Electronic Signature - Selected Problems of The Electronic Signature Law and of Its Implementation

Daniel Olejár
olejar@dcs.fmph.uniba.sk

Faculty of Mathematics, Physics and Informatics,
Comenius University,
Bratislava, Slovak Republic

Abstract

The European Commission identified the need for electronic signature as a key issue for electronic commerce and issued Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. According to the Directive "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001." During the preparation of Slovak e-signature law some key problems determining the philosophy of the law were identified. The other problems appeared when the public key infrastructure (PKI) was discussed. The paper addresses some of these problems and proposes possible solutions.

Keywords: electronic signature law, information security, and public key infrastructure.

1. Introduction

The introduction and massive use of information and communication technologies (ICT) induced profound changes in modern society, sometimes called Information revolution leading to Information Age in the history of mankind. The global connectivity at acceptable price provided by Internet reduced limitations of physical distance and created conditions for birth and growth of e-business, distant working, distant learning, access to enormous information sources, real participation of citizens on decision processes, simplifying the communication with administration, etc. To take advantage of possibilities offered by modern ICT, the society has to create adequate conditions. Though building technical infrastructure is a very important step, it is only necessary precondition for entering into Information Age. Probably the hardest task to be solved is the analysis of traditional processes, mechanisms and paradigms from the point of view possibilities and restrictions of ICT and their redesign or creating new ones.

E-business and other applications of ICT have opened serious information security questions: how to authenticate the partner on the other end of line; how to ensure the integrity of documents in digital form created, sent, processed and stored by insecure devices and communication channels? How to avoid the repudiation of origin or repudiation of receipt of a document? How to solve disputes on contracts made by electronic means? Cryptology offers technical solutions based of so called digital signatures for some of the above-mentioned problems. Nevertheless, to avoid incompatibility of particular solutions and legal problems, the general implementation of cryptographic solutions needs a common legal framework. The European Commission identified the need for electronic signatures (a generalization of digital signatures) as a key issue for electronic commerce and issued Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [1]. According to the Directive (Article 19) "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001."

2. Brief history of Slovak e-signature law

The work on Slovak electronic signature law started in 1999. Ministry of Economy created a working group and in cooperation with Slovak Association for Electronic Commerce (SAEC) prepared a proposal of e-signature law in the mid of 2000. The proposal did not pass the Governmental Legislative Council and became an object of strong criticism from professional circles. Independent experts and professional groups tried to create other proposals but they effort did not bring any significant results. Some members of Slovak National Council recognized the importance of the e-signature law and submitted a deputy's proposal of the law in the end of the year 2000. An expert group (associated with Slovak Informatics Society, see www.informatika.sk/e-podpis/) supporting their initiative was created and though the deputies finally withdrew their proposal, the expert group continued its work on an independent proposal of the e-signature law. (The same did the original SAEC group at the Ministry of Economy.) Though both initiatives have identical goals and the same starting point [1], their efforts resulted in different, mutually incompatible proposals. The Directive [1] itself is not a complete law, it is - as stated in its title - creating only the framework for electronic signatures. National laws based on [1] have to take into account national legislation and the infrastructure, which is necessary to build in order to implement electronic signatures. There are some key problems (technological, organizational and legal), which are to be solved, and the choice of one of possible solutions determines the philosophy of the final law. (That is the reason why the proposals of SAEC and SIS groups differ so much.) Some of these problems are specific for Slovak Republic, but every e-signature law must address most of them. We will discuss some of them in present paper.

3. Key problems of e-signature law

The problems determining the e-signature law are of various natures; the authors must decide which laws and standards they will use as a base of the law, what will be determined by the law and what will be left to ordinances. It must be established some trade-off between security requirements and practically feasible implementation; the requirements of the Directive must harmonize with national legislation. The final form of the electronic signature law will depend on solution of these and other particular problems.

3.1 Philosophy of the law

There are many various standards on digital signatures, UNCITRAL prepared a model law on electronic signatures, and some states already issued electronic signature laws. The principal question is whether to use some of them as a model law, or to write an independent (national) law. The need for electronic signatures exists even before the legislative initiatives of EU, UNO or national governments and it is dictated by electronic commerce. Since e-commerce (or e-business) is global in its nature, creation of a national law can solve some local, national problems; but the possible incompatibility of the national law with international e-signature legislation may be a serious barrier for participation on international e-business. Therefore the first axiom of e-signature law is international compatibility and particularly compatibility with EU Directive [1]. Though various laws declared their compatibility with [1], the reference model for Slovak e-signature law ought to be [1].

