PERIODICA POLYTECHNICA SER. SOC. MAN. SCI. VOL. 11, NO. 1, PP. 67–82 (2003)

PROBLEMS IN THE IMPLEMENTATION OF THE ELECTRONIC SIGNATURE

Krisztián EGERSZEGI and Péter ERDŐSI

Department of Information and Knowledge Management
Budapest University of Technology and Economics
H–1521 Budapest, Hungary
Phone: (36 1) 463-1832, Fax: (36 1) 463-1225
e-mail: egerszegi@itm.bme.hu, erdosi@itm.bme.hu

Received: January 9, 2003

Abstract

Electronic signatures are not a new invention; the theory behind them has been around for more than 25 years. Yet, their practical application has not become massively widespread to the present day, and Hungary constitutes no difference in that respect. In addition to providing an outline of the present context of electronic signatures, the study goes thoroughly into the conditions of applicability, from a functional point of view, and fitted into the conditions of Hungarian society. A separate chapter examines the issue of security, as one of the most important conditions of applicability. Security is explored also from an encryption and IT perspective, demonstrating the fact that there is yet enough to be done until full acceptance is achieved.

Keywords: cryptography, electronic signature, digital signature, encryption, decryption, certificate, Public Key Infrastructure (PKI), certificate authority (CA), IT security.

1. Definition of the Electronic Signature

The EC Directive 1993/93/EC created the basis for the legal acceptance of the electronic signature in the EU member states. This directive defines the electronic signature as a data item in electronic format that is attached or logically associated to another piece of electronic data and can be used as a certification method. This includes the automatic signature file attached to the end of an e-mail message that contains the name of the sender, or the digitized image of the manual signature. More advanced electronic signatures are those that can be matched uniquely to the signer, identify the signer, the signer has the control over the entire process of their creation, and they are attached to the relevant data in a way that allows the detection of any ulterior changes made to the data. Although the Directive is theoretically formulated in a platform-independent manner, its terminology practically contains the elements of the Public Key Infrastructure (PKI) system [5].

The Hungarian legislation created the law regarding the electronic signature following the principles of the EU Directive. In its definition, the electronic signature is some electronic data or document used for the identification of an electronic document and is inseparably attached to the latter. An electronic signature of enhanced security is suitable for the identification of the signer and can be matched

uniquely to the signer, is created with a tool controlled exclusively by the signer, and is connected to the contents of the document in a way to enable the detection of any changes made to the document after the signature has been attached to it. Additionally, the qualified signature is defined as an electronic signature of enhanced security created using a secure signature creation tool, and for which a qualified certificate has been issued with the purpose of authentication [1].

The ETSI ES 201 733 standard that contains the electronic signature formats (hereinafter: the Standard) focuses on the success and further development of the electronic commerce. From this point of view, the electronic signature is 'an important security component that can be used to protect the reliability of information and of the electronic business.' Therefore, the electronic signatures created according to the Standard appear as proofs of an explicit assumption of certain responsibilities between the parties of an electronic transaction. That is, the Standard focuses on the validity of the signature, including every requirement regarding creation of the signature, as well as those needed to prove its authenticity to the recipient. The Standard states that the term 'electronic signature' used in the Standard is equivalent to the term 'advanced electronic signature' used in the Directive. The public key cryptography is nominated here as mathematical background, although the signature formats are extended beyond the digital signature [8].

1.1. MAC Code

From cryptographic point of view, the electronic signature concept includes the Message Authentication Codes (MAC) and the digital signature (DS). The MAC is a fixed-length data generated from the message itself and a secret key – typically a symmetrical cryptographic key. The recipient will re-generate the MAC code from the secret key they hold and the message received, and this code must be the same as the received code, unless the message was altered during transmission. This method, however, will not ensure undeniability, since any person who holds the secret key can generate the same MAC code from the same message. It can be a suitable solution for a small number of parties, where the key used for coding or decoding can be securely communicated to each other, or they can agree on the coding procedure prior to communication without the risk of giving away information to any unauthorized party. The drawback of symmetric cryptography is that confidential handling of the keys is not really feasible in case of a large number of parties, and the communicating parties cannot be uniquely identified because of the identical keys [2].

