Analysis of the act on electronic signatures

Erika Fülöp Szilágyi and Péter Sasvári

Department of Entrepreneurship, Institute of Business Sciences, University of Miskolc

Introduction

On the turn of the new millenium, with the vast spreading of electronic message-sending, a demand arose to be able to send messages in electronic way that can produce a legal effect. For that it is inevitable that parties be able to state authentically who the message is from and whether its content has been unchanged since posting. This function could be fulfilled by electronic signature if suitable technology and legal background are given.

As a result of this study it can be stated that the act is in compliance with EU directives and a good basis for introducing digital signatures, but there are still several technological questions open that can basically influence the security of the system and can lead to legal and tecnological loopholes.

Recognising the development trend the Hungarian National Assembly passed the 'Act XXXV of 2001' on electronic signatures to create the legal framework for the provision of certified electronic communication, data transmission in business contacts. The range of notions related to electronic signatures, the basic principles, the services and their conditions, the requirements that service providers should meet, their responsibilities and their supervision (by the Communication Authority) have been regulated, as well as breach of contract cases and of course possible fines to be imposed.

Outline of legal regulation

a) Why is the act on electronic signatures needed?

The two contracting parties could agree on acceptance of contracts in electronic form, but they were required to make a traditionally-certified written contract in advance. This worked without any particular legal regulation. With the legislation these bilateral agreements have become simpler, although there is still a possibility of divergence from the provisions of the act. However, the legislation gives the opportunity to introduce electronic documents in fields where the use of them was not possible earlier.(company procedures, tax authority, public administration). The aim of the present law is to introduce the usage of electronic signatures into several state–controlled areas. The essential condition for that is amending the related laws.

b) EU directives

The fact that there are laws and regulations concerning electronic commerce and electronic signatures all over the world was the other important factor that promoted legislation procedure. Nowadays technical development requires applicability of electronic communications and documents in official areas as well.

The European Parliament and Council issued a directive in January 2000 in connection with electronic signatures in which defined the basic principles concerning electronic signatures, and ordered all the member countries to establish their own regulatory systems based on the common principles.

Among other things it is written in EU directives that electronic signatures have to be accepted as equal in all respects to traditional signatures and the member countries of the European Community must mutually accept one another's electronic signatures and

certificates and encourage other countries in the region to join the system. The harmonization of laws and of course the technological background is essential for the functioning of such a system that includes several countries.

Several international organizations deal with the standardization of elements of Public Key Infrastucture. Unfortunately the standards and recommendations made so far do not form a homogeneous, coherent system, while there are overlaps as well.

Outline of the Hungarian act

a) Outline

While forming the Hungarian regulation the fundamental point of view was to comply with the EU principles entirely. In addition, the prevailing Hungarian laws had to be taken into consideration. There is a textual proposal in the closing stipulations of the present act to amend the laws closely related to the issue, creating the basic case for the use of electronic signature and electronic documents.

The law regulates three important ranges of areas:[3]

-the validity of the law, which at the same time defines the opportunities of employment (we do not deal with this part at all);

-regulations of services related to electronic signatures;

-regulations concerning the activity of the Communication Authority (hereinafter called the Authority).

In the enactment another essential principle was that legal regulation should be independent from technologies. In the used legal terminology well-known technical terms are named after their functions.

The act defines the following notions:

- a signature in electronic form, an advanced electronic signature, a qualified electronic signature
- an electronic document, electronic document data, an electronic instrument
- signature creation data (private key), signature verification data (public key)
- a signature creation device, a secure signature creation device (typically a chip card or smart card)
- a certificate, a qualified certificate
- a time marker
- a verifying electronic signature, placing an electronic signature
- a signatory, qualified certification service provider

b) Structure of operation defined by the act

The following services related to electronic signature are regulated by the act:

- an electronic signature certification service (for issuing and registering electronic certificates)
- a time-marker service
- placement of signature creation data on the signature creating device

The above mentioned services have to be notified to the Authority. It registers the service provider and continuously controls its activity in respect of complying with the laws and regulations and the general contract conditions. In case of any irregularity it can take immediate measures, impose a fine or even suspend the service with immediate effect.

