# Problems of Digital Sustainability

**Tamás Szádeczky**

Department of Measurement and Automation, Kandó Kálmán Faculty of Electrical Engineering, Óbuda University
Tavaszmező u. 17, H-1084 Budapest, Hungary
szadeczky.tamas@kvk.uni-obuda.hu

*Abstract: The article introduces digital communication by drawing comparisons between the histories of digital and conventional written communication. It also shows the technical and legal bases and the currently reached achievements. In relation to the technical elements, it acquaints the reader with the development and current effects of computer technology, especially cryptography. In connection with the legal basis, the work presents the regulations which have emerged and made possible the legal acceptance of the digital signature and electronic documents in the United States of America, in the European Union and among certain of its member countries, including Hungary. The article reviews the regulations and the developed practices in the fields of e-commerce, electronic invoices, electronic records management and certain e-government functions in Hungary which are necessary for digital communication. The work draws attention to the importance of secure keeping and processing of electronic documents, which is also enforced by the legal environment. The author points to the technical requirements and practical troubles of digital communication, called digital sustainability.*

*Keywords: electronic archive; digital sustainability; preservation; electronic signature; data security*

## 1 Introduction

We may distinguish three revolutions in the development of written communication [1]. The first revolution was the invention of alphabetical writing carrying phonetic value around 1300 BC., which segregated the text from the content. The second revolution in the 15$^{th}$ Century was the book printing invented by Gutenberg, Johannes Gensfleisch, which made written material widely available. The third revolution – which is called the digital revolution – is currently going on. We cannot accurately define its nature without an historical overview, but we may declare that it has modified all of the essential structures of written communication. At the same time, however, it has kept all the achievements of the previous revolutions. This is the key to digital culture and to the information society.

With the development of digital communication, computers conquered space in the area of applications which traditionally used paper. We can consider records management, accountancy and generally the creation of the public documents, notary documents and simple contracts as those applications. The necessary technical conditions have existed since the 1990s, when the technology of encryption with an asymmetric key was worked out in detail, in addition to computer and network technologies. First this development made creating electronic signature possible, and then came the acceptance of defining the legal consequences. We may solve electronic authentication of documents by electronic signature in the international practice and in Hungarian legal requirements. In the European Union and in the Republic of Hungary there are at present political and legislative endeavours aimed at rapid development in these areas. The problems of this process are referred to as the issue of digital sustainability [2].

The basic question of this research is: What is the difference between conventional and digital communication, especially as regards the long-term storage and usage of electronic documents. The research question was analysed via observation, information gathering and empirical statements based on the personal professional practice of the author.

# 2 Conditions of the Development of Digital Communication

The technical requirements necessary for the development of digital communication can be divided into three parts: computer technology, networking technology and data security procedures, providing a practical equivalent to the requirements of traditional written communication.

The first Turing-complete digital computer, the Zuse Z3, was constructed by Zuse Konrad in 1941. The creation of the transistor in 1947 revolutionized the world of crude electromechanical computers [3]. The integrated circuit, a mass of transistors fixed onto a single sheet, was developed in 1958. The first personal computer (the IBM PC) appeared in 1981, making it possible for home and office users to have computational performance. This was a huge invention compared to the usage of time slices in computer centres earlier.

The development of computer networks started in 1962, when the Advanced Research Projects Agency (ARPA) set up a research team called the Intergalactic Network, a group of which developed the time-sharing system. This system made possible the sharing of a mainframe computers' services between numerous users on a telex network [4].

In 1969 a research team of ARPA created the first packet switched computer network, the ARPANET. This network connected only a couple of universities and military systems at that time. It was not until the end of the 1970s that the civilian and broad usage of the network was in sight, but already at this time rapid enlargement had started. ARPANET was interlinked with NSFNet during the late 1980s, and the term 'Internet' was used as the name of the new network, which has since become the large and global TCP/IP network.

According to the World Internet Project 2007, 49 percent of Hungarian households (about two million) owned a personal computer at home, and the third of these computers (35%) also had an internet connection [5].

There is another significant requirement – but one which generally receives lesser emphasis – in connection with the development of digital communication: human resources. This means inclination and ability of citizens and clients to use the developments in digital communication and to actively participation in the information society. Because of the limited nature of this paper, the human resources and the economical aspect are beyond its.

