Digital Signature in Organisations

Ivana Lukašíková

Bachelor Thesis
2010

Tomas Bata University in Zlín
Faculty of Humanities

Univerzita Tomáše Bati ve Zlíně
Fakulta humanitních studií
Ústav anglistiky a amerikanistiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ivana LUKAŠÍKOVÁ**
Studijní program:	**B 7310 Filologie**
Studijní obor:	**Anglický jazyk pro manažerskou praxi**
Téma práce:	**Elektronický podpis v organizacích**

Zásady pro vypracování:

Definujte problém, který je cílem práce.
Proveďte literární a informační rešerši k tématu elektronického podpisu.
Analyzujte současný stav a možnosti poskytované organizacím certifikačními autoritami.
Proveďte SWOT analýzu z pohledu firem a občanů na technologii elektronického podpisu.
Vyhodnoťte výsledky své práce.

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Bosáková, Dagmar, Alena Kučerová, Jaroslav Peca and Pavel Vondruška. Elektronický podpis. Olomouc: ANAG, 2002

Cambell, Dennis. E-commerce and the Law of Digital Signature. New York: Oceana Publications INC., 2005

Gran, Gail. Understanding Digital Signatures: Digital Signatures (Advances in Information security). Establishing Trust over the Internet and other Networks. New York: McGraw-Hill, First edition, 2009

Mates, Pavel and Vladimír Smejkal. E-GOVERNMENT v českém právu. Praha 1: Linde Praha, a. s., 2006

Piper, Fred, Simon Blake-Wilson, John Mitchell, eds. Digital Signatures Security and Controls. Toronto: Information Systems Audit and Control Foundation, 2000

Vedoucí bakalářské práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav aplikované informatiky

Datum zadání bakalářské práce: **7. ledna 2010**

Termín odevzdání bakalářské práce: **7. května 2010**

Ve Zlíně dne 7. ledna 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta humanitních studií
L.S.
1

prof. PhDr. Vlastimil Švec, CSc.
děkan

A. Lengálová
doc. Ing. Anežka Lengálová, Ph.D.
vedoucí katedry

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby [1];
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3 [2];
- podle § 60 [3] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 [3] odst. 2 a 3 mohu užít své dílo – bakalářskou práci - nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům.

Prohlašuji, že

- elektronická a tištěná verze bakalářské práce jsou totožné;
- na bakalářské práci jsem pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně 2.5.2010 .... Ivana [illegible] ....

[1] *zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:*

(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.

(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Tato práce s názvem „Elektronický podpis v organizacích“ shrnuje základní fakta o elektronickém podpisu. Vyzdvihuje jeho vysokou bezpečnost, která je zaručena několika faktory najednou. Zabývá se také certifikačními autoritami, jejich funkcemi a popisem kvalifikovaných certifikačních autorit působících v České Republice. Rozebírá také typy certifikátů a jejich platnost v jiných zemích. Jsou zde také popsány základy asymetrického šifrování. Popisuje také možné problémy spojené s používáním elektronického podpisu, jako je např. jeho zneužitelnost či problémy s dlouhodobou archivací elektronicky podepsaných dokumentů. Snaží se zachytit důvody nízkého zájmu o elektronický podpis a zjistit podvědomí a názor veřejnosti na elektronický podpis. Nabízí také možné řešení na zvýšení použitelnosti elektronického podpisu a zlepšení obecného náhledu na elektronický podpis.

Klíčová slova: elektronický podpis, zaručený elektronický podpis, certifikační autorita, kvalifikovaná certifikační agentura, certifikát, kvalifikovaný certifikát, bezpečnost, kryptografie, šifra

ABSTRACT

This thesis “Digital Signature in Organizations” summarizes the basic facts about Digital Signature. It emphasizes the high level of safety of a Digital Signature which is guaranteed by several factors at once. It also deals with the certification authorities, their functions and list of qualified certification authorities operating in the Czech Republic. Thesis also deals with the types of certificates and their validity in other countries. There are also described basics of asymmetric cryptography. It also describes the potential problems associated with the use of Digital Signatures, such as his security risks or problems with long-term archiving of electronically signed documents. It tries to capture the reasons for the low interest in the Digital Signature and establish awareness and public opinion on the Digital Signature. It also offers a possible solution to increase the usage of Digital Signatures and improve the opinion on the Digital Signature.

Keywords: Digital Signature, Advanced Digital Signature, Certification Authority, Qualified Certification Agency, Certificate, Qualified certificate, Security, Cryptography, Cipher

ACKNOWLEDGEMENT

I would like to gratefully and sincerely thank doc. Mgr. Roman Jašek, Ph.D. for his guidance, understanding and patience. Then I would like to thank my father ing. Petr Lukašík, for professional help with my thesis. Finally, I would like to thank my family and friends for their physical support, which they have given me during my studies.

CONTENTS

INTRODUCTION

Hand written signatures are commonplace, but there is now another possible way to acknowledge volition – a digital signature. Thesis will try to describe all positives and negatives of a digital signature and propose some solution how to increase and improve the usage of a digital signature. This thesis will demonstrate the basics of coding and will explain how a digital signature is created. Types of certificates and certification authorities will be described, and different alternatives will be given for ways to gain a certificate in the Czech Republic. Furthermore, this thesis will discuss the current status of digital signature legislation in the Czech Republic as well as in the E.U.

Ultimately, this thesis will prove that a digital signature has the same importance as a hand written signature. The authenticity of a digital signature should not be challenged, despite the public's generally held opinion that the security of a digital signature is insufficient. In fact, it is easier to forge a hand written signature than a digital signature. Digital signature is worse imitable and less exploitable than the handwritten signature. The security of a digital signature is guarantee by an Act No. 227/2000 Coll., on Digital Signature in the Czech Republic. The purpose of the Act is to create equal conditions for the use of a digital signature.

There is also a general lack of interest to set up a digital signature. Digital signature is used mainly by managers, businessmen and information technology workers. Hopefully the public distrust of digital signatures will gradually disappear, because digital signatures make life easier. People spend a lot of time in banks or offices, whereas using digital signatures would minimize this time or free it up altogether.

I. THEORY

1 BASIC FACTS ABOUT DIGITAL SIGNATURE

Digital signature is created by a data in electronic form, which are joined to the data message or are logically associated with it. These data allow verification of the signatory's identity in relation to the data message. (Mlýnek 2007, 126 s.)

Digital signature is practically generated from a huge number of ones and zeros. Digital signature is a complex mathematical act, reaching sizes up to 4096 bits. Digital signature is unique and has the same usage as handwritten signature. In the addition of handwritten signature, digital signature has explanatory function. This function means, that document belongs to the electronic signature and the content of the document is original. (Požár, 2005)

Electronic signature is usually used in internet banking, communication with public administration bodies and the financial transactions in general.

Electronic signature is a legal concept, but the digital signature is a technical term. Digital signature is a concrete realization of an advanced electronic signature. (Mlýnek, 2007)

1.1 Digital Signature versus Handwritten Signature

Digital signature (the same as handwritten signature) is the result of a process, which begins with the decision of the signatory. Task of signature is to affirm the will of the person or her identity. (Mates 2006)

As the definition says, the electronic signature isn't just a numeric code which is assigned to the user on some office and than this code is written by the user on each document. This idea (if there is any idea) circulating in the heads of a relatively great part of the public and thus raises the fear of a simple breaking of digital signature.

Individuality of handwritten signature is obtained by creating a dynamic stereotype of writing that can be described as a set of conditioned reflexes. These conditioned reflexes depend on regular practice. The authenticity of the handwritten signature is verified by using various methods such as: the method of observation, analytical, synthetic, and comparative methods. All these methods are mainly subjective. Digital signature is, since the time of making a decision up to verifying the authenticity an objective result of technological process. We are talking about variable-signature, which is worse imitable and less exploitable than the handwritten signature. (Mates 2006)

1.2 Importance of Digital Signature Usage

Electronic signature increases the number of documents that can be processed electronically. Electronic signature can be used for signing a document of any length and content (Požár 2005).

Sign and verify documents can be much faster with digital signature than with the handwritten signature. There can be signed things by digital signature such as: diskette, photograph, database access, etc. (what may be problem for handwritten signature). (Mates 2006)

2 LAW ABOUT DIGITAL SIGNATURE IN THE CZECH REPUBLIC

Act No. 227/2000 Coll., on Digital Signature ensures the legal aspects of electronic signatures, electronic signs, the providing of certification services and other necessary services related to these act.