Issuing a qualified certificate or placing signature creation data on the signature creation device can be done only by qualified certification service providers. Qualification is carried

out by the Authority. In order to become qualified the applicant has to meet requirements: (no criminal record, proper qualifications, liability insurance, sufficient financial recources, use of secure electronic signature products, etc.). The Authority conducts a comprehensive on-site inspection at least once a year. If the service provider does not comply with the regulations, and the measures taken are not sufficient, the Authority can revoke the qualification.

The certification service provider issues electronic certificates. It has to identify the claimant. If it is successful the claimant's signature verification data, other data used for identification and data related to the issue and use of certificate (name of service provider, limits on use, indication of the beginning and end of the period of validity, etc.) have to be recorded in a certificate and signed by the service provider's own signature creation data. The service provider keeps a register of the issued certificates and all the data they are based on. It also receives data related to changes, keeps a record of the current status of certificates, their suspension and revocation. This status record together with the regulations and signature verification data have to be made available to the public via telecommunications network systems.

Analysis

A complicated system of many factors involves several dangers. Irregular behaviour of one person endangers the other persons in the system. Mapping these dangers, estimating the strength of existing defensive methods, and defining further effective defensive methods—in view of the complexity of the system—is a demanding task.

In the following section we examine the system created by the act with the help of a safety hazard analysis. According to the generally accepted methodology of risk analysis there are three applicable defences in order to eliminate possible dangers: preventive, detective and corrective solutions. A good system employs all the three defences against dangers. In case of a given risk the lack of one of the solutions can be acceptable if the other defences are strong enough and compensate for the missing control.

In the table below we list the risks endangering the different parties, and the risks imposed by the irregular behaviour of participants. In each case we examined the defensive strategies proposed by the act to a given danger, their deficiencies, and the defences that could be effectively employed.

Table 1. Dangers and control measures in various cases [1]

	Danger	Control measures		
		Preventive	Detective	Corrective
Protection of signatory	Loss of signature creation data (non-authorized person can sign)	Chip card storage PIN code, identification with a password	Detection of theft, loss	The user initiates revocation of the certificate at the service provider; Taking legal action
	Deciphering signature creation data (non-authorized person can sign)	Application of cryptography that is hard to decipher	-	Revocation of certificate; Liability of service provider; Insurance
	Somebody else (non-authorized person) suspends the certificate	Suitable identification	Notification of the owner about the suspension	Reinforcement; Compensation; insurance
	Blackmail, compulsion	(Other laws are relevant)	-	(Other laws are relevant)
	The signatory discloses his/her signature creation data to another person to create two certificates with the same signature verification data at different certification service providers	Central database needed for registered signature verification data	Central database needed for registered signature verification data	Voidable in court
	Use of forged certificate	Application of cryptography that is difficult to decipher	Central database needed for issued certificates	Liability of service provider; Insurance
	Use of revoked certificate	Recording the date of signing and revocation	Continuous observation of revocation list	Court presumes the authenticity of qualified signature
	Manipulation of signature verification data of service provider	Manipulation of signature verification data of service provider !!!!	Authority should issue attested certificates to service providers	Imprint of signature verification data of the Authority should be

			Signature verification data of the Authority should be accessible	accessible
Protection of certification service provider (CSP)	Compromising signature creation data of the certification service provider[CSP]	Strong physical defence [security measures against burglary]	Burglary is always detectible	Revocation list about signature creation data of service providers; Fact of revocation has to be published (official announcement); Insurance
	False suspension (based on false report)	Lack of legal remedy against the Authority	Notification	Lack of opportunity to appeal against the Authority's decision
	Employees	Clean criminal record	Inner control	Court trial
		Registered expert; Definition of inner proceedings at the service provider; National security screening; Public servant oath	Keeping strict records of activities	Insurance RISK
	Blackmail	Other laws are relevant (technological defence: quiet alarm)	-	Other laws are relevant; Revocation
	Deciphering signature creation data of service provider and forging its signature	By applying strong cryptography this danger can practically be eliminated Signature creation data has to be in accordance with technological developments	-	Notification of users; Insurance
Protection against	Certification service	Certification service	Suspicious signs;	Court trial;

