**International Review of Social Sciences and Humanities**
**Vol. 4, No. 2 (2013), pp. 43-53**
**www.irssh.com**
**ISSN 2248-9010 (Online), ISSN 2250-0715 (Print)**

# Comparative Analysis of Handwritten, Biometric and Digital Signature

**Tomáš Bálint**
(Corresponding Author)
Department of Applied Mathematics and Business Informatics
Faculty of Economics, Technical University of Košice
Nemcovej 32, 040 01, Košice, Slovak Republic
E-mail: Tomas.Balint@tuke.sk

**Jozef Bucko**
Department of Applied Mathematics and Business Informatics
Faculty of Economics, Technical University of Košice
Nemcovej 32, 040 01, Košice, Slovak Republic
E-mail: Jozef.Bucko@tuke.sk

(Received: 27-8-12 / Accepted: 10-10-12)

**Abstract**
Information and communication technologies have influenced a whole variety of business processes in the past few years. New emerging methods and techniques are trying to find their place and application in enterprises. This is the case of documents' signing, too. Handwritten signature has been used as a traditional method for centuries. However, it seems today that it cannot provide a satisfactory level of security and confidence anymore. Therefore, these days new biometric and digital signature schemes are gaining on popularity. The paper provides a comprehensive study of three approaches to the problem of documents' signing. Traditional handwritten, biometric data based, and digital signatures are defined, characterized, and analyzed. Based on the technical characteristics of each signature method, corresponding utility functions are derived. These functions are built upon the profit functions which represent profits gained by the usage of various cryptographic and authentication methods. In the same time basic cost analysis is performed in this paper. Finally, based on the findings and conclusions presented in the paper, further studies in this perspective field will be subject of our interest in the future.

**Keywords:** biometrics, cost analysis, digital signature, handwritten signature.

## 1. Introduction

Making of contracts and closure of various deals is one of the key business processes. Important part of this process is the validation of the deal by different methods. The vast usage of information and communication technologies (ICT) in the recent years has modified also this field of business administration. The ICT development caused the necessity of

transition from traditional paper exchange of documents towards the electronic one. Traditionally, handwritten signature has been used when closing a deal. Nowadays new progressive methods, such as biometric and digital signatures, are gaining on popularity. These new techniques modify the way new deals are closed. Various technical, as well as economical, problems have to be taken in consideration when using these signing methods.

The key factor in the process of transition towards fully electronic communication is the creation of public-key infrastructure (PKI) [5] with its core element – digital signature which represents digital identity of a subject in digital world [2]. Digital signature, according to Directive 1999/93/EC [7], fully replaces the traditional handwritten signature. Even though this signature is more safe than standard, the level of confidence in it is not as high as would be expected. The main reason of this situation is the lack of users' knowledge about the underlying technology and the complexity of digital signature's use. Traditional handwritten signature is something everybody sees. On the other hand, digital signature is basically a digital file created by the machine which is hard to verify by naked eye. Both types of signature can represent the same person but the majority of people believe more in traditional signature than in digital. For this reason, a third type of signature evolved – biometric signature. This signature type is an intermediary step in the process of transition from handwritten to digital signing of documents. It uses the advantages of both types – physical basis of traditional signature and digital properties of digital signature [14].

It has to be taken in consideration that these technologies change already existing business processes and the way how they are functioning. Internet and digital communications modify fundamentally the approach of subjects to the business transactions' realization. This change implies in the same time the rise of new methods of criminality which leads to uncertainty and mistrust among business partners, too [6]. Therefore, digital signature process has to comply with security policies of every company which uses it. If these policies are missing, there exist high risks of signature misuse which lead to the uncertainty in business relations. On the other hand, existing management of information security does not mean automatically that the information security has been adequately provided [16].

The main motivation to write this paper is the fact that above mentioned modern digital methods of signatures are adopted worldwide these days. In addition, these methods can be considered as an important element of business innovation [10; 17]. In the same time, information security problems are not considered today only as a technological issue, but also as an economics problem [1; 3]. Due to this fact, the last section of the paper deals with financial aspects of modern signature methods' use.