The purpose of the Act is to create equal conditions for the use of digital signatures. The terms which are defined by the law: electronic signature, advanced electronic signature, certificate, qualified certificate, the certification service provider, accredited provider of certification services. These terms will be discussed below in more details. Levels of protection and the various powers of these terms are strictly defined and valid in the Czech Republic. The Act establishes also the obligations of the signatory .In communication with the public administration should be used just advanced electronic signatures and qualified certificates. These qualified certificates are issued by accredited certification agencies, which are established by the Ministry of Interior of the Czech Republic. (Mlýnek 2007)

3 KINDS OF DIGITAL SIGNATURES ACCORDING THEIR SECURITY

3.1 Digital Signature

“Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". This electronic signature is based on asymmetric cryptology. In this electronic signature we can’t be sure that the holder of the key is also the owner of the key. (Mazzeo 2004, online)

3.2 Advanced Digital Signature

Advanced Electronic Signature had to fulfil these rules:

- 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 that any subsequent change of the data is detectable"

Usage of advanced electronic signature warrant that the text which was send is original and wasn’t changed by hacker. This electronic signature guarantee integrity and authentication of enclosed document. (Mazzeo 2004, online)

3.3 Advanced Digital Signature which is based on Qualified Certificate created by an Qualified Certification Agency

According European Law this type of electronic signature had to fulfil these rules:

- the indication that the certificate is issued as a qualified certificate;

- the identification of the Certification Authority and the State (European or foreigner) in which it is established;

- the name (or pseudonym) of the signatory, to identify her/him;

-signature-verification data which correspond to signature-creation data under the control of the signatory;

- the indication of the period of validity of the certificate;-the identity code of the certificate; and

- the advanced electronic signature of the certification-service-provider (Certification Authority). (Mazzeo 2004, online)

Advanced electronic signature based on a qualified certificate from an accredited certification service provider is the most credible. For contact with public authorities we have to use only advanced digital signature based on qualified certificate. For ordinary communication we may use any of the above mentioned signatures.

4 CERTIFICATION AUTHORITY (CA)

The public key can be gained from the owner of the key or we can find it placed in the Internet. If the recipient needs the authenticity of the document, we will use services provided by one of the qualified certification authorities. In other words it means that the public key is genuine. Today, the use of qualified certification authority is almost necessary. Digital signatures is used mostly by citizens or companies for communicate with the public administration. For these acts it is necessary to have a credible third party, which the qualified certification authority is. Therefore, most digital signatures can’t exist without the protective wings of the certification authority.

According to the law, the certification authority is a private entity providing a service which consists in connecting individuals with their public-key. This connection is provided by

certificate. (Mates 2006)

The certification authority acts as a third independent intermediary between two communicating sites. Certification authority issue Certificates and Certificate Revocation Lists. (Budiš 2008)

4.1 Functions of Qualified CA

1 Authentication and authorization of users and other certification authorities

2 Saving of data and their distribution

3 Issuance of certificates and administrative functions of certificates

4 Notarial function (Budiš 2008, 70s.)

4.2 Qualified CA in the Czech Republic

In the Czech Republic there are three qualified CA: The first certification authority, as, Czech Post and eIdentity, a.s. From a consumer perspective point of view it does not matter which of those qualified authorities choose. For example: The first certification authority, a.s. has the biggest number of branches, or the PostSignum has the cheapest certificate: 190Kč per year. The certificate is normally issued for one year. After expiry of certificate, client must re-apply for a new one. Re-issuing of certificate is paid by client. One of the services which is provided by agencies are warning the customer about the impending end of the validity of certificate. This actually provides the continuity of certificates and excludes the period without an electronic signature. (eAgri.cz, 2010)

Applying for accreditation of certification service provider is 100 000 CZK (Zákon č. 227/2000 Sb., o elektronickém podpisu)

4.2.1 První certifikační agentura, a.s.

První certifikační agentura, a.s.is the biggest certification agency in the Czech Republic.This agency provide its services also in the Slovak Republic. Places of registration are branch points of ČSOB in district towns, some regional offices, branches of PVT. This altogether is about 300 workstations. They have already issued hundreds of thousands of certificates. The company I.CA was founded in 1996 and gradually, due to increased demand of their services was founded the subsidiary company PVT, which was called První certifikační autorita, a.s. The name První certifikační agentura, a.s. is still used today. This company is owned by these major companies: Česká spořitelna, a.s., Československá obchodní banka, a.s., Telefónica O2 Czech Republic, a.s., Asseco, a.s., Státní tiskárna cenin s.p. (Ica.cz, 2008)

Ministry of informatics issued accreditation for První certifikační agenturu on 8th March.2002. This accreditation created by the Act No. 227/2000 Coll., on electronic signature, allows to issuing qualified certificates.(První certifikační agentura online, 2008)

Ministry of Informatics awarded První certifikační agenturu, a.s. with extended accreditation. This extended accreditation obtained from 1.2.2006 by Act No. 227/2000 Coll., on electronic signature. It allows issue qualified system certificates and qualified time stamps. (Businessinfo.cz 2002)

4.2.2 PostSignum QCA

Qualified certification authority by Česká pošta, s.p. is PostSignum QCA. PostSignum has become a qualified certification authority by 3rd August 2005, based on a decision of the Ministry of Informatics. PostSignum QCA also publishes qualified system certificates and qualified time stamps. Information System PostSignum QCA received 21st December 2007 certification of compliance with the standards ISO 9001 (Quality Management System) and ISO 27001 (Information Security Management System).PostSignum has 82 places with the service of Czech POINT and 7 mobile registration authorities. You can create an electronic signature in one of these places. (Česká pošta online, 2010)

4.2.3 eIdentity, a.s

eIdentity received accreditation t as an accredited provider of certification services in September 2005. eIdentity, a.s. tries to make advanced safety technologies available for general population. Ministry of Informatics of the Czech Republic provided by the law, the supervisory function of the quality and safety services which are provided by the eIdentity. eIdentity has the only place for registration- in Prague. (eIdentity online, 2010)

4.3 Certificate Revocation List (CRL)

CRL is a list from revoked certificate. These are certificates, which still exist but have been excluded. For each transaction, it is possible to verify the validity of this official list, which is accessible to the public. CRL is issued by certification agency. Certificates are listed on this schedule until their validity expires properly. Certifying Agency updated this list regularly. (Katsikas, 2005)

5 CERTIFICATE

The certificate is a data message that is issued by a certification service provider. Certificate combining data for verification of electronic signatures with the signatory and allows verify its identity. Certificate may also combine data for verification of the electronic signs to the person and allows to verify its identity. (source: Law on Electronic Signatures § 2 point. k) (eAgri.cz, 2010)

Public key certificate deals with control, distribution and storage of the keys. It is a digital document, which contains following information: the public key, name, date of commencement of, expiry date, name of the certification authority that issued the certificate, the serial number and others information. Certificates basically combine a specific person with his number. Electronic signature becomes trustful by use of the certificate. Such a signature is called a qualified electronic signature. (Shaw, 2000)

Publisher of certificates is a certification authority (CA). The certification authority is present during the communication of two sides. Certification authority serves as an independent and credible body that verifies the identity of the person with his electronic identity. The certificate is signed document. By using the certificate, there isn't necessity to exchange key between entities. Elect only by the same certification authority. Therefore it is important to have a trusted certification authority. (Budiš, 2008)

5.1 Creating of certificate

Creation of certificate consists of the following steps:

- Generating key- Certification Agency generates public and private key
- The applicant provide information about himself
- The applicant sends the public key and information about himself to the certification agency
- Certification agency verify the necessary information, whether the certificate to the applicant could be provide
- Certification agency will create a certificate and sign it with the public key
- The certificate is ready and certification agency sends it to the applicant (Adediran, 2002)

5.2 Types of certificates

5.2.1 Certificate issued by CA

Certificates are usually issued by CA, so the owner and the issuer of the certificate are the same. This solution, however, does not ensure its credibility. This should be proved by another way. CA should ensure a discrete and credible way of delivering the certificate for both communicating sides, or to do so by a trusted intermediary. List of CA in accordance with the law on electronic signature is on the website of the Ministry of Interior (www.mvcr.cz). Certificate issued by CA is usually valid for 5 years or more (Budiš, 2008)