1.2. Digital Signature

Asymmetric cryptography may provide a good solution to eliminate the drawbacks of symmetric cryptography.

It is not necessary to previously agree on the procedure and the key used, as the signature/encryption and the verification/solution are realized using the same procedure, but with the use of two different keys. The property of these keys – the public key and the private key – is that although they cannot be created from each other, the public key is suitable to determine that a message encrypted with the private key has been encrypted with that particular private key.

Creation and verification of the digital signature is in fact a digital fingerprint generated from an arbitrary data set, i.e. the transformation of a unique fixed-length array of digital signals generated from a data series, using an asymmetric pair of keys. The senders encrypt with their own private key the fingerprint generated from the data to be transmitted. The recipients decrypt the fingerprint using the sender's public key, and re-generate the message using the known algorithm, thus checking whether the transmitted data have been altered during transmission.

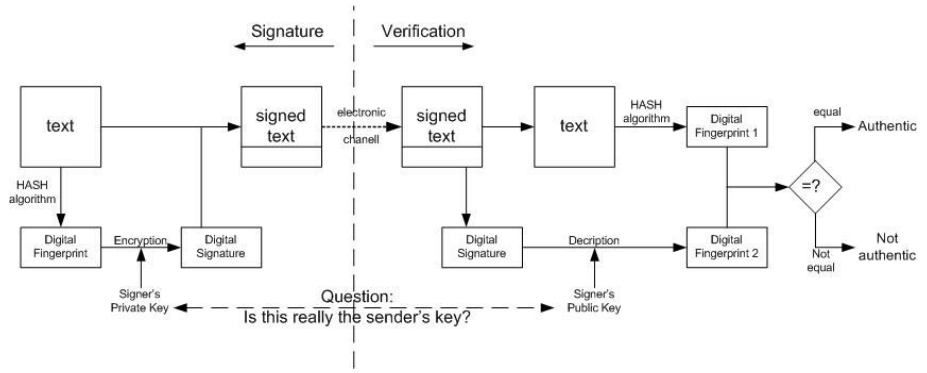

Fig. 1. The process of creation and verification of the digital signature

This property is suitable for the identification of the communicating parties in the course of electronic communication, provided that it can be proven that the private key corresponding to the public key is the exclusive property of the sender. It is not easy to be determined, as the communicating parties are usually in different geographical locations, i.e. the digital signature alone does not provide a complete solution for the identification of the communicating parties. This issue can only be solved by involving a creditable third party [10].

1.2.1. Certificate-based Authentication

Certificate-based authentication can be implemented with the PKI (Public Key Infrastructure) systems, and can guarantee the identity of the communicating parties through certificates.

A PKI system may include – without being limited to – the following components:

Signature Policy and Regulations

- Certificate authority
- Registration authority
- Certificate distribution
- PKI-compliant applications

It is important to see that the digital signature and the issue of certificates appear as separate functions in the PKI system. A digital signature system may be implemented without certificates, as well (e.g. PGP), and the verification keys of the digital signature may also be certified. Of course, the latter can provide higher reliability if it is properly implemented [3].