## 2. Signature

The notion of the signature is generally vaguely defined. Everybody implicitly knows what the word "signature" means but it is very complicated to define an exact meaning of this term. In this section we are trying to clarify basic concepts related to different types of signatures.

## 2.1 Handwritten Signature

Handwritten signature is the oldest and the most frequently used method for the validation of various contracts. Its main advantage is the ease of use. Subject can sign a document with any writing instrument available at the moment. Moreover, personal meeting and on site signing of document is still considered by general public as the most trustworthy method of document exchange and validation.

Historically, expression "signed, sealed, and delivered" was used [4]. It describes the fact that, as a legal requirement, document had to be not only signed, but also provided with the seal of signer. Furthermore, this document had to be delivered to the other subject involved in the contract. Thus, the document was valid only if all three steps were finished. Nowadays, simple signature is enough to validate a document. This historical change in the document validation process is due to the increasing number of contracts signed every day.

Handwritten signature is still very popular and prevailing technique for different types of legal actions. The problem is that sometimes a document can be valid even if not signed or invalid even if signed, as it is described in [15]. In the same time, this type of signature is not sustainable in globalized and fast moving world as we can experience it today. The need for faster and more digitized communication is stronger. Therefore new methods of signature are developed.

## 2.2 Biometric Signature

Biometric signature represents the attempt to shift traditional handwritten signatures into the digital world. Before we can define this type of signature, several concepts related to information security and biometrics has to be clarified. [2]

### 2.1.1 Preliminaries

Biometric systems have their specific properties and behaviour. Key characteristics are resumed in [11]. Authors mention following properties:

- Different biometric samples of the same person will never be the same.
- Biometric systems make errors - sometimes valid users are rejected and vice versa (see below).
- Biometric data are not secret.
- The role of the output device is crucial, and this device must be trusted or well secured.
- The biometric system should check user's liveness - prevents the use of simple biometric data copies.
- Biometrics is good for user authentication. They cannot be used to authenticate data or computers because these systems do not have biometric characteristics.

Another important issue which is present in the case of biometric systems is their accuracy. Accuracy is a parameter of biometric system which defines its reliability. To express this parameter, two measures are usually used. First is the False Acceptance Rate (FAR) which expresses the ratio between all signatures which were accepted even when they are not valid and all signatures. Second, False Rejection Rate (FRR), represents all valid signatures which are not accepted. These characteristics together define the accuracy of biometric system [8].

### 2.1.2 Biometric Signature

In this paper we consider biometric signature as a digital data representation of handwritten signature with its unique characteristics such as pressure applied to signature pad, speed of signature, and graphical representation of the signature pattern itself. It has to be pointed out that signature validity depends on the message which has been signed. Therefore, the modification of the message content after signing process results in the invalidation of the signature. [8; 9; 12]

Biometric signature in this form represents only electronic version of handwritten signature. This fact implies that somebody aware of the handwritten signature pattern of a person can successfully try to imitate it.

Two important properties of biometric signatures have to be taken in the consideration. First of all, biometric signatures can be easily visually verified. Furthermore, it is possible to positively testify that the signature belongs to the person who actually signed the data. On the other hand, exact proof (based on mathematics methods) is hard to compute [11].

## 2.3 Digital Signature

The most discussed signature solution today is the implementation of digital signatures. This technique of data verification is starting to gain on popularity these days. There are various

factors to consider when thinking about deployment of digital signatures in business environment.

Digital signature is based on public-key cryptography [5]. In this concept a pair of keys, public and private, is used. Subject can provide confidentiality, i.e. encryption, to his data with public key of the second subject involved in the transaction. Private key on the other hand serves to the purposes of authentication, integrity, and non-repudiation. Digital signature schemes are used to create electronic signature which is more legislative term. [5]

According to the EU parliament directive, which the member states of the EU should follow in the scope of the Electronic signature law, the electronic signature is defined as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication." [7]. Under the term of verification European Union understands particularly verification of a signatory, i.e. the person who creates the data in the electronic form (electronic signature) to the other electronic data (electronic document). Apart from the signatory's verification, the electronic signature allows electronic documents verification (whether verified and signed document are identical), as well as verification of signature creation time (i.e. that the time stated in the signature has not been modified later on). If validity of electronic document is verified by electronic signature, which represents data creating a base for verification of signature and document, then the signature could be created only by the owner of the corresponding data for creation of the electronic signature itself. The electronic signature, likewise authentic signature, is a result of some process, resulting from a decision of the signatory, whose function is to confirm the will of this person, or his or her identity. Unlike own-hand signature, the electronic signature is result of technological process which is linked to the signed document. This means that the electronic signature is changing and is different for every new-signed document.