5.2.2 Commercial certificate

Commercial certificate, or clients certificate, is not connected with the Law on electronic signature. It depends only on agreement of communicating parties and technology they use. The level of these certificates differs and is not controlled by anyone. This is the most common type of certificate issued in the Czech Republic. (Budiš, 2008)

5.3 Policy of qualified certificates from other countries

The Czech Republic distinguishes, whether qualified certification comes from the European Union or from other countries. If a qualified certificate from EU country is labeled as a qualified certificate, it is also qualified certificate in the Czech Republic. If a qualified certificate isn’t from the European Union, but comply with the law on electronic signature in the CR, it must satisfy other conditions: certification service provider must fulfill the condition of European Union, certification service provider is recognized as an accredited certification service provider in any state from the European Union, or operating on the territory of any European Union state. (Zákon č. 227/2000 Sb., o elektronickém podpisu)

6 CRYPTOGRAPHY

Cryptography is the science of creating ciphers. Cryptography deals for exampl with encryption algorithms, cryptographic tools. Encryption turns freely available information into unintelligible information to the surroundings. Cryptography is divided into symmetrical and asymmetrical. Electronic signature is based on the principle of asymmetric cryptography

The encryption process protects confidential and personal information. Decryption is the transformation of encrypted data to its original form. (Požár, 2005)

6.1 Symmetric cryptography

Symmetric cryptography is based on the existence of a secret key that is common to both the sender and the recipient. The text which is send is converted to a cipher by using the key. Receiver decrypt encrypted text by using the same key. The advantage of symmetric encryption is its speed and easy calculation. Problem for symmetric encryption is to ensure secure transmission of keys. For transmission of the key is often use a courier services (Kahate, 2003)

Minimum key length is 40 bits. The key of 40 bits may be satisfactory only for a small company. For great companies is 56 bits the minimum key length. (Jašek, 2006)

6.2 Asymmetric cryptography

Asymmetric cryptography (so-called: public-key encryption) belongs to a class of encryption methods, where is used a pair of keys to encode and decode messages. These keys are clearly described by mathematical algorithms. The task of the algorithm is to provide a readability,or in the case of electronic signature to verify authenticity of the document easily. But there’s a necessity of knowledge of the public key (in the case of electronic signature it is private key). On the other hand, its main task is to avoid readability of the document, if the keys are not known.

A pair of keys is a defining characteristic of asymmetric ciphers. One key is used to encrypt the document and the other is used to decrypt the document.

Symmetric cryptography is characteristic by usage of a single key to encryption and decryption of the messages. The great advantage of the symmetric cipher is a great speed. Major disadvantage is considerably less security because the encryption key must be sent through an open information channel. It is relatively easy for hacker to catch the key.

The disadvantage of asymmetric ciphers is complicated computing operation. In practice, we can find a combination of asymmetric and symmetric ciphers. There a message is encrypted by symmetric cipher and a key of symmetric cipher is sent to an open information channel, where it is encoded by an asymmetric cipher. (Jašek, 2006)

6.2.1 Outline the principle of asymmetric encryption algorithm

An asymmetric cryptography algorithm usually belongs to a class known as NP complete problems. From mathematical point of view it is nondeterministically polynomial problem, which simply means that currently isn't known procedure to solve this task in a deterministic polynomial time. If will be found such an algorithm that would mean that all NP complete problems will crash into the so-called P-class problems. P-class problems are already possible to solved in deterministic polynomial time. So far, was not proof that such algorithm exists.

Practically, we can describe this problem by the following example.500 children wants to attend a kindergarten next year. Capacity of the kindergarten is only 100 children. This case is so-called P-class problem, where there is select 100 children with very simple method. For example, every fifth child or the first hundred children choose according an alphabet and so on. The situation will be more complicated when the director of the kindergarten asks following request. Select the 100 children according following conditions. I give you a list of pairs of children. From each pair can be selected one child or no child, but can't be selected both children from the one pair. This makes from simple P-class problem a very complex NP complete problems. Numbers of combination for solving such a task is much bigger than numbers in our known visible universe. If we want this task break by the so-called brute force, that means to calculate all the combinations, we would get into a situation that we need non-deterministic amount of a time. This means that before we solve the task, content of such message would become meaningless. It is impossible to say whether such a task, will be solved for five minutes (with almost zero probability of selecting the correct input conditions) or after a period of hundreds of millions or billions years. The relationship between P and NP problem is one of the seven most complicated math problems. However, it is not to said that such an algorithm doesn't exist.

To break the cipher by using the brute force (ie the massive computing power) have not paid for MD5 hashing algorithm, which is still used for example to check the integrity of large data files. Paid for a small key length (128 bits) and today is no longer generally considered implausible.

Another way how to break the current asymmetric cryptography, is by using the principle of quantum computers. Research on this task is at the very beginning and deals with Heisenberg principle of uncertainty of matter. In practice this means that if I read the quantum information and change it, I depreciate the information.

If the research in this area will continue successfully, it would mean a collapse of safety asymmetric ciphers. (Adámek, 1989)

6.2.2 Description of some asymmetric algorithms

There will be not given a precise mathematical proof, but it is not the purpose of this work. There will be simply described principles, advantages and disadvantages of their procedures. Particular emphasis will be placed on the asymmetric encryption RSA, which was chosen by the Czech legislation for electronic signature authentication.

6.2.2.1 Elliptic curves (ECC)

Elliptic curve algorithm is less demanding on computing power while maintaining high security (compare to RSA). Elliptic cipher algorithm allows working with much shorter key. It uses the so-called Schoofs algorithm for calculating the points on the elliptic curve. It is based on a relatively sophisticated theory of numbers. Interestingly, this theory has a relatively close relationship with the so-called proof of Fermat's last sentence. Yet it is a relatively new algorithm, we can expect its significant expansion in the future. This algorithm is also approved by the Czech legislation to use for the Digital signature. (Stinson 2006)

6.2.2.2 RSA

Was described in 1977 at MIT by Ron Rivest, Adi Shamir and Len Adleman. Its security is based on two factors. The first, that there doesn't exist fast algorithm for deploying large numbers to the product of primes. So it isn't possible to find in a short time factors p and q from the numbers $n = p * q$. The second factor is the so-called RSA problem, which is defined as a mathematical procedure for obtaining a set of root *n* according equality *m ^ e mod n = c,* where *e* and *n* is a public key and *c* is the ciphered text. In 1993 was published by Peter Shore algorithm with the properties of quantum computers, which can solve the problem of factorization. Currently is the RSA algorithm safe. Its disadvantage is the relatively high mathematical complexity, which means that the key of 2048 bits has problems when it is used in for example: PDA, etc (Stinson 2006)

7 SECURITY OF DIGITAL SIGNATURE

Security of electronic signature is very high. It is due to several factors. Advanced electronic signature is based on a reliable mathematical method- on asymmetric encryption. There could be almost certainly said that the asymmetric cipher is unbreakable. Breakability of digital signature is rather theoretical than practical possibility, even when using the latest technology. Another security feature is the trusted certification agency. In the Czech Republic there are three certification agencies accredited by the Ministry of Interior: The first certification authority,a.s, PostSignum and eIdentity a.s. Accredited certification agency can be proclaimed as credible. It is under the supervision of the Ministry of Interior and had to follow its regulations. The private key must be treated with responsibility and care. The owner must approach to his private key like to his PIN code from the card. Unfortunately owners of their private key are quite often unaware of this whether from their own indolence or negligence. For example: owner of private key will provide the key to his assistant, who will handle contracts. It is comfortable for the owner at the moment, but he could never be sure that the assistant will not misuse his trust. (Mates, 2006)

7.1 Signatory's duties

Signatory must store his private key safely to prevent the tampering of data. If he finds out a potential risk, he must immediately inform an accredited certification agency that controls his signature. Signatory must provide true and complete information which are needed for qualified certificate. (Požár, 2005)

8 PROBLEMS AND SECURITY RISKS WITH THE USAGE OF DIGITAL SIGNATURE

8.1 Security risks with Digital Signature

There are two options for information leakage, when is digital signature used: unreliability and human error, and unreliability and failure of technical systems (Brabec, 2001)

In practice occur following security risks of digital signature: Theft of the private key - the private key is usually stored on the hard disk, frequently it is storage on more places at once. Here is a risk of misuse private key, when the computer is used by another person.