In the following parts of the chapter, the development of the data security procedures and the legal-political conditions will be outlined, because of their emphasized significance in the present approach to the topic.

## 2.1 Data Security Procedures

The development and free public usage of data security procedures ensure a connection between the requirements of written communication and those of digital communication. It is necessary to ensure confidentiality, authenticity and originality in order to achieve the logic safety of electronic data. We accomplish this with mathematical methods, which cryptography (science of encryption) deals with. The encryption of information is practically the same age as writing, because since we started writing messages on paper (or on clay tablets) we have wanted others to be unable to read it.

Modern cryptosystems are wholly based on mathematical encryption methods, made by computers, which were developed at the end of twentieth century. There are two kinds of encryption methods: symmetric and asymmetric. The primary difference between the two is that the same key is used for encryption and decryption in the case of the symmetric one (this method is called single key because of this), while we perform the encryption and decryption processes with two different keys in the case of the asymmetric one (the two key method).

The modern computer-based symmetric encryption was developed in the 1970s. It applies reversible functions on blocks (generally 64-256 bits) by mixing and replacing characters or blocks of the clear text. In this method, it is possible to attain a good security level with the combination and numerous repeating of relatively simple procedures [6]. A popular symmetric cryptosystem of this kind is

the Data Encryption Standard (DES). While it is today insecure because of its short key length (56 bits), it is nevertheless occasionally used. As a result of break competitions on DES[1] we can state that any confidential message encrypted by DES is breakable in minutes with the appropriate hardware. From the principle of symmetric encryption (in civilian use) the cyphertext is breakable in all cases; it depends only on time.[2] Due to Kerckhoffs' principle, the security of encryption depends only on quality of the applied mathematical algorithm and the length of key, and thus not on the secrecy of the algorithm. Despite this, in individual cases, in the interest of increasing security (DES) or due to reasons of intellectual property (IDEA), the algorithm may be secret. Nowadays the Advanced Encryption Standard (AES) is used more often than anything else. AES, developed in the 2000s, uses 128-256 bits of key length and is hopefully based on an appropriate algorithm. Nobody has yet found a weak point on it, and thus experiments show that AES would be breakable in millions of years with all computers in the world [7].

The other branch of modern cryptography is public or asymmetric key cryptography, developed in mid 1970s. This branch is based on mathematical problems of one way trap door functions: discrete logarithm, discrete square root, and factorization with very large prime factors [8]. The solution to these problems is simple with a certain secret (private key), while without the secret it is more complicated. The application of asymmetric systems requires a larger key (1024-4096 bits) and more time for the coding and decoding processes, but the attained security is equal to that of the symmetric cryptosystems. For asymmetric encryption, it is necessary to generate two keys (a key pair) from a common secret. The common secret is destroyed after their generation. One of the key pairs' members will be the cryptographic private key, which the owner must not let out of his possession under any circumstances. If this occurs after all, it is deemed compromised and it is not allowed to use the key pair any more. If possible, it is necessary to revoke it. The other member of the key pair is the public key, which can be published on the Internet, and it is allowed to be shared on any unsecure communication channels. The usage of the two keys is equivalent, and thus it is possible to encrypt with one key and decrypt with the other key. Thus the application of different directions becomes possible (encryption and electronic signature).

The process of making an electronic signature is the following: you make a fingerprint from the data with a hash function. This function is a trap-door function, which means that the accomplishment of the function is simple in one direction, but in the other direction it is a complicated mathematical problem. This function generates a constant-size (128-512 bits) data set from the discretionary

1 see http://www.rsa.com/rsalabs/node.asp?id=2108

2 There is a theoretically unbreakable algorithm, One Time Pad, but its usage is not practical in civil environment, but it worths for military usage.

