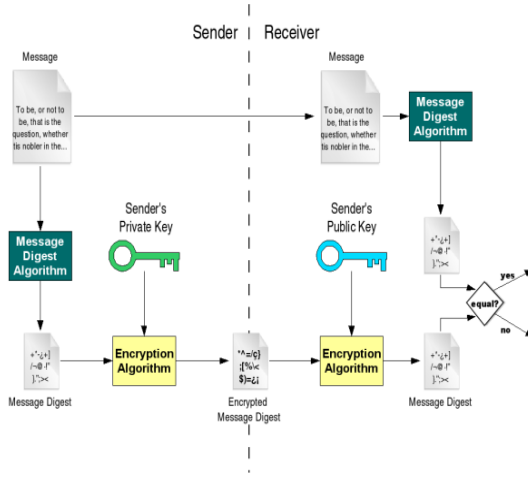

Figure 3 Validating a Digital Signature [9]

2.3. Digital Certificates

Digital certificates that can be named as also digital IDs are identities of a person in digital world.
In other words they are the similar ones of identity cards, driving licences, passports. Like in real world, when a person shows his/her digital certificate, it means that he/she proved his/her identity and reach on-line services. Digital certificates also link the identity of the person to a public key that is used in building digital signatures. Not only a natural person can have a digital certificate and signature but also legal entities can have. Today some corporations are related to provide digital certificates. This corporations must be different from the people/coporation that gets and gives digital certificate service. Digital certificates are shown in Figure 3.

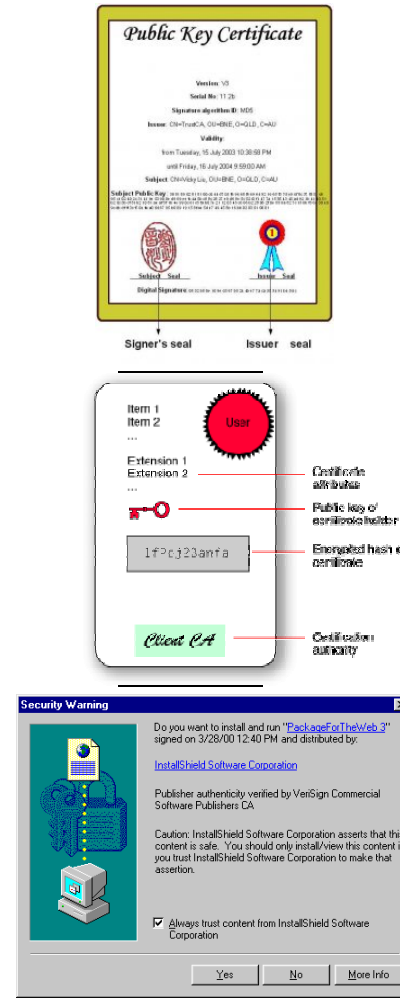

Figure 4 A Digital Certificate [10]

3. THE LAW PROPERTIES OF DIGITAL SIGNATURE

Digital signature presents many easinesses to user with its doing many operations in the electronic world.

But, similar to the operations that signature is used, it must be done some law arrangements in the applications that digital signature is used. The situations in Turkey and international areas about digital signature can be observed like in this section and some sample countries and their laws about digital signature is handled.

3.1. International Arrangements About Digital Signature

Especially from 1996, in many countries, some studies are done about digital signature. In many countries' digital signature arrangements, UNICTRAL (United Nations Commission on International Trade Law) [11] model laws and European Community directives are effective. This model law is built because of 2 detections. First of them is that modern communication vehicles increase and second is that when the electronic datas which are important in the way of law are tired to be sent with electronic ways, there become some problems [12].

A. AMERICA

i. United States of America (USA)

EPIC (Electronic Privacy Information Center) reported that building a standart about digital signature in USA and making law arrangements are started by DSS (Digital Signature Standart) which is built by NIST (National Institute of Standarts) [13]. The most important approvement in USA, is the acceptance of the S.761 numbered law in 2000. This law of is like that. "If a record or an agreement is done with an electronic signature, it doesn't mean that it is not valid, in force etc for only its using an electronic signature [14][15]. The most interesting thing about this law is, the president of that time, Bill Clinton's signing the law with a digital signature.

ii. Canada

It has an Electronic Operations Law that contains all electronic operations and brought into force at 10 April 2001 [16].