CA can improperly manipulating provided data and abuse their powers.Copy of the public key. Breaking the algorithm (the probability is close to zero).

Such a treatment of the electronic signature is illegal. Security risks of digital signature can be successfully avoided by compliance with recommended practices. Rate of exploitability of electronic signature is still minimal. Just to commemorate: the electronic signature is still harder to misuse than handwritten signature! (Mates, 2006)

The human factor is the weakest item in security of the digital signature.

Other ways to exploit the electronic signature is owner’s fraudulent access. Key document is signed by the owner but he will argue to the police that the key was stolen by somebody. So he simulated the abuse of his key. (Požár, 2005)

8.2 Hacking

Hacking is one of the risks for an digital signature (but not just for it) in the future. It is an act that breaks security systems. Individuals who operate hacking are hackers. Not all hackers breaking the law. Hackers in community compete with each other, who will at first overcome security measures or to calculate various combinations. But most hackers acts illegally for their self-enrichment. Hackers are future threat for digital signature, but still rather theoretical threat. Break the digital signature according to current knowledge in mathematics and information technology, is close to zero. In the future, this do not need to be truth.(Kahate, 2003)

8.3 Archiving of documents

Most of the documents you need archiving for a long-term. Documents must be storage for up to 10 years. For paper documents is not that long time problem. You just need to have a big enough archive space. In information technology is a period of 10 years a long time. For archiving electronic documents are better simple formats such as text format or PDF. Currently, there are various methods how to ensure long-term archiving of electronic documents. The best method how to ensure long-term archiving of documents is a method of migration. Migration method is based on data transformation from the original format to the current format. During migrating there is a loss of integrity, which means for digitally signed documents, loss of their safety. This problem may be solved by a credible body which will guarantee the security of these documents. When there will be a loss of integrity, it will create a new integrity which will fully replace the original one. (Budiš, 2008)

II. ANALYSIS

9 SWOT ANALYSIS

9.1 Strengths

-High level of security of electronic signature based on many factors at once

-Trustworthiness of electronic signature is supported by the CA, which is under the supervision of the Ministry of Interior

-There is created the Law about Digital Signature in the Czech Republic

-Visiting of offices and banks is generally unpopular- digital signature reduced or completely abolished number of these visits

-Ability of document to pertaining to the digital signature and the unlikelihood of any changes in the content of the document.

-Digital signature is from the time of the decision until the validation, the objective result of the technological process (verification methods that prove validity of handwritten signature are only subjective)

-Accredited certificate which is issued in the Czech Republic is valid for all countries of the European Union

-Digital signature increases the number of documents that can be processed electronically

-Digital signature can be used for signing documents of any length and any content

-Sign and verify documents with electronic signatures is faster than the handwritten signature

-Digitally signed can be diskette, photograph, database access, etc, what may be a problem for handwritten signature

-Possibility of choice of qualified certification agency for customers (competition improve services for customers)

-Great number of branches that allow the creation of a digital signature (Czech post offices, etc.) -cut of costs for postage services

-Environmental friendliness (using of digital signature saves paper)

9.2 Weaknesses

-Establish an electronic signature is for the general public still a complex and complicated process

-Low public awareness about digital signature

-Usage of electronic signatures in government is still limited

-Necessity to renew an electronic signature every year

-It is paid service

-There is a problem of long-term archiving of electronically signed documents

-Stereotypes, which result in a lack of trust in electronic communication and electronic signatures as such, especially among older generations

-Expensive upfront investment which enable the electronic communication (this point is controversial, because most users already have computer with internet access)

9.3 Opportunities

-Growing interest about new possibilities in electronic communication

-E-commerce in the public service

-Public services will communicate with citizens in 100% cases electronically

-Simplifying of manuals about the establishment of digital signature, in a form such as brochures, flyers, etc.

-Simplifying the procedure of establishment of a digital signature

-Well-informed staff, help-desks, etc

-Direct installation of digital signature by certification authority in the customer's computer

-Teaching of pupils in secondary schools about digital signature, in subjects such as economics, information technologies pupils can create an electronic signature with their teacher

-Short office hours, most offices have office hours up to 18.00, while the working hours of many citizens are longer

-For a long-term archiving of electronically signed documents, there should be use a migration methods, which ensure data transfer, and the creation of a credible authority, which creates a new integrity of the original document

-The security of electronic signature may be increased by a chip cards

-Obligation for corporations to established a data boxes for communication with authorities

9.4 Threats

- Owners of private keys acts irresponsibly, which leads to poor public opinion about the safety of electronic signature

-There will be find an algorithm, which leads to breaking of electronic signature

-Community of hackers, which declined the security of electronic signature

-Theft of a private key

-CA will misuse its powers

-Private key owner will misuse his private key

-Users betray authentication data to their PC, but they do not realize the potential risk of misusage of their electronic signature

-Finding new methods how to confirm volition

-Increase of operating costs in the electronic communications

-Disinterest of the public to create digital signature

9.5 The SWOT Matrix

SO S: high level of security O: simplifying the procedure of establishment of a digital signature	WO W: Low public awareness about a digital signature O: simplifying the procedure of establishment of a digital signature
ST S: high level of security T: Disinterest of the public to create digital signature	WT W: Low public awareness about digital signature T: Disinterest of the public to create digital signature

Tab.1: The SWOT Matrix

10 SURVEY ON A DIGITAL SIGNATURE

10.1 The results of the survey: Public awareness and opinion on Digital Signature

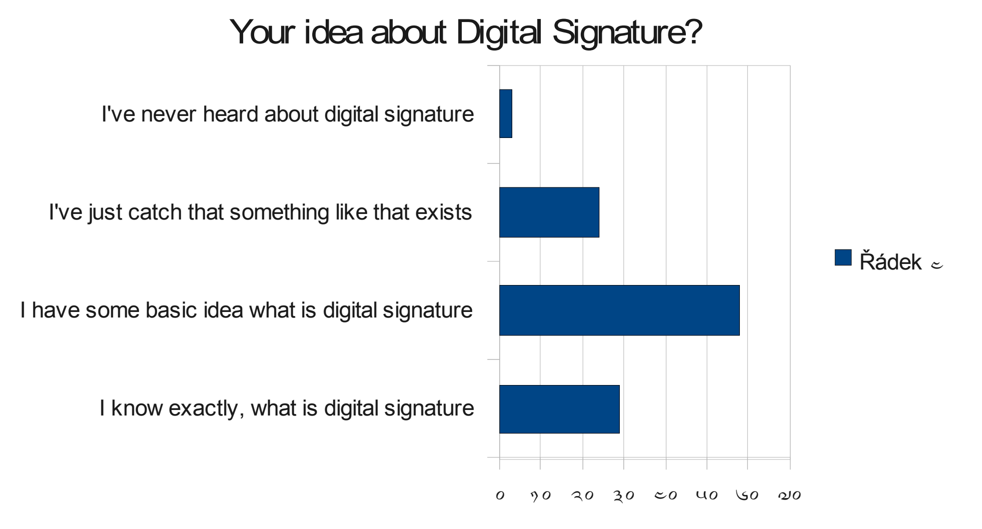

FIGURE 1: Public awareness about a Digital Signature

25,44 % of people answered that they know exactly what is a Digital Signature. Majority of the people 50,88 % have some basic idea about Digital Signature. 21,05 % of respondents just catch that something like that exists. Only 2,63 % of them never heard about Digital Signature.