Further elements that can be implemented in the PKI system:

- *timestamping* (TS): placed behind the digital signature, it certifies that the document (commitment) provided by the signature did not exist before the timestamp, and ensures the continued authenticity of the digital signature after the certificate expires or is withdrawn.
- the *online certificate status provider* (OCSP): it allows online verification of the validity of a signature (this is important especially for immediate transactions)
- *attribute authority*: this helps to decide whether the signer is authorized to sign a specific document (e.g. limited-value signatory authorization)

In this structure, the above-mentioned creditable third party is the Certificate Authority (CA) that produces the certificates related to digital signatures. The CA certifies that the user and the public key corresponding to the user's private key belong together, and it holds the user responsible for the confidentiality of the private key. So the certificate contains the user's specific data and public key. In addition, the CA has to keep official records of the certificates issued and their status (validity, expiry and its cause, expiry date etc.), and has to make those records available via a public communication network for those concerned, in order to allow them to check the authenticity of their communication partner and of the messages.

The certificate usage method and conditions have to be defined in the related regulations, which have to be accepted by those concerned, and the users have to be trained properly regarding the usage of the certificates.

1.2.2. Certificate Types

Certificates can be issued for various reasons, therefore they can be of different types: organization, role, person and tool certificates.

- *Organization certificate*
  The certificate serves for the certification of an organization or an organizational unit of that organization. It allows the creation of an organization-level signature. In case of a company this corresponds to the company signature.

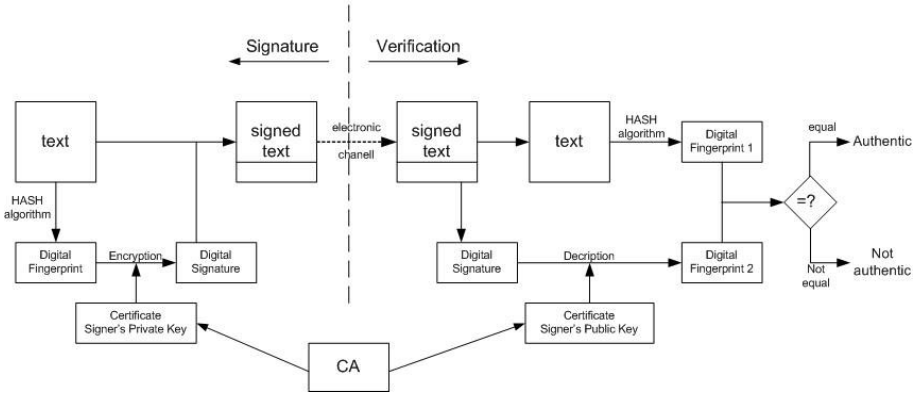

Fig. 2. The process of creation and verification of the digital signature with CA

- *Role certificate*

  This certifies that a natural person is the member of an organization, and, in addition, it can also certify the role of that person within the organization.

- *Personal certificate*

  This serves for the identification of a natural person.

- *Device certificate*

  The device certificate is used to certify a certain device, such as a server.

When using a certificate, it is important to know when and what type of certificate to use, because a person may have several types of certificates, according to his/her role within the organization. For example, a person who is authorized to use the company signature should not use his personal certificate to authenticate a contract, because the personal certificate is not enough for this purpose; he has to use the organization certificate – just like the company signature on paper documents – in order to assume responsibilities in a reliable on behalf of the company [9].

2. The Environment of the Electronic Signature

No special infrastructure will be used to create and verify the electronic signature. This new service will be integrated in the existing IT environment. This means that the signatory and signature verification environment is part of an IT micro-culture, which is an element of an IT macro-system. In a wider sense the given macro-system can be considered as the (global) environment of the electronic signature, but in this article we will only discuss the more restricted micro-environment.

2.1. The Signature Creation Environment

The signature creation environment means all the hardware and software elements used to create the signature. This includes the device used to display data that will be signed (for documents it can be a word processor), the utility or built-in program for cryptographic operations, the hardware with the operating system and network that supports it, as well as the card that generates and stores the keys, together with its software and interfaces.

2.2. The Signature Verification Environment

The signature verification environment is usually integrated with the signature creation environment, i.e. the clients of the signature systems can create as well as verify signatures. But the separation of the two systems could be justified by the fact that those who can assume responsibilities are fewer than those who can verify their fulfillment. For instance, in a dictatorial organization fewer people are entitled to issue orders than those entitled to verify and carry out those orders. It is equally true that the signature verifiers might need to create signatures in other situations, therefore it is not recommended to separate the two types of operations.