B. EUROPEAN COMMUNITY

i. Germany

German Digital Signature Law which is called SigG is accepted in 2001. The digital signature definition of this law which investigates general dominations companies who give certificate services, technical security, auditing and result domination is like that "Electronic signatures are datas that can be attached to other electronic datas and make a connection to those datas and also be useful for recognizing the users" [17].

ii. France

In Civil Law in 2000, (with 2000-230 numbered law) there is electronic signature law in 1316-4 by law. To apply this by law in 2001, (2001-272 numbered decree) an arrangement was done and brought into force [18]. In France, electronic signature usage is not in desired amount because of the querying authorization of courts for the commercial agreements that are signed with electronic signature [19].

iii. Spain

The e-signature law that leaves the authorization and responsibility to Telecommunication and Information Security Ministry was brought into force in 2003. Although it has a comprehensive law about the subject, Spain is not in the countries that use e-signature widespreadly [20].

iv. Finland

The studies about the subject in 1998 in Finland which is one of the countries that the usage of electronic and mobile signature is high. In 2000, the law about the subject is accepted and started to be applied in the name of Administrative Electronic Services Law [21]. In this law, there is not a definite criteria about electronic signature is broken all the certificates will be cancelled [22].

v. Hungary

Communications Authority of Hungary [23] is the responsible foundation for the law accepted At 29 May 2001 [24].

vi. Norway

The Electronic Signatures Act of Norway is accepted at 15 June 2001 and modified at 17 June 2005 [25].

vii. Luxembourg

It has a digital law that is accepted at 14 August 2000 [26].

C. FAR EAST
i. China

The "Law of the People's Republic of China on Electronic Signatures," passed by the 11th conference of the Standing Committee of the 10th State Council of the People's Republic of China on August 28, 2004, is hereby promulgated and will take effect as of April 1, 2005. It is a law of 36 articles and some subjects it explains are :
- what electronic data is,
- when it can be used as evidence,
- in which documents electronic signature is not accepted
- what are the legal responsibilities [27].

ii. Malaysia

Malaysia is one of the first countries that realizes importance of digital signature and before many developed country. It prepares a very detailed law about the subject. It gives importance to the subject licence of digital sertificates and also private key security that are neglected by some other countries [28].

iii. Singapore

One year later Malaysia, its neighbour Singapore accepted a detailed digital law similar to it in 1998 [29].

D. AFRICA
i. Ghana

Ghana has a new electronic signature law that is accepted in 2008 [30].

ii. South Africa

A very detailed electronic communications and transactions act in South Africa that consists articles about

- consumer protection
- domain name authority and administration
- limitation of liability of service providers
- cyber inspectors
- cyber crimes

came into force in 2002 [31].

E. Others

Apart from the ones mentioned above some other countries also have laws about electronic and digital signature. The table below shows the countries that have digital laws in alphabetical order and the years of their digital laws [32].

Table 1 Other Countries With Digital Law

Austria	Signature Law	200(
Belgium	Signature Law	2001
Bermuda	Electronic Transactions Act	1999
	Certification Service Providers (Relevant Criteria and Security Guidelines) Regulations	2002
Czech Republic	Act on Electronic Signatures	200(
England, Scotland and Wales	Electronic Communications Act	200(
	The Electronic Signatures Regulations	2002
Estonia	Digital Signature Law	200(
	Digital Signatures Act	2003
India	Information Technology Act	200(
Ireland	Irish Electronic Commerce Act	200(
Lithuana	Law on electronic signature	2002
Malta	Maltese Electronic Commerce Act	2001
	Last ammended	2005
Moldova	Law about Electronic Document and Digital Signature	2004
New Zealand	Electronic Transactions Act	2002
Philippis	Electronic Commerce Act	200(
Romania	Law on the Electronic Signature	2001
Russia	Federal Law of Russian Federation about Electronic Digital Signature	2002
Slovakia	Act no.215/2002 on electronic signature	2002
Slovenia	Electronic Business and Electronic Signature Act	200(
Sweden	Qualified Electronic Signatures Act	200(