The electronic signature is information attached to electronic document or information logically connected with the electronic document in any other way. An advanced electronic signature means, according to the Directive, an electronic signature which meets the following requirements [7]:

- it is uniquely linked to the signatory,
- it is capable of identifying the signatory,
- it is created using means that the signatory can maintain under his sole control,
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Nowadays, the conditions and requirements on the attributes of electronic signature fulfil the best digital signature. The electronic signature is often defined to be a digital signature, but these terms are not the same. The digital signature is only one possibility of electronic signature. The digital signature is a tool, which is exactly technologically defined on the basis of the asymmetric cryptography. On the other hand, the electronic signature is much wider term. Legislators established it, with aim to avoid limitation of law to only one method of electronic signature. The aim was being open to the other methods, or to future cryptographic methods, which would fulfil conditions of law concerning the electronic signature. [5]

It should be also pointed out that in the case of digital signatures the problem of verification as presented with biometric signatures is nonexistent. Due to the construction of digital signature via mathematically strong cryptographic algorithms, the verification is pretty easy with appropriate mathematical methods. Therefore, we can certify with 100% certainty that the signature is valid or invalid. The problem of FAR and FRR is not present in case of this type of signatures. However another problem occurs here. We can prove only that the signature belongs to the subject defined in its structure but we cannot prove that this subject was really the person who signed data.

Another important advantage of digital signatures is in variety of their use. Handwritten and biometric signatures can be used only for the authentication and authorization purposes. On

the other side, digital signatures can be used not only for the subject identification, but also for the signature of applications and their source code or servers' identification.

## 3. Technical Analysis

Biometric and digital signatures are methods which are based on sophisticated cryptographic primitives. Therefore we have to focus in the first place on basic characteristics of cryptographic systems. Traditionally following five characteristics are taken in consideration when evaluating any security system [12]:

- **Confidentiality (privacy)** - keeping information secret from all but those who are authorized to see it
- **Data Integrity** - ensuring information has not been altered by unauthorized or unknown means
- **Entity Authentication (identification)** - corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.)
- **Authorization** - conveyance, to another entity, of official sanction to do or be something
- **Non-repudiation** - preventing the denial of previous commitments or actions

Signatures, in the first place, prove somebody's identity (authentication). In security theory three basic types of authentication methods are usually defined [12]:

- **Something to have (STH)** - usually a physical device, e.g. grid card, USB token, smartcard
- **Something to know (STK)** - this category includes standard passwords, Personal Identification Numbers (PINs), and secret and private keys
- **Somebody to be (STB)** - everybody has his/her personal physical characteristics which are unique (biometrics), such as DNA, signature, fingerprints, retinal patterns, voice, hand geometry, etc.

## 3.1 Comparison of Elementary Cryptographic Characteristics

The three types of signatures, which we are analyzing in this paper, do not satisfy identically all cryptographic characteristics which were described in the previous section. They cannot comply with these characteristics identically because each type of signature is based on different mechanism. Therefore it is important to study their individual level of compliance.

Handwritten signature is the simplest one. It is pretty easy to create this type of signature. On the other hand, it cannot provide all properties which are analyzed in this section. Obviously, handwritten signature proves somebody's identity, hence we can conclude that it provides authentication and non-repudiation (signer cannot deny the fact that he/she signed the document). However, in case of handwritten signature, we cannot say that signer was authorized to sign the document. This traditional type of signature does not include mechanisms for document confidentiality, integrity, and authorization. It is not difficult to forge a document, e.g. via fax (for further reference see [15]). Furthermore, we cannot forget the fact that handwritten signature is document-independent, i.e. the change of the document content does not cause invalidation of the signature.