3. Cryptography Issues

If we examine the algorithms used today for signature creation, we will notice that the most frequently used one is the RSA. This algorithm – after the 25-year copyright protection expired – became open and publicly available. Its decryption is difficult due to the factorization problem of the integer numbers.

The RSA algorithm uses the *modulo-m* arithmetic, the theory of division with remainder. Its strength comes from the issue of factorization, decomposability and factorization into integer factors of the integer numbers [12].

Let p_1 and p_2 be two arbitrary prime numbers, i.e. numbers that can only be divided by 1 and themselves. Let m modulus be:

$$m = p_1 * p_2,$$

then

$$\Phi(m) = (p_1 - 1) * (p_2 - 1)$$

is the Euler function of the m number, that is, the number of the relative primes of m between $1, 2, \ldots, m$. Let us choose an arbitrary e natural (non-negative integer) number, for which

$$1 \leq e < \Phi(m),$$

both e and $\phi(m)$ are relative primes. Then we can unequivocally determine a d number, which is the multiplicative inverse of e, that is

$$d * e \equiv 1(\text{mod } \Phi(m)).$$

In this case, one of the keys (e.g. the public key) will be the (m, e) pair, and the other (e.g. the secret key) will be the (m, d) pair.

Let M be the message to be encrypted, where

$$1 \leq M < m.$$

The encryption operation will be

$$M_{\text{enc}} \equiv M^e(\text{mod } m),$$

and the decryption operation will be

$$M \equiv M_{\text{enc}}^d(\text{mod } m). \qquad [4]$$

3.1. The Issue of Prime Numbers

The input parameters of the RSA algorithm will include prime numbers as well. The implementation has to generate these numbers, and has to verify that they are indeed prime numbers.

Probabilistic and deterministic methods are available for this operation. The probabilistic tests are quick and efficient, but do not fully guarantee that the randomly generated number of the proper size is *actually* a prime. On the contrary, the deterministic methods provide mathematically proven results, but their efficiency in generating a large number of primes is questionable [7].

3.2. The Issue of the Small Prime Numbers

If the input parameters of the RSA algorithm include small prime numbers (under 512 bits in size), then their factorization – and consequently the full decryption – is finite, and can be done in a short time. For example, a SUN SuperSPARC machine with 2×40 MHz processor performed the factorization of the product of 20-digit prime numbers (in the decimal system) in 35 minutes, of 35-digit prime numbers in approx. 2 hours and of 40-digit prime numbers in 21.5 hours [11]. The current top performance in factorization was achieved for the 155-digit product of two 78-digit primes, completed in 110 days using 300 PCs (on August 22, 1999) [13]. We presume this operation would take considerably less time today, using high-performance resources.

3.3. The Issue of Near Prime Numbers

If we select two near prime numbers as basis for the key, there are factorization methods that can be used efficiently in this case – that is, they are much faster than the full testing methods. That is why not only the selection of adequately large prime numbers, but the issue of the difference between them being large enough should be taken into consideration [11].

3.4. The Issue of Selecting the Exponent

During the encryption process the exponent provides the power to which the data to be encrypted (binary number) will be raised. Exponentiation requires many operations, therefore the selection of the exponent is very important from the efficiency point of view – especially for lower-performance chip cards. The most commonly used exponent is the 2^{2k+1} form, as these can be more easily handled in the binary system. However, as we know since 1997 (the Coppersmith theorem), from the security point of view, if the exponent is a small number, short messages can be decrypted.

3.5. Functional Issues

The expectations regarding the electronic signature in mid-2002 are exaggerated and contradictory. On one hand, there is a strong demand for the electronic document exchange to eliminate the deficiencies of the traditional document exchange (signature, stamp, ulterior modification, etc.), on the other hand, new functions should be included to facilitate its usage. But it is exaggerated to expect that the electronic signature will solve everything, and will work like a magic potion *for everything*.