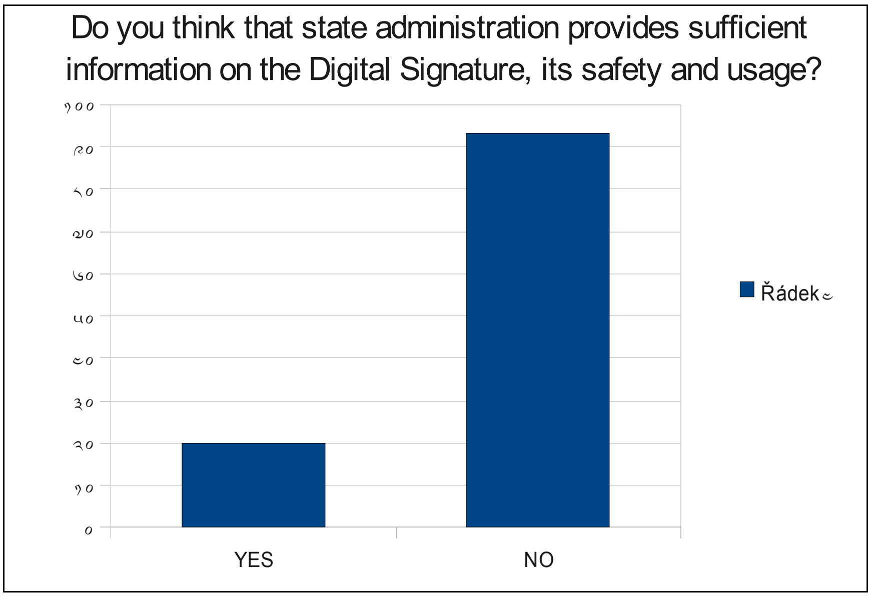

FIGURE 2: Information about a Digital Signature provided by a state administration

82,3 % of respondent's think that state administration don't provide sufficient information on the Digital Signature, about its security and usage. Compared to 17,7 % people who thought that state administration provides enough information about a Digital Signature, its usage and security.

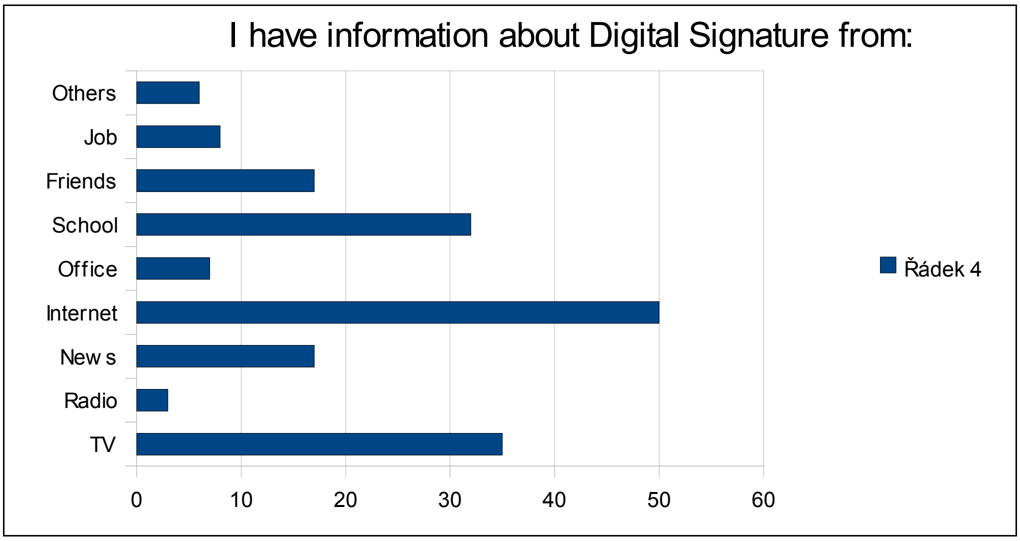

FIGURE 3: Sources of information about a Digital Signature

Majority (44,25 %) of people have information about Digital Signature from Internet. 30,97 % have information about a Digital Signature from TV, 28,32 % from school, 15,04 % from News, 15,04 % from friends, 7,08 % from work, 6,19 % from offices, 2,65 % from radio and 5,31 % of the people have information about Digital Signature from other sources.

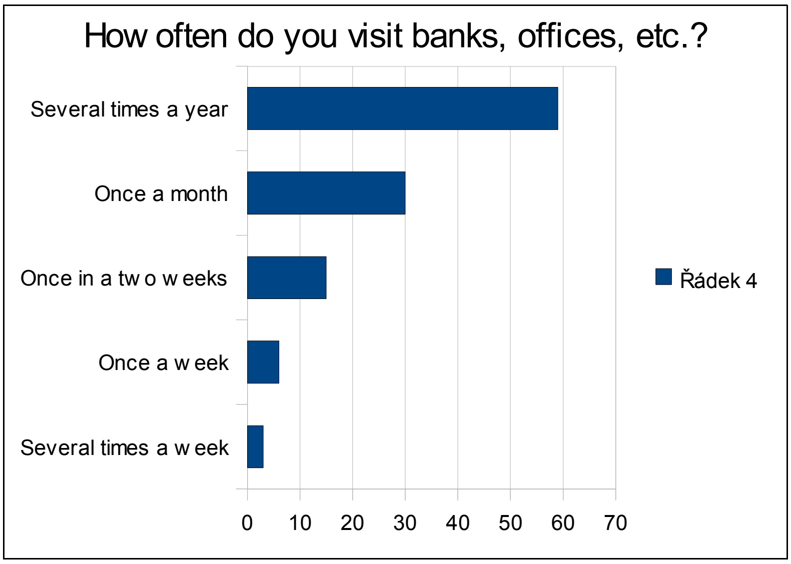

FIGURE 4: Frequency of visiting banks, offices, etc.

Majority of the people 52,21 % visit banks and offices only several times a year. 26,55 % visit banks and offices on the average monthly, 13,27 % visit banks and offices once in a two weeks, 5,31 % visit banks and offices once a week and only 2,65 % of respondent's visit banks and offices several times a week.

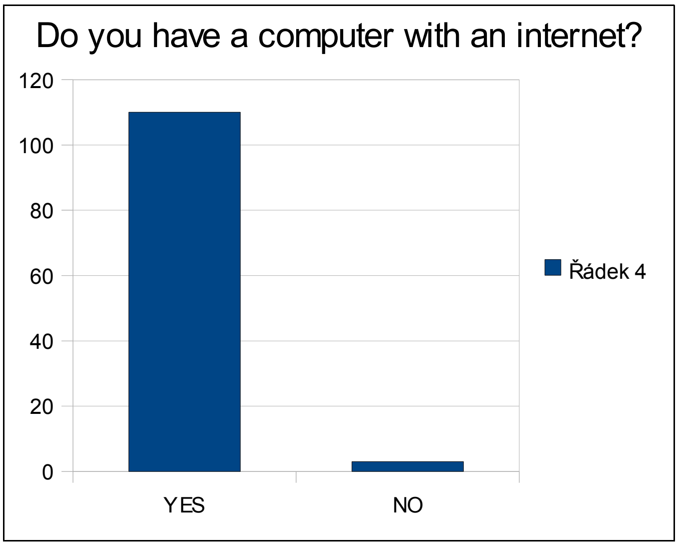

FIGURE 5: Ownership of computer with internet

Most of the people who answered the question (97,35 %) have a computer with an internet. Only 2,65 % of the people haven' computer with an internet.

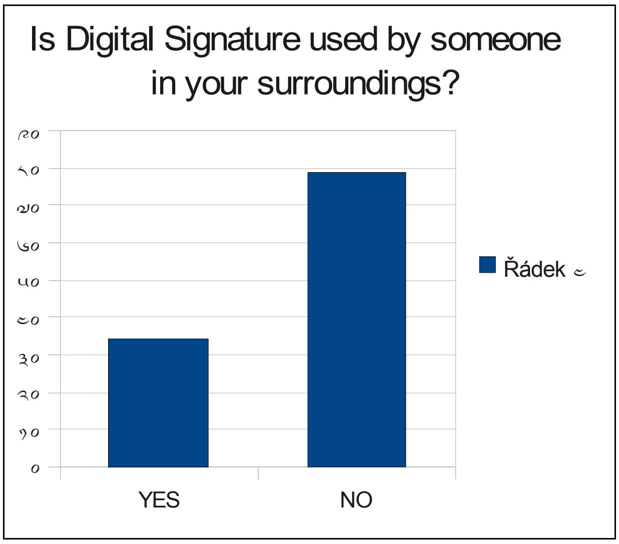

FIGURE 6: Usage of a Digital Signature in respondent's surroundings

30,09 % of people answered that someone in their surroundings. used a Digital Signature. 69,91 % of people said that nobody used a Digital Signature in their surroundings.