The Directive [1] is technologically neutral and does not deal with technical and implementation details. Can the national law be general and technologically neutral, too; or it has to choose some (technological) solutions and describe them in more details? It is difficult to build a functioning system without specification. In present days the only practically implementable solution for electronic signature is digital signature and the public key infrastructure (PKI). The developed states are building their PKIs for some years [3] and though another suitable technology for e-signature can be invented in the future, the money, time and effort invested into PKI make the rejection of present PKI very improbable. Therefore the law can be more concrete then the Directive and describe the e-signature structures and procedures based on PKI in more details. On the other hand, since only a small number of specialists are able to understand highly technological law, therefore the balance among accuracy, understandability and technological details are to be kept. Another reason for keeping technological details out of law is practical - cryptology and information and communi-

cation technology develop so rapidly, that they will induce changes in parameters and procedures used in PKI. To avoid the need for frequent changes of the law, the technical details of e-signature law (such as fees, authorized cryptographic algorithms, length of cryptographic keys, detailed security requirements, et.) will be defined in e-signature Ordinance.

3.2 Scope of the law

Digital signatures of various kinds exist even before the e-signature law will enter into force. Many of them do not satisfy the expected requirements of the law. Will the law take into account these pre-historic forms of e-signatures and tolerate them, or it will ignore them and adopt measures to eradicate all heretic form not satisfying its requirements? Directive introduces two or three kinds of e-signatures: ordinary enhanced e-signature and secure e-signatures. Since the use of e-signatures is associated with certificates issued by certification services providers (CSP), it is worth mention the categories of CSPs defined by the Directive: CSP (can provide its services without prior authorization), CSP issuing qualified certificates and accredited CSP (accreditation is voluntary.) There are four categories of systems, where e-signatures are or will be used:

- Closed systems (e.g. banks) where electronic signatures are used for special purposes (e.g. for securing accountability) and the rules of their usage are based on mutual agreement of all subjects of the system.
- Open systems with ordinary e-signatures, based on non-qualified certificates. E-signatures can be used for authentication, they do not have the legal validity of hand-written signatures and their application for legal purposes is limited but possible.
- Open systems with advanced e-signatures, based on qualified certificates and created by secure-signature-creation-devices. Such signatures satisfy the same legal requirements as hand-written signatures and are admissible as evidence in legal procedures.
- Closed systems with secure e-signatures satisfying additional security requirements (e.g. military, systems with classified information, etc.).

It is difficult to cover all kinds of electronic signatures by a single uniform law and therefore the first and fourth categories of systems will be excluded from the proposed law. Systems from the first category have their own rules and everybody who want to participate and use electronic signature within borders of such system can decided, whether he accept or refused the proposed rules. The last category of systems has its own laws and rules, too, and although technical and procedural requirements on e-signatures valid in these systems will probably meet the conditions of the e-signature law, it will be difficult to apply some other requirements of the law - e.g. some control mechanisms on them. It will be easier to regulate the use of e-signatures in special closed systems by special law than to try to write a law applicable to open and special closed systems at the same time.

The remaining two categories of systems can be regulated by a single law. The SIS group decided to bind the right to issue qualified certificates with accreditation of CPS, since the advanced e-signatures are based on qualified certificates and the CPS issuing qualified certificates must meet some strict requirements.

3.3 Electronic signatures of CA and legal persons

Serious problems concerning electronic signatures of legal persons appear. Natural person can have pair of cryptographic keys and can create electronic signature in his/her own name. The analogy with hand/written signature is straightforward. Legal person does not create hand-written signatures; legal person has statutory representatives and the law considers their signatures as signatures of the legal person. The same solution can be principally accepted for electronic signatures of legal persons. The main problem is the electronic signature of certification authority.

The electronic signature of certification authority is present in every certificate it issued. To verify an electronic signature, the recipient of a signed document has to verify the electronic signature of certification authority and only then he can trust in the content of certificate (signed by certification authority) and verify the electronic signature he obtained. Some officers of CA could be authorized to sign certificates in the

name of CA. The verification of CA's e-signature would be reduced to verification of electronic signatures of some officers of CA. And that can cause troubles.

The verification of e-signatures is based on public keys corresponding to private keys used for creating these e-signatures. To be able to do it automatically, the corresponding public keys must be available for e-signature verifying device. It is difficult to distribute to clients the public keys of all officers acting in the name of CA; and moreover, to inform all clients when some changes appear.

There are at least two possible ways how to solve it: the electronic signature of CA will be considered only as a technical electronic signature and then a unique pair of key will be defined as private and public keys of CA; digital signature created by private key of CA can be verified by corresponding public key, which will be distributed to all clients (certificate holders) e.g. together with certificates, or it can be publish on we, in newspaper, in TV - teletext.