3.6. Which Smith?

Many think that the electronic signature works somewhat like this: you select the name of the communication partner and the corresponding public key from a catalog and you can immediately send him a personal encrypted message. The problem arises when you have to find out, which one is your partner in a list of identical names. How can you obtain additional information, in order to identify unequivocally the name corresponding to the public key? Some think that addressing this issue is beyond the scope of the electronic signature system. Indeed, if an Internet provider would publish additional information beside the name and public key (address, phone number, etc.), it would be very difficult to find a form that complies with

the requirements of the data protection law and does not violate the right of self-determination regarding information.

3.7. Is the Certification Authority Really Trustworthy?

For the use of electronic signatures, the system implementations presume and specify that certification of the keys used for electronic signatures by a creditable third party increases the level of security. However, they are satisfied with declaring that the certificate provider is '*reliable*', and are not performing any inquiries regarding this issue. We should occasionally ask ourselves: how creditable is a provider? The answer is simple: as creditable as the users of the service consider it to be. What does or what can a provider do in order to increase its creditability? First of all, it has to create a secure hardware, software and human environment, and must operate a solid security sub-system. On the other hand, it must prevent the occurrence of security breaches (e.g. issuing unauthorized certificates). The sense of security can further be increased by compliance with the requirements of qualification procedures, being governmental or voluntary.

When creating the theoretical background, the authors thought that the service providers will be organized in a hierarchical structure, as a tree-graph, and each higher-level node guarantees the creditability of the subordinate nodes. However, since the tree has a root, who will guarantee the reliability of the root? The answer was: an organization – either governmental or commercial – that is considered creditable by the majority of people. This theory did not materialize. The service providers could not reach an agreement regarding the root provider, therefore the majority of the service providers are self-certified, i.e. they sign the certificate regarding their own private keys. We can only hope that these statements are true.

4. IT Security Issues

4.1. Protection of Font Sets

One of the main conditions for reliably creating a signature is to sign what we see. That is, the signature environment has to display data in a protected manner, otherwise the following situation can occur:

1. The example is generally applicable for numbers, and in case of letters, it is true in case of the Hungarian language.
2. In the signature creation environment we will replace the font set, performing the '$7 = 6$' and the '$\acute{e} = a$' replacements. Of course, we will ensure that the alphanumeric characters '6' and 'a' will not disappear, redefining them over other unused graphic characters.

3. When typing in the document to be signed we will type: '... átvettem **7**.000.000 (h**é**tmillió) forintot...' ['...I received 7.000.000 (seven million) HUF...'] (the characters that will be replaced are shown in italic). The following will appear on the screen: '...átvettem **6**.000.000 (h**a**tmillió) forintot...' ['...I received 6.000.000 (six million) HUF...'].
4. We will ask the party to sign it.

If we want to verify the signed document in another (e.g. the recipient) environment, where the font set is the original one, we will read the following: '...átvettem **7**.000.000 (h**é**tmillió) forintot...' (I received 7 million HUF), and the signature will be OK! And we can claim the missing 1 million HUF from the recipient.

4.2. The Final Result of the Verification

In an inadequately controlled IT environment it is easy for viruses and intruders to access the system and perform activities without the user's knowledge. It is possible to write a malignant program code that captures the final outcome of the signature verification in the communication layer and changes it to '*valid*' in each case. This way there is no need to use crypto-analytic methods to undermine the security of the process, it can be compromised without the need to reveal the secret key.

4.3. Changing the Signature

If the intruder attacks the communication layer, in the absence of proper care he can separate the signature from the sent document, alter the content of the document, re-create the signature and attach it to the changed document – all this, of course, in the name of the original sender. This method is only functional if the recipient does not know the public key of the sender, and receives it attached to the document. In this situation the recipient will *believe* that the changed document was sent by the initial sender. This risk is present in every situation where the recipient obtains the sender's certificates, i.e. the public key from unreliable sources or no reliable CA is included in the process.