quantity of data. Changing one single bit in the input should modify at least 50 percent of the output bits (avalanche effect). We call the data set received an output fingerprint, since it characterizes the input data in a unique way. It is impossible to restore the input from the output and it is almost impossible to find two inputs with the same output.[3] In practice SHA-1, RIPEMD-160, and Whirlpool algorithms are used. MD5 was suspected of being unsafe for years and its algorithm was broken in December 2008, and since that time its usage has been unsafe [9]. After the execution of this process on the document we have to sign, we encrypt the fingerprint with the cryptographic private key. We receive the electronic signature as a separate file which is independent from the document. We may send the signed document and the signature together to the addressee on a public channel, for example by e-mail. The addressee decrypts the electronic signature with our public key and obtains the fingerprint that we made. During this time he or she makes a fingerprint from the document we have sent with the same hash function and compares them. If they are the same, we can claim with certainty that no changes have occurred in the signed document, and that the signature on the document was made by the pair of our public key. On the other hand, it does not prove that this private key actually belongs to the sender, or that it has not been revoked, and we cannot ascertain the time of the signing. These criteria have to be proved by additional functions and controls. We may solve the problem of authenticity by binding the keys to one person, using two methods: with the web of trust (WoT) method [10], used by Pretty Good Privacy (PGP). According to this method, individuals trusting each other sign each other's keys. If the addressee trusts any of the persons signing the sender's key, or can follow back the signatures to a reliable person, this assures the sender's authenticity. The disadvantage of this method is that vast confidential networks are necessary in which two unknown people may have common acquaintances. The other method is Public Key Infrastructure (PKI). In this method, a third party who is entrusted by all communicating parties attests the reliability of all customers. This occurs with the use of a certificate, which is an electronic data set, and implies the public key. The third party is entrusted by the state or the public, who verifies the owner of the key and the key's relation prior to issuing the certificate (for example with the request of an ID or a verification e-mail). If the Certification Authority (CA), which is the national root, is trusted, other elements of the path are automatically entrusted. The publicly entrusted entity is called Certification Service Provider (CSP).[4] The Timestamping Authority (TSA), who electronically signs the accurate time that the sender builds into the electronic signature of the document, does the authentication statement of the time of the electronic signature. A request for a timestamp generally happens on-line through the internet. The trustworthiness of the TSA is proven by its certificate issued by a trusted CA. The usage of key pairs, or rather the certificates, can be limited. A key pair can be used for an electronic

[3] weakly or strongly collision free security, see [8]

[4] CSP and CA are often used in same sense

signature, encryption, authentication or certificate issuance (such as CA). If we want to use more functions from among these but the certificate is restricted, we will need more key pairs and certificates.

The outlined technology has been developed to be suitable for the service of trusted digital communication. This fact alone is not sufficient for reaching this aim without considering other aspects.

## 2.2 Regulations and Practice

After the algorithmic and technical infrastructural realisation of the electronic signature, it was necessary to actualize practical usage in order for legislators to allow paper-based signatures to be replaced with electronic signatures. Utah, in the U.S., in early 1995 was the first state to pass a digital signature act. In Europe, Germany was the first country that accepted electronic signatures in 1996 (Gesetz zur digitalen Signatur), followed by the United Kingdom in 1999 (Building Confidence in Electronic Commerce – A Consolidation Document) and the European Union in 1999 (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on Community framework for electronic signatures).

The first step in Hungarian legislation was Act XXXV of 2001 on Electronic Signatures [11].[5] Electronic governmental services started partly on the basis of this rule of law. Electronic tax returns became available from the end of the nineties in several phases, and this improved considerably in 2002 and 2006 [12]. The electronic data-supplier service of the land registry (TakarNet) started in 2003, client gate (detailed later) began in 2005, regulations on electronic records management have existed since 2006, electronic public procurement started in 2007, electronic company registration was launched in 2008, as was the electronic auction of revenue authority and the change of Act on Accounting to simplify the storage of electronic invoices.