certification service provider (CSP)	provider(CSP) issues fake certificate	provider(CSP) should be qualified by the Authority; Continuous checking by the Authority; INSUFFICIENT DEFENCE Regular report needed about the issued certificates	Central database needed for registered signature verification data	Authority calls certification service provider(CSP) to account; Revocation of certificate; Compensation
	Certification service provider(CSP) revokes certificate suddenly (before time or without cause)	Choosing reliable service provider; Qualification of service provider	SP should send the owner a notification about the revocation Revocation list should be checked continuously	Court trial
	CSP closes down or made to end and certificates issued revoked	Choosing reliable service provider; Qualification of service provider	SP should send owner a notification about the revocation Revocation list should be checked continuously	Court trial
	CSP issues certificate to another person with the same signature verification data	Choosing reliable service provider; Qualification of service provider	Suspicious signs; Central database needed for registered signature verification data	Revocation of certificate; Court trial; Compensation (CSP is liable according to the act)
	CSP does not keep or publish the certificate revocation list	Central database needed for registered signature verification data	INSUFFICIENT DEFENCE	
	CSP withholds issued certificates	Central database needed about the issued certificates	Authority control INSUFFICIENT DEFENCE	Calling to account
Global	Cracking RSA	Elaboration of alternative cryptographic algorithm	-	Crisis management

Summary

The draft bill does not deal properly with the problems of handling time and validity. The date of signing has to appear in the electronic signature, it would be practical to put this down in writing in the regulations as well. The revocation time of a given certificate also has to be put down in writing, and this requirement is missing from the act.

As for the time-marker service, the bill does not make separate statements (it simply makes an analogy between the time-marker service and signature verification service) and thus does not deal with the problem, that the exact date of an event can be defined only by two time stamps.

The bill contains excessive limitations on issuing time markers: according to it a time marker is the common digital signature of the date put on the electronic document by the service provider. It excludes cases when the time marker service provider signs only the date (which is the practice in elaborated protocols). The shared (different) registers of the revocation list and certificates means a relatively big vulnerability. It is essential to create a central database for certificates and revocation lists, otherwise it would be difficult to check service providers, and calling them to account would be hopeless.

The system lacks a reliable and effective signature verification service. In a debated case the person who wants to verify a signature can do nothing but start a court proceeding, which is costly and inefficient. In addition, the control over verification service providers may turn out to be insufficient. The profit gained from abuses is a lot more than the invested costs. The appearance of organised crime behind verification service providers cannot be exluded in the present system.

At some points of the law there is a confusion of ideas (e.g. Art. 9 (3): the verification service provider identifies the requesting person and then attests his/her electronic signature).
It may also cause trouble that there are differences between word processing softwares (eg. different versions of (Microsoft Word) so it may occur that the signed, intact document signed by the user may look different on another computer. (in an extreme case hidden text may appear which was not seen at the time of signing) An electronic document may contain only text. But what do we mean by this exactly? Can only Rich Text Format, or Word Document be considered texts? (in an extreme case it may contain macros)

It may occur that several people have to sign a document or that different parts of the document are signed by different people. Even a case may occur when somebody from the signatories wants to sign the document in the traditional way (this is not excluded by the law). The formal requirements in such cases have to be put down in the law.

As a result of this investigation it can be stated that the draft bill is in compliance with EU directives and a good basis for introducing digital signatures, but there are still several technological questions open that can basically influence the security of the system and can lead to legal and technological loopholes.

In the present act the goverment is authorised to regulate some unfinished rules (e.g. detailed requirements of services related to electronic signatures and service providers). The elaboration of the enacting clauses still lies ahead. During this careful elaboration process the above mentioned dangers can still be eliminated.

Bibliography

1. ENDRŐDI Csilla - HORNÁK Zoltán: **Az elektronikus aláírásról szóló törvény elemzése**
2. Community framework for electronic signatures
3. Az 1999/93/EK direktíva összefoglalója
4. Elektronikus aláírás: jogszabályi és szabványosítási kérdések
5. http://www.euroastra.com/mime/cikkek/torvterv.html (European Electronic Signature Standardization Initiative (EESSI) honlapja)
6. http://europa.eu.int/scadplus/leg/en/lvb/l24118.htm
7. http://www.ict.etsi.org/