5. Applications of the Electronic Signature

The legal background will settle sooner or later. A much more interesting question at this point is: what are the possible uses of the electronic signature creation and verification data (the private and public key, i.e. the PKI). We will discuss the possible applications according to market segments [6].

5.1. Financial and Credit Institutions

5.1.1. Authentication of Electronic Transactions

A very important factor in the propagation of electronic commerce is the possibility to authenticate the electronic transactions, that is, to provide the acceptor of the transaction the certainty that he will receive the expected counter-value. K&H Bank already tested certificate-based home banking in collaboration with MATÁV (the Hungarian Telecommunication Company), and the experience shows that it is operational.

However, a number of differences can be noticed among the various types of certificates. Different certificates are needed for high-value transactions, for different levels of commitment and different user roles, and they can only be used for the purpose and value limit defined when the certificate was issued. This means on one hand that there is unlikely to have an "all-around" super-certificate, and on the other hand it also means that a different certificate (but not necessarily a different key!) is necessary for each field of application.

5.1.2. Digitally Signed Bank Notes

Ever since money was invented, there were always people who took up forgery. Different methods have been invented to prevent counterfeit money. One of the earliest methods was to try the coin with the teeth to make sure it contains gold.

Nowadays, it is not enough to examine the raw material in order to ascertain the authenticity of the money, therefore the bank notes are filled with numerous typographic and other security elements. Counterfeiting is made difficult by microtexts, special graphics, color-processing, color-switching prints, non-repetitive graphic elements, visible fragments and details that appear only if illuminated with ultra-violet light.

However, the prerequisite of unforgeability is not the presence of many security elements on the bank note, but the fact that the data and technology needed to create the bank note itself are not available in commerce. This is the only thing that can prevent professional counterfeiting. The high cost or the long time needed to crack a code would be just a temporary setback, as long as the data and technology are available on the market. The digital signature, the digitally signed bank note could be a key technology in fighting forgery.

The idea of applying digital signature on bank notes came into Hungary from the USA. The technology is based on combining the generation of the digital fingerprint with the two-keyed (asymmetric) cryptography. A digital fingerprint will be generated from the set of digital signals representing the properties of the bank note (e.g. the co-ordinates of the randomly mixed signaling elements, serial number, denomination, issuer, date, etc.). This is a fixed-length series of signs, different for each set, and, encoded with the secret key of the issuer, a unique

identifier will be generated for each individual bank note. This will be visibly marked on the bank note – that is how a digitally signed bank note is created.

What makes this stand out from among all the other security elements is that those can be linked to the denomination value, while the digital signature uniquely identifies a particular bank note. For each bank note a different signature will be created, since there are no two bank notes or bank note papers with identical fiber structure. Thus, if the secret key used for the signature is indeed secret, a third party cannot record on the bank note data that will make the otherwise forged bank note to appear as valid upon verification.

The technology of the digitally signed bank note has been known to the National Bank of Hungary for several years. This non-typographic protection against forgery was already applied for several earlier European currencies. Domestic application of this technology has several impediments. One is of economic nature. For mass distribution, the signature verification devices have to be manufactured at an affordable cost, because even the most refined security element is worthless if it cannot be quickly and easily verified. Another issue is whether it is rational to apply this kind of protection for the domestic currency after the introduction of the Euro. The digital signature should nevertheless become the main protective measure for the bank notes of the future.