The Hungarian electronic signature law – corresponding to Directive 1999/93/EC – distinguishes three levels of electronic signatures independent from the technical background. At the bottom level there is the 'simple' electronic signature, which means a name written down into the electronic documents without any safety requirement (for example the signature at the end of an email). The legislator does not bind any special legal consequence to it, but only makes its acceptance subject to free consideration. The second safety level is the advanced electronic signature, which has to meet the requirements for the capability of identifying the signatory, uniquely linked to the signatory, which is created using devices that the signatory can maintain under his sole control; and it is linked to the document to which it relates in such a manner that any change to the data of the document made

5 abbreviated as 'Eat.'

subsequent to the execution of the signature is detectable.[6] The binding legal consequence is the correspondence to the legal requirements to put into written form excluding several specified fields.[7] From among the electronic signatures, the safest one that meets the highest requirements is the qualified electronic signature. The qualified electronic signature is an advanced electronic signature, which is created with a secure signature creation device (SSCD) and which comes with a certificate issued with it.[8] The requirements for qualified certificates are the strictest and these certificates are subject to additional regulation. An electronic document supplied with a qualified electronic signature is a full, conclusive private agreement. Thus, its authenticity and the fact of its belonging to the signer cannot be disputed until proof to the contrary. In the case of the last two levels, an independent audit and authority supervision is compulsory for the operation of Certification Service Providers and the production of certificates. The audit is carried out by independent audit companies (currently two) designated by the minister responsible for informatics and supervised by National Communication Authority. The security and quality of electronic signature and certification services in Hungary is ensured by these controls. Presently four Certificate Service Providers are operating in the Republic of Hungary.

Several non-PKI-based identification systems are used in Hungarian e-government applications, such as a smartcard solution in tax revenue procedures between 2004 and 2006 and 'Client Gate' from 2005. 'Client Gate' is a web-based online authentication system operated by Senior State Secretariat for Informatics. Registration occurs in local administrative offices with an identity-check; later several governmental services are accessible via this portal after SSL username and password authentication.

# 3 Problems of Digital Sustainability

The long-term preservation of electronic documents, especially of the electronically signed ones, is a complex task. The electronic data and its physical form must be protected from destruction. It is necessary to solve the long-term probative value of the electronic signature by the storage of its certification path, and it is also necessary to ensure access to the application capable of opening the given document.

The long-term preservation of the soundness of electronic data is aggregate combination of physical, logical and operational safety tasks [13]. In all cases, the redundancy of the data storage system and safe long-term storage of data storage devices is necessary.

6 Eat. 2. § 15.
7 Eat. 3. § (2-3) family law and judicial proceedings, unless the law explicitly allows
8 Eat. 2. § 17.

## 3.1 Excessive Velocity

The Hungarian government is struggling to move citizens' and other clients' paper-based activities to electronic procedures. This means in the long term, in practice, the creation and usage of electronic documents exclusive. This endeavour seems an exaggerated foreshadowing process in certain cases.

Legislators have not provided time for the conversion from paper-based processes to electronic ones. For example, the electronic tax return, electronic records management and the electronic firm registration happened this way. The majority of companies had less than one year to switch to the electronic tax return in the firm registration procedure; some companies had only half a year. There was no possibility for lawyers to register companies without adopting new technologies and knowledge [14]. We can consider this as switching to digital communication from the traditional written communication. We practiced the traditional communication for several thousand years, yet the number of illiterate people is one hundred thousand in Hungary [15]; therefore, a paradigm shift of this scale seems hopeless in several years. Well-developed countries, which have already introduced these steps towards digital communication maintain the opportunity to use paper-based documents. For example, in Austria the electronic firm registration procedure was available in the 80s with computers via the telephone network, a considerable part of public and criminal procedures became electronic in 90s, and a refining of the informatics opportunities for payment became available in this decade. Despite this intense and continuous development, the clients still have the opportunity to use paper-based documents in the above procedures, which he or she can download from the website of the Ministry of Justice.

## 3.2 Diversity of Formats

The variety of formats and the resulting diversity of processes and differences of applications have caused considerable difficulties until now and probably will cause them later as well. The well-known and more or less widely used electronic document file formats are the plain text file (txt), Microsoft Rich Text Format (RTF), and the Portable Document Format (PDF). Currently in Hungary TXT, RTF 1.7, PDF 1.3 formats fall under interpretational obligation by authorities in electronic administrative procedures [16]. The primary disadvantage of these formats is that these are unstructured; therefore, these can only clumsily be processed in automatic systems. The Microsoft Word document (DOC) is more widely used, but it is a licensed, proprietary format; its precise construction is Microsoft's trade secret. This has made it impossible for any other companies' software to be fully compatibility with it. To correct these generation faults both developer sides (Microsoft and OpenDocument Foundation) made new formats based on XML. Extensible Markup Language (XML) is a general aim descriptor