Biometric signature is more sophisticated. It adds dynamic characteristics, so called signature geometry, to the signature itself. For this reason, biometric signature is not only a simple digital image of handwritten signature, but it is a complex set of data. Furthermore, biometric signature is interconnected with the document itself, hence document-dependent (change in the document causes invalidation of signature). This characteristic provides integrity. Biometric signature, in the same time, can provide also authentication and non-repudiation, because these properties are inherited from handwritten signature. We have to remember that biometric signature is basically digitalized version of traditional handwritten signature. If the

biometric data are used as a digital key they can serve also for the purposes of encryption, and provide document confidentiality.

Digital signature, described in section 2.3, is the most abstract cryptographic primitive of all three. The subject has to rely on sophisticated mathematical algorithms, when he wants to use digital signature. This particular type can provide all five key cryptographic characteristics because of the way how it is designed (for further reference see [12]). Summarized comparison of the cryptographic characteristics for handwritten, biometric, and digital signatures can be found in Table 1.

**Table 1** Comparison of different signature cryptographic characteristics

| | Handwritten signature | Biometric signature | Digital signature |
|---|---|---|---|
| Confidentiality | No | Yes | Yes |
| Integrity | No | Yes | Yes |
| Authentication | Yes | Yes | Yes |
| Authorization | No | Yes | Yes |
| Non-repudiation | Yes | Yes | Yes |

## 3.2 Comparison of Authentication Methods

The main purpose of a signature is usually the identification of the subject. In the beginning of section 3, three types of objects, which can be used for this purpose, were described.

Handwritten and biometric signatures share common characteristics. First of all you have to know something, i.e. the way your signature looks like, and then you have to be somebody - signature has biometric characteristics as for example speed of writing. Thus, we can conclude that in this case we deal with two-factor authentication. Furthermore, the shape of your signature is not secret, anybody can find the way you sign documents just by finding an old one signed by yourself.

On the other hand, digital signature is not connected with you as a human being, hence independent from your biometric characteristics. You can use this type of signature when you know a corresponding password or PIN code protecting the private key, i.e. you need to know something. The security of digital signature system can be improved when the subject will use an USB token to store this private key. In this situation, subject needs also something to have, hence it is a case of two-factor authentication. A summary of different authentication methods for all three signature types is presented in Table 2.

**Table 2** Comparison of signature properties with different authentication methods used

| | Handwritten signature | Biometric signature | Digital signature |
|---|---|---|---|
| Something to have (STH) | No | No | Yes |
| Something to know (STK) | Yes | Yes | Yes |
| Somebody to be (STB) | Yes | Yes | No |

## 3.3 Utility Derived From the Usage of Different Signature Methods

Every type of before mentioned signature's types can provide to the user a certain degree of utility. It was demonstrated in sections 3.1 and 3.2 that each of three studied types of signature has different capacities to provide elementary cryptographic characteristics and to be compatible with 3 authentication methods. Utility can be then expressed as a linear combination of individual profits gained by each particular characteristic. Therefore we can construct relation (1).

$$U = f(\pi_c, \pi_i, \pi_a, \pi_{aa}, \pi_{nr}, \pi_{STH}, \pi_{STK}, \pi_{STB}) \quad (1)$$

In this relation, $U$ represents utility derived from the usage of different signature methods and $\pi_i$ are profit functions for each component. The meaning of each profit function is in Table 3.