5.2. Companies

The companies are already using the electronic signature in several areas, and numerous pilot projects are in progress. In addition to signing electronic mails, there are other important applications. PKI can be used by companies in their private e-business solutions, and in the e-commerce as well. The starting point is when all employees have their own certified pair of keys. Besides signing letters, the electronic signature can also be applied in the following areas:

- access system: access restricted areas using a card and a PIN code, using biometric identification;
- computer login: instead of the traditional user name and password, the employee logs on to the workstation using his personal card;
- access to resources in a network: various network access rights can be granted or denied for the holder of the card (file server, printer, etc.);
- Single Sign On: access to several systems with appropriate access rights, following a one-time identification;
- remote access: the user can access certain parts of the company network from an external location or from his home computer – e.g. using a virtual private network;
- electronic administration (government, bank, etc.);
- tax return, fulfillment of data service duties;
- electronic shopping, etc.

The functions allowed or prohibited by the company regulations are practically up to the management. Usage of the PKI systems within a company has a further considerable benefit: it forces employees to learn how to use the PKI system. This knowledge may become useful at the next job.

The issue is whether the pair of keys will be mobile or not, i.e. if a person holds such a pair, will it be possible to certify it elsewhere following another registration procedure, i.e. will it be possible to carry it along? This, of course, raises many security issues, since the service providers could rightfully require the user to prove that he is the exclusive owner of the key to be certified, especially in case of enhanced security signatures.

5.3. Government

Regarding creation of a governmental certification service, a Government Decree (47/2002) and a Government Resolution (1026/2002) have been issued. These state where electronic signature will be introduced, for the state administration areas the certification authority created by the Ministry of Interior has to create an enhanced security certification authority by September 30, 2002, and a qualified certification authority by March 30, 2003.

What we know for certain is that qualified certificates have to be accepted in any eligible governmental or judicial proceedings. What nobody knows yet is who will be the first qualified certification authority in Hungary. If the business sphere will be satisfied with the authenticity of the enhanced security electronic signatures, then the qualified certificates needed in administrative proceedings will most probably have to be provided for the population by the government. The above mentioned certification authority, however, did not intend to provide qualified certificates for the population.

Another big question is: whom will the governmental certification authority accept as clients, that is, who will it issue certificates to? The possible spheres, from the narrowest towards the wider:

- government officials and closely related external employees;
- pubic servants;
- higher education sphere;
- public education employees;
- everybody.

If the governmental service will not be made widely available, the administration will have to specify the types of certificates it accepts from the citizens within the electronic administration. If it will accept only qualified certificates and it will be the only qualified authority, the circle is closed... If the market segment will have to wait long before the qualified certification authorities appear, the electronic public administration will be impossible or at least restricted during that waiting period.

If the governmental certification authority will not issue certificates for the government officials only, it is justified to ask whether it will limit its responsibilities in any way? Will such a restricted certificate serve the planned purpose?

According to APEH (the Hungarian Tax and Financial Auditing Office), the governmental certification authority represents the long-term guarantee for the propagation of electronic tax return among the tax payers, but it forecasts that the first electronically signed and certified tax return will not be received before the 2002–2003 tax year. If the governmental one will be the first qualified certification authority, then APEH has to be prepared to receive electronic tax returns by the 2003 tax year.

An additional problem is that the demand for the use of this service cannot be considered as massive, not even in the governmental sphere. In addition to ensuring authenticity, the PKI system can also be used to protect confidentiality, although not with the same pair of keys. Despite all this, the technology, as far as we know, is yet to be widely used, even though the government requires very strict confidentiality from its business partners, who are frequently using the benefits of the Internet. It is a security system axiom that if you send something through the Internet without encrypting it, you practically publish it...

The potential users are still waiting, or they approach with very small steps to the daily use. Hitherto they were waiting for the law to be published, then to become effective, then for the decrees regarding its execution, and next they will wait for the establishment of the Communications Authority and of the certification authorities, and the list will continue. However, we have to see that, at the moment, the actual use of the PKI system only depends on the user's determination. The PGP world uses the digital signature for some time now. The issue of confirming the user's identity by a third party can be considered as solved. A PKI system for trial or testing purposes can already be built on open source bases. It seems useful to learn how to use the certificates now, while any mistakes or errors do not yet have severe legal repercussions.