language, with the goal of the formation of special descriptor languages. XML, which is an improvement on the SGML language standardized by ISO in 1986 [17], became a W3C recommendation in 1998 [18]. The aim of XML is to structure data. It is licence-free, platform-independent and widely supported. An XML document is valid if it is well-formed (suits for the syntax of the XML language) and it matches a defined content rule, which defines the accepted value types and value places. This definition of the rules can be done with Document Type Definition (DTD) or XML Schema Definition (XSD). The OpenDocument format (ODF) developed by OpenDocument Foundation [19] and Office Open XML (OOXML) developed by Microsoft [20] are based on this technological framework. These formats may become the widely used future document formats. The forms possess unique XSD with severe bindings based on this technology and can be automatically processed.

The general and the records management metadata problems are professionally particular, but in administrative informatics there are considerable questions. These are about in what kind of form, value and entity the metadata (data about data) appears. Many initiatives have been initiated to try to resolve this issue: the Dublin Core Metadata Initiative (DCMI), Managing Information Resources for e-Government (MIREG), GovML and PSI Application Profile [21].

A foreign country example for the format problem is that it was not possible to restore the measurement data of the Viking space probe stored on magnetic tape in 1976. It was necessary to type in everything again from the earlier printed documents because the stored format was unknown.

## 3.3 On-Line Data Security

If we store the electronic data in a working computer system on-line, it is necessary to protect the system physically against disaster losses (fire, water damage, even by the public utility drinking water supply or drainage, earthquake, the destruction of the object due to other reasons); against incidents due to a deficiency of technical requirements (deficiency of power supply, power supply disturbances, the deterioration of climatic circumstances (which may be temperature or humidity problem), informatics network problems)); against electromagnetic disturbances (even in case of intentional damage); and against technical reliability problems (production mistakes, fatigue, other breakdowns). The logic safety covers the reliability of software elements (the operating system, applications), protection against intentional damage (viruses, worms, malicious programs, network attacks, and hacker activity), the security of network protocols, setting rights, identity management and access management. [22] The reliability of software components could be enhanced by defensive programming techniques, with mitigating risks like data leakage vulnerability. [23]

## 3.4 Offline Data Security

The storage of the digital data can be done on optical or magnetic media if the data does not change, and this solution seems to be more beneficial in terms of expenses. The primary medium of optical data storage is the DVD nowadays. This is not an eternal data storage solution, contrary to public belief. Depending on the quality of the disk we may be confident of the survival of the data up to at most 10 years, but based on the author's own experience, the data can be lost from the disk even after two years. Arising from this, it follows that in the case of optical data storage use, periodic regeneration is inevitable, which in practical terms means copying the discs. The benefit of the optical data storage is the insensitivity to electromagnetic fields, but it is necessary to maintain the suitable temperature, humidity and mechanics at the time of storage. The other widely used data storage is magnetic tape, which has a longer history than optical drives. The capacity of magnetic tape storage still exceeds the capacity of the optical; a cassette tape can have one Terabyte capacity.[9] Over all of requirements of optical storage, the requirement of protection against electromagnetic interference (EMI) also appears. Regular regeneration of the media is necessary because the magnetic carrier demagnetises over time.

Those who store or archive data must provide the necessary environment for the opening of electronic documents, but users and operators are inclined to forget this requirement, despite its particularly large significance. Presupposing the worst case, imagine we have to open a stored electronic document 100 years later. The word processor application was made by a software-developing firm working in a garage in 1992. The format of the document does not comply with any kind of standards, and the full computer architecture has changed, but legal regulations do not allow the document to be destroyed. In this naturally strongly polarized example we have to store the archived document, the application able to open the document, the operating system capable of running the application and the full hardware configuration capable of running the operating system. The simplification of this procedure can be done by the emulation of a system capable of all of the above or a special realisation of the emulation and the migration called Universal Virtual Computer (UVC) [24]. This problem arose already at the time of the research of the state security documents after the political transformation in Hungary, when the researchers were unable to read important documents stored on magnetic tapes, because the proper reader could not be obtained or reproduced.[10] Of course the interest in keeping this information secret may be playing a part in this issue.