Another solution respects the requirement of personal responsibility for creating electronic signatures of CA. The CA will have pair of asymmetric cryptographic keys; the public key will be published. Some officers are responsible for creating electronic signatures of CA, e.g. for issuing certificates. Every officer will have his key pair. Issuing a certificate, he signs it by means of private key of CA. He must create a record on certificate issuing and sign it by his own electronic signature. Digital signature in certificate, together with electronically signed record creates (advanced) electronic signature of CA satisfying requirements of the Directive (it is capable of identifying the signatory), Slovak legislation (only natural person can sign in the name of legal person, the signature of legal person does not exist) and PKI (stability of the electronic signature of CA and automatic uniform method of electronic signature verification).

There are at least two solutions for electronic signatures of other legal persons: they can be created directly by legal persons statutory representatives, or in a similar way as electronic signatures of CA. The last way will be suitable e.g. for automatic processing of orders in e-commerce procedures.

3.4 PKI architecture

The role the state is planning to play in PKI determines the architecture of the future Slovak PKI. The state certification office (the exact name was not defined, yet) will play the role of root certification authority and of the accreditation board. It will regulate the whole state PKI (issue or approve standards, norms, ordinances, control CAs and their registration authorities, etc.), register the accredited CAs, issue certificates of their public keys, co-ordinate the interaction of its own PKI with foreign PKIs. The basic architecture of state PKI will be hierarchic one, constituting a rooted tree with root CA as root and accredited CAs as leaves. The basic architecture can be slightly modified, since Slovak accredited CAs can mutually cross-certify their public keys. Root CA will not issue the certificates of public keys of non-accredited CAs; on the other hand, they can cross-certify their public keys. The non-accredited Slovak CAs will create an unconnected mesh. The interesting situation can arise when an accredited CA would cross-certify with a non-accredited CA. This is in principle possible, since the accredited certification authority can provide a non-accredited services (e.g. issuing non-qualified certificates, too). If an accredited CA issues non-qualified certificates, it must sign them using another private key than that dedicated for issuing qualified certificates.

3.5 Cryptographic keys management

There are lot of problems concerning generation, distribution, usage, storage, archiving, destroying and reconstruction of cryptographic keys. We concentrate on the following four topics: generation of cryptographic keys for clients, clients' key protection, key escrow and key ageing.

The generation of asymmetric key pair requires special cryptographic module (software or hardware), since the keys must fulfil some qualitative and security criteria (length of the keys, cryptanalytic strength), the uniqueness, etc. There are three principal solutions: to generate the cryptographic keys for clients by certification authority; to provide the client cryptographic software, and let him generate the keys for himself, and finally, to provide client a cryptographic smart card able to generate asymmetric keys of required quality. The generation of clients' keys by certification authority solves the problems of keys cryptographic quality and uniqueness; the CA can generate them on a dedicated hardware cryptographic module, test their quality and uniqueness and export them in a secure way (e.g. it can write them on a secure smart card). It must guarantee the safe erasure of exported keys from the module; otherwise there is a risk of violation private "signature" keys confidentiality. The generation of cryptographic keys by client can rise the client trust in confidentiality of his private key, but the integrity and quality of software cryptographic module must be guaranteed. Only CA, issuing a certificate for the public key can check uniqueness of generated keys. (The existence of the same key pair cannot be excluded, since the CA does not have the records of all certificates issued by other CAs.) In this case the secure storage of generated client keys, requiring a special hardware can be a major obstacle. The third solution - generating keys by client's cryptographic smart card is recently the most appropriate solution. (Besides the generation of asymmetric keys, certification authority can generate other kinds of cryptographic keys for its clients.)

The Directive [1] identified the protection of clients' private keys as a necessary precondition of the legal validity of electronic signatures. The proposed law obliges every signatory (the holder of a key pair used to create and verification of electronic signatures) to protect his private key, but naturally, does not define haw to do it. Specialised hardware modules, particularly smart cards will be appropriate solutions; the risks of other, cheaper solutions must be analysed. (See e.g. [5].)

Key escrow is probably the most controversial service, which may be provided by certification authority. The principle of key escrow is in storing information on secret or public cryptographic keys sufficient for reconstruction of cryptographic keys on demand of a legal authority. Despite of the possible misuse of cryptography to hide criminal operations, the proposed e-signature law does not support key escrow. Certification authority must neither copy nor store clients' private or secret keys if he does not require it explicitly (e.g. the backup of keys).