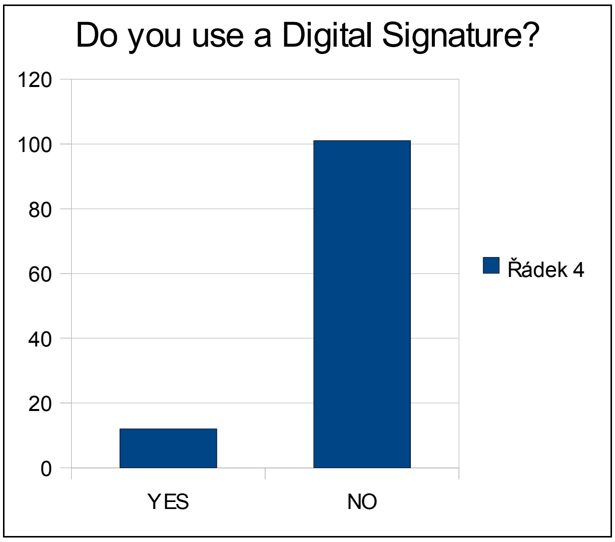

FIGURE 7: Usage of a Digital Signature

10,62 % of respondents use a Digital Signature. 89,38 % of them don't use a Digital Signature.

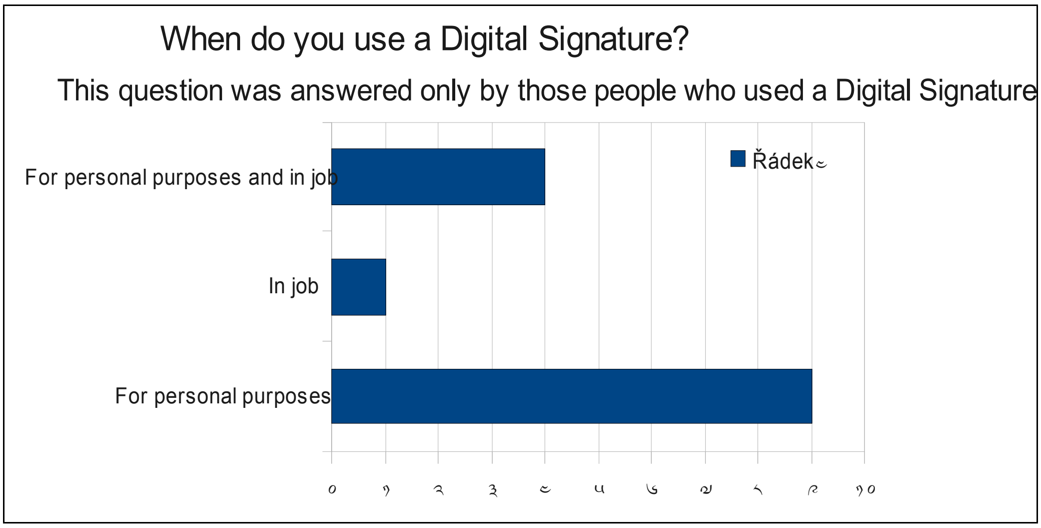

FIGURE 8: Places of usage a Digital Signature

64,29 % of the people who answered that they use a Digital Signature, use it only for personal purposes. 7,17 % use of them use a Digital Signature only in job and 28,57 % of them use a Digital Signature for personal purposes and also in work.

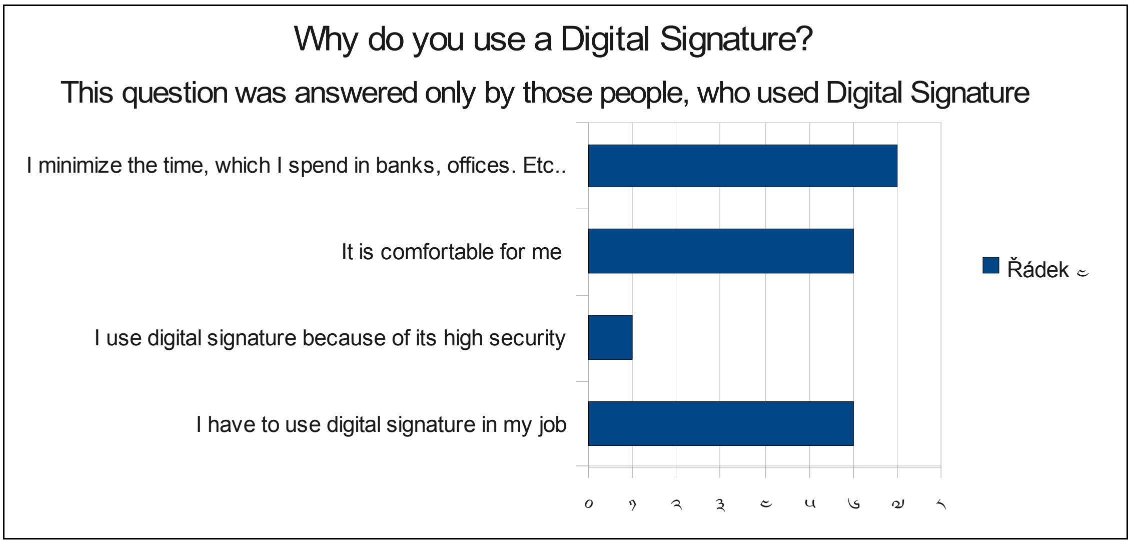

FIGURE 9: Reasons for usage a Digital Signature

46,67 % of the people who answered that they use a Digital Signature, use it because they minimize the time which they spend in banks and offices. 40 % of them said that it is comfortable for them to use a Digital Signature. 40 % of them answered, that they use a Digital Signature because they have to use it in their job. 6,67 % answered that they use a Digital Signature because of its high security.

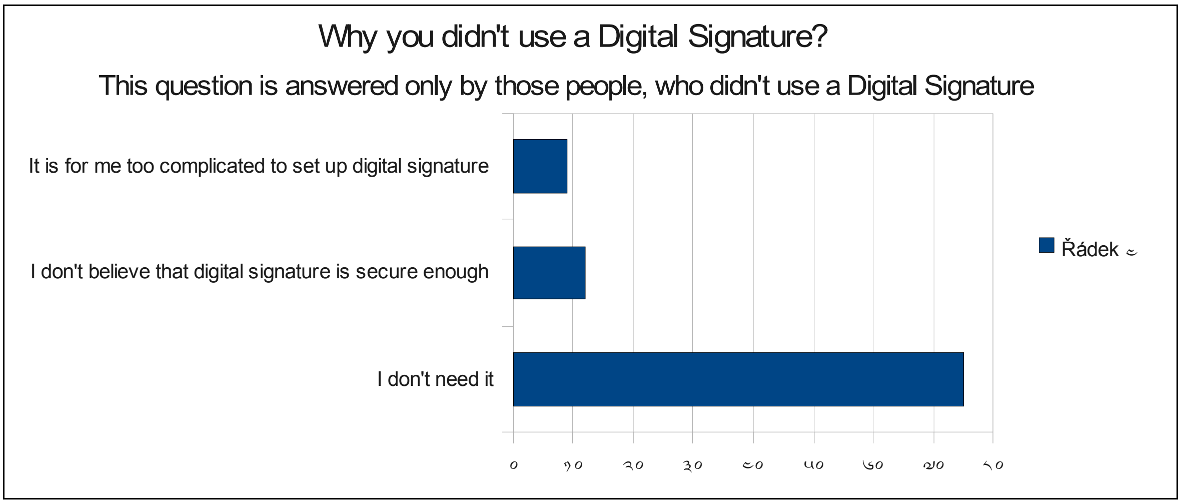

FIGURE 10: Reasons why isn't Digital Signage generally used

81,52 % of respondents who don't use a Digital Signature answered that they don't need it. 13,04 % of those who don't use a Digital Signature, don't believe that a Digital Signature is secure enough. 9,78 % of them answered that it is too complicated for them to set up a Digital Signature.