**Table 3** Profit functions

| | | | |
|---|---|---|---|
| $\pi_c$ | Profit gained by confidentiality | $\pi_{nr}$ | Profit gained by non-repudiation |
| $\pi_i$ | Profit gained by integrity | $\pi_{STH}$ | Profit from STH authentication method |
| $\pi_a$ | Profit gained by authentication | $\pi_{STK}$ | Profit from STK authentication method |
| $\pi_{aa}$ | Profit gained by authorization | $\pi_{STB}$ | Profit from STB authentication method |

Based on these formal definitions we can design utility functions for each of three studied types of signatures. To determine the presence of each technological characteristic we use the results which are summarized in Table 1 and Table 2. The utility function for handwritten signature is as follows (2):

$$U = f(\pi_a, \pi_{nr}, \pi_{STK}, \pi_{STB}) \quad (2)$$

In the case of biometric signature the only characteristic which is not supported is the authentication by something that subject has to have (STH). The user of biometric signature does not need any type of special device for the purposes of signature creation and validation. For this reason, the utility function has only one profit function missing $(\pi_{STH})$. We can express the corresponding utility function which defines the utility derived from the use of biometric signature in the following way (relation (3)).

$$U = f(\pi_c, \pi_i, \pi_a, \pi_{aa}, \pi_{nr}, \pi_{STK}, \pi_{STB}) \quad (3)$$

The last type of signature which we are studying in this paper is digital signature. It provides, together with biometric signature, all five cryptographic characteristics in the way they were defined in subsection 3.1. The difference, when compared to biometric signature, is in the support of three authentication methods. Digital signature does not support authentication based on something that subject is (something to be (STB) authentication method). Hence, the profits function $(\pi_{STB} = 0)$ in the case of digital signature. The utility function which corresponds to this coefficients' vector is then as follows (4):

$$U = f(\pi_c, \pi_i, \pi_a, \pi_{aa}, \pi_{nr}, \pi_{STH}, \pi_{STK}) \quad (4)$$

Based on the utility function $U$ we can compare financial profit gained by the usage of each type of signature and in this way compare them. From (2) we can conclude that handwritten signature produces the lowest utility and therefore also the lowest profit. In case of biometric and digital signature the difference is only in one coefficient - $\pi_{STH}$ is missing in case of biometric signature. In the same time, the last coefficient $\pi_{STB}$ is not present in digital signatures. The relative profitability between these two options is therefore defined only by the relation between these two profit functions. If $\pi_{STH} > \pi_{STB}$, the usage of digital signatures is more profitable than the usage of biometric signature, and vice versa. More detailed evaluation of these utility functions needs further empirical studies which will provide estimates of each respective profit function. The utility derived from the usage of each analyzed signature type is illustrated in Figure 1.

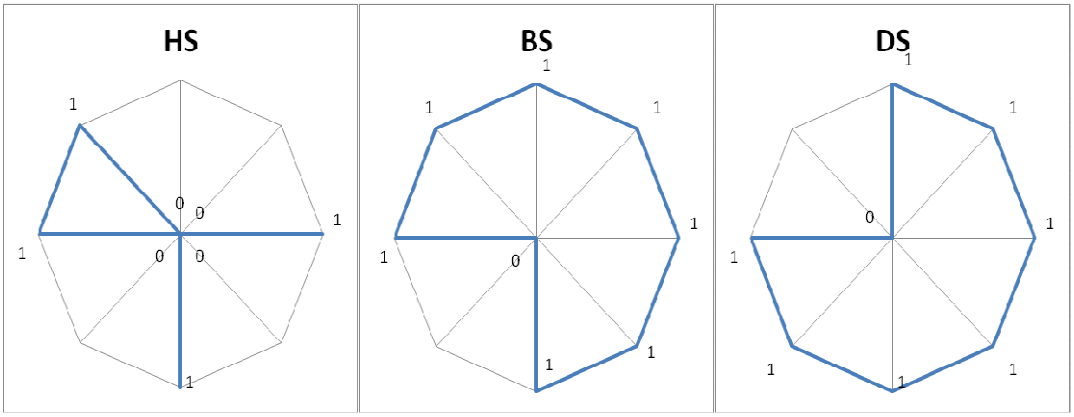


**Figure 1:** Comparison of utility derived from each signature type

## 4. Cost Analysis

In the previous sections we have studied technical properties of all three signature types. We have to realize that these properties can be obtained at certain costs. Tradeoffs between desired technical parameters and their implementation can be sometimes important. For this reason, we analyze costs of solutions based on handwritten, biometric, and digital signatures. Cost analysis in this section is divided in two domains: acquisition costs and operational costs. In the following analysis we assume that subject who signs a document has at least basic literacy skills, i.e. he/she can read and write.