[9] see http://www.ibm.com/systems/storage/tape/

[10] Based on the oral information of Dr. Trócsányi Sára, head of department of Office of Data Protection and Freedom of Information Commissioner, Hungary, Pécs, November 15, 2008.

As a mixed on-line and off-line data security solution for general documents, records and book digital libraries can be used as a part of conventional libraries [25]. This solution has been under research for a decade in the Western countries, but is not well known in Central and Eastern Europe.

## 3.5 Authenticity of an Electronic Signature

The validity of the electronic signature is provable after a couple of hours or days. The reason of this is that in order to check the validity, we toned to know the current certificate revocation list (CRL) of the CA at the time of the signature, in which the certificate service provider publishes the certificates revoked due to being compromised or to something else. This time can significantly be reduced with the use of Online Certificate Status Protocol (OCSP). After this procedure, the authenticity of the electronic signature is continuously provable, if the revocation lists and the full certification path is accessible. The electronic archiving activity receives a role here: at the moment of archiving, the valid authentication data is stored and re-authenticated by the electronic archiving service provider. Thus the authenticity of an electronic document signed by the archiving service provider depends only on the existence of the electronic archiving service provider, but is not influenced by the falling out of a part of the certification path, for example by the terminating of CA activity or the compromise of the CA key. This is the point where the electronic archiving service provider's activity rises above the issue of the simple safe data storage.

**Conclusions**

It follows from the previously expounded manifold requirements and problems that during storage and processing of electronic documents, an organization faces serious difficulties. The risk stemming from the outlined problems is diverging in different countries. The faster that digital communication develops, the harder it is to find time to solve problems. Therefore the chance of a later escalating of troubles increases.

The rapid development of administrative informatics in Central and Eastern European countries belongs to this category [26]. In to the author's opinion, these countries did not analyse well enough the 30 years of experience of Western European states in this field, even though avoiding same mistakes would be possible that way. These undiscovered problems may cause serious data loss in the government sector.

Digital preservation deals with the dangers stemming from the above-mentioned problems and with the protection against them. The hypothesis of an apocalyptic future because of all the above is called the digital dark age [27]. According to this theory, most of the electronic documents made in the 21$^{st}$ Century will disappear with just a few written memories remaining, similar to the Middle Ages. Leading representatives of this theory are the Getty Research Institute researchers [28], and

Kuny, Terry [29]. However, a refutation was also born which states that the experiences until now are only examples of deficiencies in data restoration, not in data loss [30]. As a comprehensive solution to the technical problems, an ISO reference model was made called Open Archival Information System (OAIS) [31].

Against the excessive speed, better policymaking may provide protection in Hungary; for the format problem and partially data security problem, stricter regulation may provide protection. The efficient handler of the electronic signature and the partially data security problems should be the electronic archiving service providers working on the market. Certainly, because the complexity of these problems and the deficiency of the market, many claim there is no electronic archiving service provider working well (in a suitable measure used) in Hungary. On the other hand, the organisations obliged to preserve electronic documents reckon that they are able to do justice to these requirements with their own infrastructure and human resources. Based on the author's own experience the village local governments with ten employees also think that they will be able to satisfy this task on their own, but it does not seem so in the long run.

As a problem statement for further research we could find out the exact specialties of digital sustainability in Central and Eastern Europe and make recommendations on reducing the gap between WEU and CEE states.

**References**

[1] Rubin, J. S., 'The Printed Book: Death or Transfiguration', Journal of the World Book Community, 1990, Vol. 1, No. 1, pp. 14-20

[2] Kevin Bradley, Defining Digital Sustainability, Library Trends, 2007, http://findarticles.com/p/articles/mi_m1387/is_1_56/ai_n21092805/ [2009. 11. 01.]