4. DIGITAL SIGNATURE ACCORDING TO TURKISH TRADE LAWS

The studies about digital signature in Turkey started in 2000 in Undersecretariat Of Foreign

trade. Tthey continued by the studies that is done in Ministry of Justice in 2002 and it takes the today situation with 5070 numbered Electronic Signature Law and published in Official Gazzette in 2004.
In this law, digital signature definition is done like "Electronic signature defines the electronic datas that are attached another electronic data, connected to them and used to validate the identity of user" [33] [34]. In the aforementioned law, there are dominations about aim, concept, definitions, secured electronic signature and certificate services, control and punishment [35].
The 5070 numbered law is generally suitable to 99/93/EC numbered "Council – Commission Directives About Electronic Signature" of European Community [36]. With this law, some alteration in the some other laws must be done. For example to the expression in the 1. article of Debt Law that was like "Signature must be handwriting of the beholden people" another expression like "Secure electonic signature has the same authorization with wet signature" is added after Electronic Signature Law [37].
Giving digital certificate operation started by intermediary companies in 2005. If we look at these digital certificate cronologically, Electronic Information Security Incorporated Company, Tubitak UEKAE [38], TurkTrustBilgi Communication and Informatic Security Services [39]. EBG Informatic Technologies and services [40] as these companies.
Some articles in Turkish law are like that :

Article 1 :
The aim of this law is to organize juridical and technical properties and usage basics of electronic signature.

Article 5 :
Secured electronic signature gives the same juridical results with handwritten signature.

Article 13 :
The responsibility of elecetronic certificate provider to electronic certificate owner is dependent to general provisions.

Article 14 :
The juricidal results of electronic certificates that are given by a service provider established in a foreign country are determined by international agreements.

Article 15 :
The control of activity and oprations of electronic service providers related to applying this law is made by corporation.

Article 26 :
Cabinet Council enforces the provisions of this law.

Article 23 :
The 295/A article below is added to 18.6.1972 dated and 1086 law no Civil Procedure Trial Law the way that is comes after article 295.

Article 295/A:
Electronic datas that are made by secured electronic signature according to hoyle are under the heel of bond. These datas are accepted as evidence until its adverse is proved.

5. CONCLUSION

Although technologic improvements that are based on time, effort and money diposal were thought as luxury in ancient times, they become necessarities today.

The machines, robots that people think when technologic improvement is discussed are the tools that can make many operations that are made manually. This is the hardware side of the technologic improvement. On the other hand there is another side of the improvements that is called software. Internet is the most important part of this side. Internet which could be used finitely and for only military when it first occurs gets a vehicle that people use for entertainment, communication, information sharing etc today. But the real improvement about internet took place when people can do the operations by using only computer and internet that they spend time, effort and money and whenever/wherever they want.
Today we can make lots of applications that couldn't come to our minds a few years ago. We can say every banking operations, money transfers, learning information like tax number, online applications for central exams, paying bills, taxes, notary operations, passport applications, buying tickets for a show or

public transport vehicle between these operations. These operations that ease life are not free of problems as they are in real world. The most important problem is how it will be decided the person who made the operation is whether the real person who is claimed to make the operation or not. In the paper operations it is easy. The person who makes the operation can validate his/her identity by using his/her own wet signature, seal, stamp etc. But making these processes is impossible in digital world. So, the internet operations can cause problems. To avoid these problems, digital signature concept is arised especially in last 15 years.

Digital signature can show that the person who makes the operations is the person who is claimed to make these operations or not.

In this paper, after it is mentioned about what digital signature is, properties of it and how a digital signing is being made, it is investigated how the laws of many countries in the world and Turkey attend to digital signature. After this investigation it is seen that some countries give importance to this subject and have laws about this subject, some countries have only studies about digital signature but any way at all considerable number of countries are aware of digital signature. When it is looked at the country investigations and Table 1 too, it can be easily seen that the digital signature law studies are made especially in the last 1990s and early 2000s.

In Turkey there is also a digital signature law and it is applied elemantarily.

If we make a general evaluation about this subject, in a world that the countries known as super powers introduce digital signature laws only 8-10 years before, Turkey's starting to study and introducing law about the subject after only a few years of the other countries is a gladsome development. Also we can say mention that Turkey's digital signature law is compatible to the Council - Commission Directives About Electronic Signatures of European Community, there are many companies that provide digital certificate services which are necessary for having a digital signature, TUBITAK is studying about this subject and these also show that Turkey is in a good position about the digital signature subject. Due to these and other developments similar to these, Turkey approaches to the values it aims day by day.