## 4.1 Acquisition Costs

Acquisition costs can represent an important decision criterion when company thinks about adopting or refusing an investment. Therefore, a careful feasibility study has to be carried out before the project is accepted. In case of handwritten signature these costs are virtually non-existent because there are no prerequisites for the adoption of this signature type.

The situation is completely different in case of biometric and digital signature. For the adoption of biometric signature two types of investments need to be performed before the use. A company has to buy an appropriate hardware, i.e. some sort of tablet or signing pad which will be used to enter the signature itself. Second necessary component in this case is some sort of recognition software. This software can be sometimes a little bit expensive, especially when a high performance is expected from the biometric system.

Digital signatures' systems have approximately same prerequisites as biometrics. The user needs some specific hardware to store securely his/her signature's data. For these purposes an USB token or smartcard can be used. Furthermore, corresponding software needs to be installed. These tools provide signing functions to the end user. In case of digital signature, the person who signs has to have also his personal digital certificate which contains private key. This type of key is necessary for the operation of document signing. The comprehensive overview of these prerequisites is in Table 4

**Table 4** Acquisition costs of different signature types

| Handwritten signature | Biometric signature | Digital signature |
|---|---|---|
| *No acquisition costs* | Hardware for signatures (tablet, signing pad, …)<br>Recognition software | Digital certificate with Public & Private Key<br>Secure storage device (USB token, Smartcard, …)<br>Software for digital signature processing |

## 4.2 Operational Costs

After initial investment was made, question of operational costs arises. An investment usually implies not only acquisition costs but it is necessary also to invest in it during the whole duration of project. This applies the implementation of different signature schemes as well. For example, in case of handwritten signature, two subjects signing a document need to meet together for this purpose. This fact can be interpreted as costs for signature realization, i.e. transport costs.

The situation is much more complicated when biometric signature is used. All parties still need to meet each other when signing a document, as in the case of handwritten signature. Furthermore, because biometric signature system is a digital one, it has a software part which has to be updated on regular basis. Special attention has to be devoted to the updates of software database which contains digital patterns used for the purposes of signature comparison. This database needs to be kept up to date in order to permit authorized subjects to sign documents. This can be a particularly difficult task in large systems.

In case of digital signatures the situation is slightly different. There is no need to meet together because the documents can be signed with private keys and then sent to the business partner over Internet. However, a new problem arises in this case. Usually certification authorities issue digital certificates, which are needed for the purposes of subject identification and as a proof of private key's possession, with an exactly defined validity period. After this time, the certificate and private key which is connected with it are not valid anymore. For this reason, a subject needs to obtain a new digital certificate (or renew the old one). Therefore this property of digital certificates can generate significantly important operational costs, especially in large organizations where hundreds or even thousands of certificates have to be renewed. We cannot forget also the costs of regular software updates. These costs have also the capacity to change significantly the results of cost-benefit analysis for the implementation of digital signatures' system. The overview of operational costs invoked by the three signature schemes is in Table 5.

**Table 5** Operational costs of different signature types

| Handwritten signature | Biometric signature | Digital signature |
|---|---|---|
| Need to meet each other | Need to meet each other<br>Biometric signatures' database need to be updated on regular basis | Software updates scheduled on regular basis<br>Digital certificates renewal |

## 4.3 Total Costs

The total costs for each signature type consist of initial acquisition costs and regular operational costs. In the case of handwritten signature this sum of costs corresponds directly to the operational costs because acquisition costs are zero.
Biometric and digital signature types involve acquisition as well as operational costs as was shown in the previous subsections. Total costs are then the sum of both partial cost functions.

## 5. Conclusions

The paper presented three different approaches to the problem of documents' signing. Traditional handwritten signature is still the most popular one all over the world. On the other hand, new emerging digital methods of signing, such as biometric or digital signatures, are gaining on popularity. The biggest advantage of these technologies is the use of strong cryptographic primitives which assure better verification of signatures, hence better proof of document validity and authenticity.