5.4. The Higher Education Sphere

One of the tasks to be completed in the near future is to generalize the use of the electronic signature, a further keystone of modern literacy, in order to ensure that the services based on it are properly used. The international experience shows that this knowledge can come either from the workplace or from the educational system. The use of PKI systems in the higher education institutions could have the additional benefit that – like in the case of employees – the current use of the certificates could become a basic skill that will follow the graduates after they leave school, and can be used in electronic administration as well as in a business environment.

Many of the higher education institutions operate an electronic educational system. Their main problem is solving the issue of authenticity in a reliable fashion, i.e. preventing people to elude the system and perform various operations –

administration, enrolment to classes, recording grades, etc. – in the name of others. If identification is not unequivocal, there is no chance for accountability.

We can also presume that the higher education sphere cannot support by itself the implementation costs of the PKI technology; this will have to be financed from budget sources.

6. Conclusion

The electronic signature is not a magic potion, but undoubtedly it plays a major part in the propagation of the electronic communication and in increasing its security. However, this function will only be fulfilled if the implementations take into consideration the latest achievements in the field of cryptology, and the manufacturers will not improve the efficiency in the detriment of security. To ensure the proper use, the security level of the information systems must be adjusted in order to prevent massive occurrence of security breaches and the subsequent total loss of confidence in the electronic signature.

These are all tasks to be carried out in the near future, since the propagation of the electronic signature is far from being speedy. This could be the consequence of the fact that the demand for the use of the electronic signature is not yet established. The security of the Internet communication is not required by either the governmental or the business segments, and even the academic sphere is just slowly moving in this direction.

Hopefully this situation will change and, after overcoming these teething-troubles, the use of the electronic signature will be synonymous to reliable and secure communication.

References

[1] The Law no. XXXV/01.09.2001 Regarding the Electronic Signature.
[2] MENEZES, A. J. – VAN OORSCHOT, P. C. – VANSTONE, S. A., *Handbook of Applied Cryptography*, October 1996, CRC Press.
[3] BRANDS, S. A., *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, MIT Press, 2000.
[4] STINSON, D. R., *Cryptography, Theory and Practice*, CRC, 1995.
[5] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (13.12.1999).
[6] EGERSZEGI, K. – ERDŐSI, P., *Qualified Signature*, InfoBYTE January 2002.
[7] ENDRŐDI, CS., Analysis of Public Key Cryptography Algorithms Based on Elliptical Curves, Diploma Paper, BME, 2001.
[8] The ETSI ES 201 733 V1.1.3 Standard Regarding Electronic Signature Formats.
[9] FEGHHI, J., *Digital Certificates: Applied Internet Security*, Addison Wesley Longman, Inc., 1999.
[10] FEGHHI, J. – FEGHHI, J. – WILLIAMS, P., *Digital Certificates/Applied Internet Security*, 4th Printing, April 2000, Addison-Wesley.
[11] PETHŐ, A., Parameter Selection in Public Key Cryptosystems, Presentation at the Cryptography Seminar at the SZTAKI, May 7, 2002.

[12] RIVEST, R. L. – SHAMIR, A. – ADLEMANN, L., A Method for Obtaining Digital Signatures and Public Key Cryptosystems.
[13] CAVALLAR, S. – DODSON, B. – LENSTRA, A. K. – LIOEN, W. – MONTGOMERY, P. L. – MURPHY, B. – TE RIELE, H. – AARDAL, K. – GILCHRIST, J. – GUILLER, G. – LEYLAND, P. – MARCHAND, J. – MORAIN, F. – MUETT, A. – PUTNAM, C. – PUTNAM, C. – ZIMMERMANN, P., Factorization of a 512-bit RSA Modulus; August 22, 1999.