6. REFERENCES

[1] Orta, M., "Elektronik İmza ve Uygulaması", Seçkin Yayınları, Ankara, 2005.

[2] Buyukbahceci, M., "Dijital Sertifikalar ve Dijital İmzalar", e-imza & e-Turkiye Sempozyumu, Ankara / 15.07.2004.

[3] Wikipedia, Digital Signature, http://en.wikipedia.org/wiki/Digital_signature

[4] Federal Information Processing Standards Publication Digital Signature Standard (DSS), Information Technology Laboratory National Institute of Standards and Technology, Issued June, 2009.

[5] Digital Signature, http://www.arx.com/digital-signatures-faq

[6] http://searchsecurity.techtarget.com/definition/digital-signature

[7] E-imza (Kavramlar, Hukuki Boyut ve Uygulamalar), Yuksel SAMAST - TURKTRUST A.S. BT Vizyon –İstanbul Toplantısı / 03.05.2005.

[8] Webopedia, Digital Signature, http://www.webopedia.com/TERM/D/digital_signature.html

[9] Public Key Cryptography http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html

[10] E-bergi, Digital Signature, http://e-bergi.com/2008/Ekim/Sayisal-Imza

[11] E-bergi, Digital Signature, http://e-bergi.com/2008/Ekim/Sayisal-Imza

[12] Dijital İmza ve Dijital İmzanın Borçlar Kanunu Hükümleri Açısından Ele Alınması, Yard. Doc. Dr. Zarife Senocak, 2001.

[13] Electronic Privacy And Information Center, Digital Signature,http://epic.org/crypto/dss/

[14] Energy Commerce, http://www.house.gov/commerce/

[15] Wikipedia, Electronic Signature, http://en.wikipedia.org/wiki/Electronic_signature

[16] İnci Demirel, Hukuk Elektronik Yasam ve

Ticaretin Hizmetinde veya Siber Uzayda Hukukun

[17] German Signature Law, thukuku.bilgi.edu.tr/documents/alman_imza_kanunu.doc

[18] France Digital Law, http://turk.internet.com/haber

[19] European Commission/DG Enterprise and Industry, Benchmarking of existing national legal e-business pactices, Country Report France, 2006.

[20] European Commission/DG Enterprise and Industry, Benchmarking of existing national legal e-business pactices, Country Report Spain, 2006.

[21] Ozenc, K, Avrupa Birliği'nde Elektronik İmza, Ulusal Elektronik İmza Sempozyumu, Ankara 7-8 Aralık 2006, s. 172-176.

[22] European Commission/DG Enterprise and Industry, Benchmarking of existing national legal e-business pactices,Country Report Finland, 2006.

[23] http://www.hif.hu/

[24] Act XXXV of 2001 on Electronic Signatures

[25] The Electronic Signatures Act of 15 June 2001 no. 81

[26] Signature electronic of Cryptography of Luxemburg

[27] Law of the People's Republic of China on Electronic Signatures

[28] Laws Of Malaysia, Digital Signature Act 1997

[29] Electronic Transactions Act of Singapore

[30] Electronic Transactions Act of Ghana, 2008

[31] Government Gazette of Republic of South

[32] Africa Vol. 446 Cape Town 2 August 2002 No. 23708

[33] Wikipedia, Digital Signature and Law, http://en.wikipedia.org/wiki/Digital_signatures_and_law.

[34] 5070 Law no Turkish Electronic Signature Law, http://www.mevzuat.basbakanlik.gov.tr,5070 Sayılı Elektronik İmza Kanunu, Kasım 2008.

[35] TBMM, Turkish Laws, http://www.tbmm.gov.tr/kanunlar/k5070.html

[36] Sayılı Elektronik İmza Kanunu, Kasım 2008.

[37] TBMM, Turkish Laws, http://www.tbmm.gov.tr/kanunlar/k5070.html

[38] Digital Signature, Emrah Yavuzcan, http://www.hukuki.net/hukuk

[39] Law of Mortgage, http://www.mevzuat.adalet.gov.tr/html/407.htm l , Borçlar Kanunu, Ocak 2009.

[40] Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, UEKAE, TUBİTAK, http://www.uekae.tubitak.gov.tr.

[41] Türktrust, Signature of Turkeyhttp://www.turktrust.com.tr/
EBG Bilişim Teknolojileri ve Hizmetleri A.S., http://www.e-tugra.com.tr/