However, there exist still barriers which prevent adoption of these progressive methods of signing. The biggest identified problem is the complexity of technologies used in case of biometric and digital signatures. People in general do not understand well technologies; they simply want that the systems work as smoothly and easily as possible. In case of biometric signatures, the problem of biometric data's storage cannot be neglected. People do not like to give their personal data to third parties.

In the same time all these signature types can provide some elementary cryptographic and authentication services for the signer. The paper presented a formal definition of utility functions which can appropriately express an individual level of utility gained from the use of each respective type of signature scheme. The biggest utility can be obtained when biometric and digital signatures are used. The task of choosing between them is reduced to the comparison of profits from two authentication methods: something to have (digital signature) versus somebody to be (biometric signature).

The last, but not the least, problem is the cost of hardware and software equipment needed for their functionality. Costs can be divided in two domains: acquisition and operational costs. The paper presented the composition of both cost types for each signature mechanism.

The theoretical background and proposed framework for the assessment of modern signature systems represent a solid starting point for the further research which will provide, based on the empirical evidence, further insights in the process of biometric and digital signature adoption in the business environment.

## Acknowledgement

The research was realized within the national project "Security models of distributed systems providing electronic services" (Contract No. 1/0945/12) funded by Grant Agency for Science; Ministry of Education, Science, Research and Sport of the Slovak Republic.

## References

[1] R. Anderson and B. Schneier, Economics of information security, *IEEE Security and Privacy*, 3(2005), 12-13.

[2] T. Bálint, J. Bucko and M. Esser, Digital identity, risks of its misusage and its importance for the development of e-business (in Slovak), In *Hradec Economic Days 2011: Economic Development and Management of Regions: International Scientific Conference: Peer-Reviewed Conference Proceedings: Part 1*, (2011), Hradec Králové: Gaudeamus.

[3] R. Bojanc and B. Jerman-Blazic, An economic modelling approach to information security risk management, *International Journal of Information Management*, 28(2008), 413-422.

[4] M.C. Bromby, Identification, trust and privacy: How biometrics can aid certification of digital signatures, *International Review of Law, Computers and Technology*, 24(1) (2010), 133-141.

[5] J. Bucko and P. Mihók, *E-Services in Banking (in Slovak)*, (2008), Košice: Technická Univerzita, Ekonomická Fakulta.

[6] R. Delina and R. Dráb, Socio-economic aspects of trust building for the electronic business platforms, (in Slovak), *E+M Ekonomie a Management*, 13(4) (2010), 110-122.

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

[8] A. Gupta, Y.A. Tung and J.R. Marsden, Digital signature: Use and modification to achieve success in next generational e-business processes, *Information & Management*, 41(5) (2004), 561-575.

[9] J.M. Lenz, Biometric signature verification– A sign of the times? *Biometric Technology Today*, 16(4) (2008), 9-11.

[10] S. Mason, Electronic signatures— evidence: The evidential issues relating to electronic signatures — part 1, *Computer Law & Security Report*, 18(3) (2002), 175-180.
[11] V. Matyas and Z. Riha, Biometric authentication – security and usability, *In Proc. of IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, (2002).
[12] A.J. Menezes, P.C. Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography*, (1996), CRC Press.
[13] P. Mihók, J. Bucko, R. Delina and D. Paľová, Trust and security in collaborative environments, In *Enterprise Interoperability 3: New Challenges and Industrial Approaches*, (2008), London: Springer Verlag.
[14] S. Mohammadi and S. Abedi, ECC-based biometric signature: A new approach in electronic banking security, In *2008 International Symposium on Electronic Commerce and Security*, (2008).
[15] B. Schneier, *Why Do We Accept Signatures by Fax*? (2008), URL http://www. schneier.com/essay-220.html.
[16] E.Y. Yildirim, G. Akalp, S. Aytac and N. Bayram, Factors influencing information security management in small- and medium-sized enterprises: A case study from turkey, *International Journal of Information Management*, 31(2011), 360-365.
[17] S. Zaba, Digital signature legislation: The first 10 years, *Information Security Technical Report*, 11(1) (2006), 18-25.