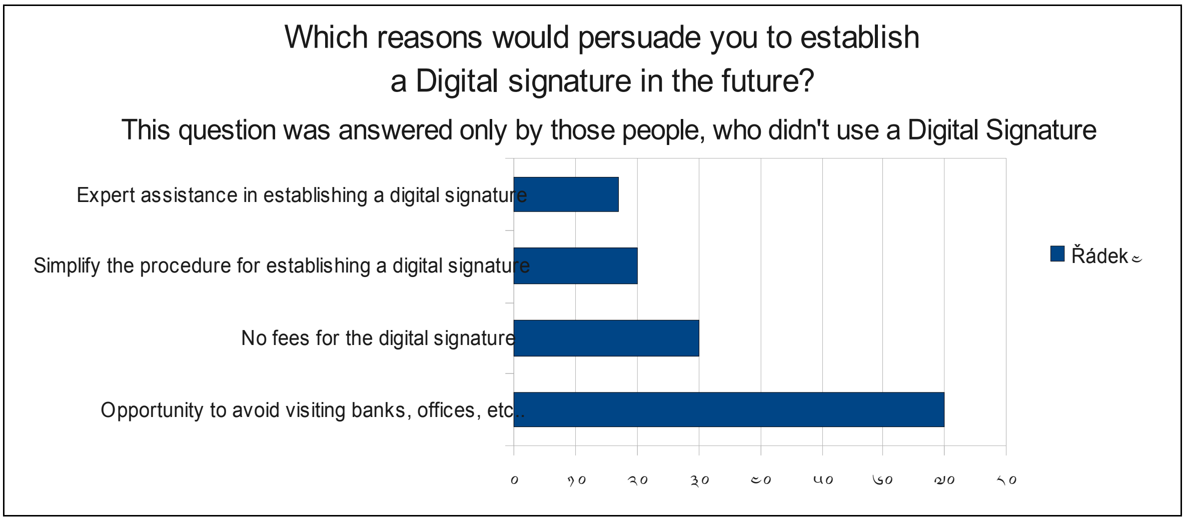

FIGURE 11: Possibilities that may growth the number of users of Digital Signature

76,09 % of the people who don't use a Digital Signature that a reason, which may persuade them in the future to set up a Digital Signature is the opportunity to avoid visiting banks and offices. 32,61 % of them may persuade to set up a Digital Signature that there will be no fees for it. 21,74 % of respondents answered that they will set up a Digital Signature if there will be simplify the procedure for establishing a Digital Signature and 18,48 % said it would be an expert assistance in establishing a Digital Signature, which may persuade them in the future to set up a Digital Signature.

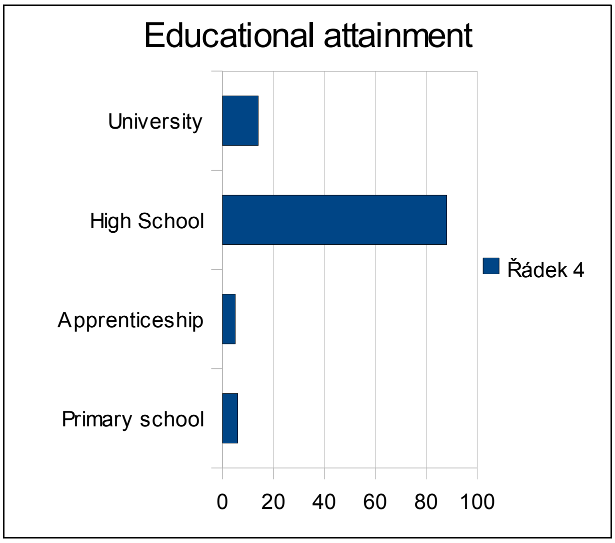

FIGURE 12: Levels of respondent's education

Educational attainment of respondents is following: 77,88 % finished high school, 12,39 % university education, 5,31 % finished primary school and 4,42 % of them finished their apprenticeship.

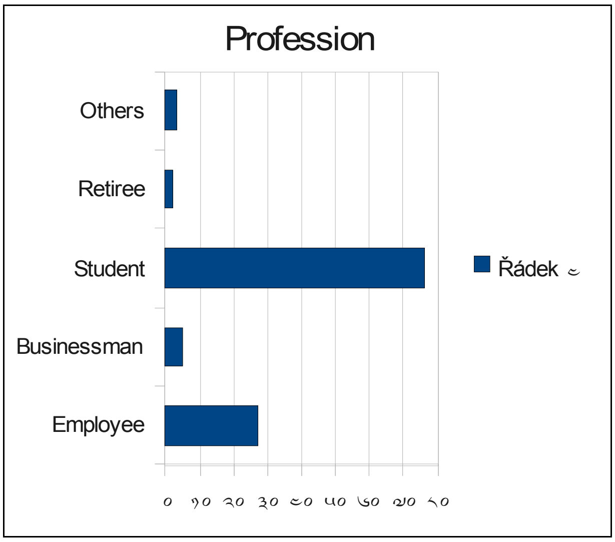

FIGURE 13: Respondent's profession

67,26 % of respondents were students, 23,89 % of them were employees, 4,42 % were businessman, 1,77 % were retirees and 2,65 % have some other profession.

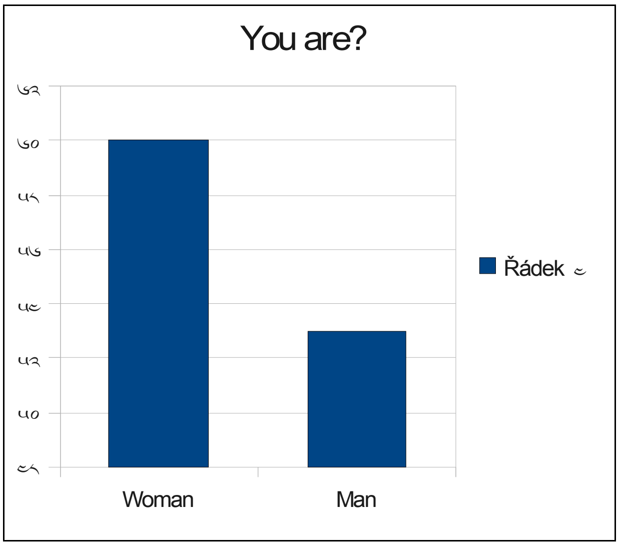

FIGURE 14: Respondent’s sex

53,1 % of respondents were women and 46,9 % were men.

11 SUMMARY

The survey was conducted electronically by using the server www.vyplnto.cz. I consider this server to be a great help in making this type of survey. The survey was called: "Public awareness and opinion on Digital Signature". The survey was active on the server www.vyplnto.cz from 5th of April 2010 to 12th of April 2010. Survey was answered by 114 respondents, which mean that it's informational value is good. It must be take into account that the survey covers only the population that actually participated in the survey. The survey was expand on www.facebook.com. Average time for completing the questionnaire was 2 minutes and 38 seconds. There were 14 questions in the questionnaire. From the survey are sure following facts. Majority (58,88 %) of the people have just some basic idea about what is a Digital Signature. 82, 3 % of respondents think, that state administration don't provides sufficient information about a Digital Signature. Internet, school and TV are the biggest sources of information about Digital Signature. 52,21 % of the people visit banks and offices just a several times a year. At least everybody (97,35 %) have a computer with an internet. 30,09 % of the people said that there is somebody in their surroundings who used a Digital Signature. At least 11 % of respondents use a Digital Signature. Majority (64,29 %) of these people who use a Digital Signature, use it for personal purposes. Reasons why these people use a Digital Signature are following : they minimize the time which they spend in banks and offices, it is comfortable for them to use a Digital Signature and because they have to use it in their job. These reasons have around 40 % of the importance. But only 6,67 % of respondents answered that they use a Digital Signature because of its high security. It means that people don't care about the high security of a Digital Signature. Majority (82 %) of those people who don't use a Digital Signature don't need it. Reason that would persuade people to set up a Digital Signature in the future is the opportunity to avoid visiting banks and offices.

CONCLUSION

There offers now one question. "Is it possible that a digital signature will completely replace the manual signature in the future?". Certainly not. But it is not the principle of digital signature. Digital signatures are used to verify identity in electronic form and is responsible to confirm the authenticity of a document which is sent. Which means that the digital signature is only an alternative to handwritten signature, especially when communicating with authorities, banks and legal entities.

Knowledge of the principles of electronic signature is an essential prerequisite for the use of secure digital signature. Digital signature algorithm is definitely highly secure. Dangerous aspect of the Digital signature is undoubtedly the human factor. People treat with the Digital signature very careless, they betray their identity, or they are not willing to learn new things, and often they are too lazy- all of these human properties reduce the level of security of digital signature. Lots of managers and entrepreneurs are not aware of the safety of digital signatures and general principles of IT security. There have been cases where senior managers allow to sign up an important documents on behalf of an information technology worker.

It is therefore important to increase education about digital signature, which will emphasizes all the advantages of digital signatures and also to point out all the above mentioned principles of its security.