[3] Köpeczi, B. (eds.) 1974, Az embergéptől a gépemberig, Minerva, Budapest. p. 206

[4] Kita, C. I., 'J.C.R. Licklider's Vision for the IPTO', IEEE Annals of the History of Computing, 2003, No. 3, p. 65

[5] ITTK, Hungarian Information Society Report 1998-2008, ITTK, Budapest, 2008. p. 38

[6] Horváth, L., Lukács, Gy., Tuzson, T., Vasvári Gy., Informatikai biztonsági rendszerek, BMF-E&Y, Budapest, 2001, p. 111

[7] Virasztó, T., Titkosítás és adatrejtés. Biztonságos kommunikáció és algoritmikus adatvédelem, Netacademia, Budapest, 2004, p. 50

[8] Menezes, A., Oorschot, P. van, Vanstone, S., Handbook of Applied Cryptography, CRC Press, 1996, p. 284

[9] Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A., Molnar, D., Osvik, D. A., Weger, B. de, MD5 Considered Harmful Today. Creating a Rogue CA Certificate, 2008, http://www.win.tue.nl/hashclash/rogue-ca/ [2009. 12. 03.]

[10] Abdul-Rahman, A., The PGP Trust Model, EDI-Forum, Langdale, 1998

[11] Act XXXV of 2001 on Electronic Signatures in Hungary

[12] Jacsó, T., Az ügyfélkapu és az eBEV használata, Saldo, Budapest, 2006

[13] Ross, S., Hedstrom, M., 'Preservation Research and Sustainable Digital Libraries', International Journal on Digital Libraries, 2005, Vol. 5, No. 4, pp. 317-324

[14] Szilágyi, K. B., Az elektronikus cégeljárás gyakorlati kézikönyve, Jogászoknak Kft., Pécs, 2008, p. 4

[15] UNESCO, UIS Statistics in brief, UNESCO, Paris, 2008

[16] Decree No. 12/2005. (X. 27.) IHM of the Minister of Informatics and Telecommunications on the technical rules on documents which can be applied in electronic administrative procedure, 1st appendix

[17] ISO 8879:1986 Information processing, Text and office systems, Standard Generalized Markup Language (SGML)

[18] World Wide Web Consortium, XML Core Working Group Public Page http://www.w3.org/XML/ [2009.11.15.]

[19] ISO/IEC 26300:2006 Open Document Format for Office Applications (OpenDocument) v1.0

[20] ISO/IEC 29500:2008, Information Technology – Office Open XML formats; ECMA-376 Office Open XML File Formats - 2nd edition (December 2008)

[21] Bountouri, L., Papatheodorou, C., Soulikias, V., Stratis, M., 'Metadata Interoperability in Public Sector Information', Journal of Information Science, 2007, No. 7, pp. 1-25

[22] Illési, Zs., 'Számítógép hálózatok kriminál technikai vizsgálata', Hadmérnök, 2009, Vol. 4, No. 4

[23] Schindler, F., 'Coping with Security in Programming', Acta Polytechnica Hungarica, 2006, Vol. 3, No. 2, pp. 65-72

[24] Lorie, R., The UVC: a Method for Preserving Digital Documents - Proof of Concept. IBM Netherlands, Amsterdam, 2002

[25] Hamilton, V., 'Sustainability for Digital Libraries', Library Review, 2004, Vol. 53, No. 8, pp. 392-395

[26] Otjacques, B., Hitzelberger, P., Feltz F., 'Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing', Journal of Management Information Systems, 2007, Vol. 23, No. 4, pp. 29-51

[27] Wikipedia, Digital dark age. http://en.wikipedia.org/wiki/Digital_Dark_Age [2009.11.20.]

[28] MacLean, M., Davis, B. H. (Eds.), Time and Bits: Managing Digital Continuity. Getty Publications, Los Angeles, 2000

[29] Kuny, T., A Digital Dark Ages? Challenges in the Preservation of Electronic Information. IFLA, Copenhagen, 1997

[30] Harvey, R., So Where's the Black Hole in our Collective Memory? A Provocative Position Paper (PPP), 2008, http://www.digitalpreservationeurope.eu/publications/position/Ross_Harvey_black_hole_PPP.pdf [2008. 10. 28.]

[31] Consultative Committee for Space Data Systems, Reference Model for an Open Archival Information System (OAIS) CCSDS Secretariat, Washington, DC, 2002