The sooner we realize the importance and continuity of digital signatures in business-management environment, the better for us.

BIBLIOGRAPHY

ADÁMEK, Jiří. *Kódování*. Praha : SNTL-Nakladatelství technické literatury, 1989. 191 s. ISBN 04-005-89.

ADEDIRAN, Peter. *A practical guide to business, law & the Internet*. London : Kogan Page Publishers, 2002. 244 s. ISBN 0749437340

BRABEC, František, et al. Bezpečnost pro firmu, úřad, občana. Praha : Public History, 2001. 400 s. ISBN 80-86445-04-06. [kniha]

BUDIŠ, Petr. Elektronický podpis : a jeho aplikace v praxi. 1. vydání. Olomouc : ANAG, 2008. 153 s. ISBN 978-80-7263-465-1. [kniha]

Businessinfo.cz [online]. 30.9.2002 [cit. 2010-03-15]. Elektronický podpis a jeho využití. Dostupné z WWW: <http://www.businessinfo.cz/cz/clanek/podnikatelske-prostredi/elektronicky-podpis-a-jeho-vyuziti/1001234/2984/>. [webová stránka] (4)

Česká pošta [online]. 2010 [cit. 2010-03-15]. Kvalifikovaná certifikační autorita. Dostupné z WWW: <http://www.cpost.cz/cz/sluzby/e-sluzby/kvalifikovana-certifikacni-autorita-id287/>.

Eagri.cz [online]. 2010 [cit. 2010-04-27]. Kvalifikovaný certifikát pro ověření elektronického podpisu. Dostupné z WWW: <http://eagri.cz/public/eagri/e-podatelna/podpora-elektronickeho-podani/osobni-certifikat/>.

EIdentity [online]. 2010 [cit. 2010-04-20]. Certifikáty certifikačních autorit, které provozuje eIdentity. Dostupné z WWW: <http://www.acaeid.cz/InstallStatic.html>.

Ica.cz [online]. 2008 [cit. 2010-04-27]. Obecné informace. Dostupné z WWW: <http://www.ica.cz/cz/menu/1/obecne-informace/>.

JAŠEK, Roman. Informační a datová bezpečnost. Vydání první. Zlín : Univerzita Tomáše Bati, 2006. 140 s. ISBN 80-7318-456-7. [kniha]

KAHATE, Atul. *Cryptography and Network Security*. New Delhi : Tata McGraw-Hill, 2003. 435 s. ISBN 0-07-049483-5

KATSIKAS, Sokratis K.; LÓPEZ, Javier; PERNUL, Gunther. *Trust, privacy, and security in digital business*. Second. Copenhagen : Birkhauser, 2005. 332 s. ISBN 3540282246, ISBN 9783540282242.

LORENC, Miroslav. ISVS.cz : Informační systém veřejné správy [online].Advice.cz, 4.9.2007 [cit. 2010-03-15]. Elektronický podpis- využití certifikátu. Dostupné z WWW:<http://www.isvs.cz/e-podpis-podatelny/elektronicky-podpis-vyuziti-certifikatu.html>. ISSN 1802-6575. [webová stránka]

MATĚJKA, Michal. Počítačová kriminalita. Vydání první. Praha : Computer Press, 2002. 106 s. ISBN 80-7226-419-2. [kniha]

MATES, Pavel; SMEJKAL, Vladimír. E-GOVERNMENT v českém právu. Praha: Linde Praha, 2006. 244 s. ISBN 80-7201-614-8

MAZZEO, Mirella. SecurityFocus.com [online]. 26th January 2004 [cit. 2010-03-15]. Digital Signatures and European Law. Dostupné z WWW: <http://www.symantec.com/connect/articles/digital-signatures-and-european-laws>. [webová stránka] 11

MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Vydání první. Brno : Computer Press, 2007. 154 s. ISBN 978-80-251-1511-4. [kniha]

POŽÁR, Josef. Informační bezpečnost. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5. [kniha]

První certifikační autorita [online]. 2008 [cit. 2010-03-15]. Certifikáty. Dostupné z WWW: <http://www.ica.cz/cz/menu/29/produkty-a-sluzby/certifikaty/>. [webová stránka]

SHAW, Michael , et al. *Handbook on electronic commerce*. New York: Springer, 2000. 723 s. ISBN 9783540673446

STINSON, Douglas Robert. *Cryptography: theory and practice*. third. The USA : CRC Press, 2006. 593 s. ISBN 1584885084, ISBN 9781584885085.

Zákon č. 227/2000 Sb., o elektronickém podpisu

LIST OF ABBREVIATIONS

CA = Certification Agency

CRL = Certificate Revocation List

ECC = Elliptic curves

EU = European Union

PDA = Personal Digital Assistant

LIST OF FIGURES

LIST OF TABLES

APPENDICES

Dotazník: Informovanost a veřejné mínění o elektronickém podpisu

Dobrý den, jmenuji se Ivana Lukašíková a jsem studentkou Univerzity Tomáše Bati ve Zlíně, oboru Anglický jazyk pro manažerskou praxi. Informace získané z tohoto dotazníku budou sloužit jako podklad pro mou bakalářskou práci s názvem Elektronický podpis v organizacích.Tento dotazník je zcela anonymní a slouží k zjištění informovanosti a veřejném mínění o elektronickém podpisu.

Děkuji za Váš čas!

1. Má představa o elektronickém podpisu:

Vím přesně, co je to elektronický podpis
Tuším, co to je elektronický podpis
Jen jsem zaslechl (a), že něco takového existuje
Nikdy jsem o elektronickém podpisu neslyšela
(povinná otázka)

2. O elektronickém podpisu jsem se dozvěděl (a):

TV Rozhlas Tisk Internet Úřad Škola Od známých V práci Jiné
(povinná otázka)

3. Jak často chodím na úřady, do bank, apod.?

Několikrát do týdne
Zhruba jedenkrát týdně
Jedenkrát za dva týdny
Jedenkrát do měsíce
Párkrát do roka
(povinná otázka)

4. Vlastním počítač s připojením k internetu?

ANO NE
(povinná otázka)

5. Poskytuje podle Vás státní správa dostatečné množství informací o elektronickém podpisu, jeho bezpečnosti a možnostech jeho využití?

ANO NE
(povinná otázka)

6. Elektronický podpis:

Používám Nepoužívám
(nepovinná otázka)

7. Vyplňuje pouze ten, kdo elektronický podpis POUŽÍVÁ: Elektronický podpis používám:

Pro osobní potřebu V zaměstnání Pro osobní potřebu i v zaměstnání

(nepovinná otázka)

8. Vyplňuje pouze ten, kdo elektronický podpis POUŽÍVÁ: Mé důvody používání elektronického:

Pokud si nevyberete žádnou z nabízených odpovědí, otázku přeskočte.

Elektronický podpis musím používat v zaměstnání
Elektronický podpis používám kvůli jeho vysoké bezpečnosti
Je pro mě jeho používání pohodlné
Díky elektronickému podpisu minimalizuji svůj čas strávený na úřadech, v bankách, apod.
(nepovinná otázka)

9. Vyplňuje pouze ten, kdo elektronický podpis NEPOUŽÍVÁ: Proč elektronický podpis nepoužívám?

Pokud si nevyberete žádnou z nabízených odpovědí, otázku přeskočte.

Nepotřebuji ho
Nevěřím, že je dostatečně bezpečný
Je pro mě jeho založení příliš složité
(nepovinná otázka)

10. Vyplňuje pouze ten, kdo elektronický podpis NEPOUŽÍVÁ: Důvody, které by mě v budoucnu přiměly k používání elektronického podpisu:

Pokud si nevyberete žádnou z nabízených odpovědí, otázku přeskočte.

Možnost se úplně vyhnout návštěvám úřadů, bank, apod.
Zrušením poplatků za elektronický podpis
Zjednodušení postupu při založení elektronického podpisu
Odborná pomoc při založení elektronického podpisu
(povinná otázka)

11. Používá někdo ve Vašem okolí elektronický podpis?

ANO NE
(povinná otázka)

12. Jsem:

Žena Muž
(povinná otázka)

13. Povolání

Zaměstnanec Podnikatel Student Důchodce Ostatní
(povinná otázka)

14. Nejvyšší dosažené vzdělání

ZŠ Učební obor SŠ VŠ