Keys ageing. The state certification office will define obligatory requirements on cryptographic parameters. Future cryptanalytic methods can discard recent cryptographic keys; and since it could be possible e.g. knowing the public key to find effectively the corresponding private key to forge a signature. Client keys have a limited lifetime, and so the risk is feasible, but there are cryptographic keys used for protection of archive files (e.g. time stamped CRLs). The protection of such files must combine the physical access control with, probably, signing the files by new, secure electronic signatures. If the lengths of cryptographic keys, or cryptographic algorithms used for e-signatures prove insufficient, the whole PKI must be able to adopt new lengths and new algorithms in a short time. The "upgrade" of cryptographic infrastructure can cause nontrivial problems, e.g. with the limited capacity of cryptographic devices like cryptographic smart cards. Such devices are to be replaced and that will be not only complex, but also a very expensive operation.

3.6 Security problems

There are many other security problems concerning e-signatures besides those of cryptographic key management discussed above. We will mention some of them briefly, now.

Availability of archived data. Since e-signatures will have the same legal validity as hand-written signatures, the validity of an electronic signature must be verifiable long time after the certificate of the corresponding public key had lost its force. That means, the certificates, CRLs and other documents together with corresponding cryptographic keys are to be archived for a sufficiently long time. The ageing is not only a problem of cryptographic keys; it concerns media and technical devices for processing the information stored on media, too. The data ought to be rewritten to new media before the old ones would loss their reliability. The required period of archiving some data can result in problems with memory devices. The progress in information technologies is so rapid, that devices common some years ago are not available in present days. To establish the availability of archived data, the archive has either to rewrite the data periodically to new media, or to maintain old storage devices in operable state.

Security aspects of signing. The signing procedure can be in general described as follows:

- The signatory creates a document/he receives a document; the document to be signed has the form of a computer file and it is in the memory of a computer
- Signatory activates the signing procedure, he submits his private key (in encrypted form) to computer
- The signatory authenticate himself to computer to decrypt the private key; the computer creates the electronic signature for the given document
- The plaintext form of signatory's private key is deleted from computer memory

Instead of submitting private keys to computer (they are usually stored in encrypted form in computer's memory), the signatory possessing a cryptographic smart card or other hardware cryptographic module, can load the document into card/module memory and create document's signature in a secure environment. Some drawbacks of the above mentioned procedures are oblivious: the private key exists for some time in insecure computer environment in open form. The operational system can swap memory and create a copy of signatory's private key. It would not be difficult to enhance the functionality of signature creation software to capture signatory's password or even private key. Therefore the confidence in software cryptographic modules must be found by integrity checks and - maybe - access control. The use of proprietary cryptographic device (smart card or hardware cryptographic module) for signing a document protects the confidentiality of cryptographic keys, since they would never leave the device. Another serious problem remains open: what is in reality the signatory signing? The common editors (like Word) will be used for preparation of documents that are to be signed. The document contains apart from the visible text some information on fonts, style of document and another information, which is not under the control of signatory. (Many signatories are probably not aware of this problem). To meet the legal requirement that the signatory confirms by his signature his agreement with the content of the document he signed, the content of the document must be separated from the structural information on the document. Since most signatories will not work with text-editors that are not user friendly, it can be hardly expected, that special low-level editors will be used for creation of documents, which are to be signed electronically. We do not know a satisfactory solution of this problem.

Security problems of electronic signature were discussed in more details in [4].

4. Conclusions

Electronic communication and commerce necessitate electronic signatures and related services allowing data authentication. European Union issued the Directive [1] to create the EU framework for electronic signatures. Electronic signature law has legislative, cryptological, technical, organizational and security aspects. Ignoring or misunderstanding of some of them can cause serious problems. Having been engaged in preparing Slovak electronic signature law and in building a commerce certification authority, we address in this paper some - particularly security - problems concerning electronic signatures and of the building of public key infrastructure. An expert group preparing the law solved some of them, while for the others the experts did not succeed to find satisfactory solutions.

5. Acknowledgement

The author thanks his colleagues from the working group for preparing electronic signature law at Slovak Information Society for many fruitful discussions; the members from the SAEC group for their critical remarks, dr. František Šebej, PhD., the chairman of Integration committee of Slovak National Council for his personal engagement in e-signature law and the Company Ditec a.s. for its support.

6. References

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

[2] European Electronic Signature Standardization Initiative (EESSI). Final Report of the EESSI Expert Team, 1999.

[3] Implementing Public Key Infrastructure in Government. Report from an International Meeting in Oslo, Ministry of Labor and Government Administration, Oslo, 2000.

[4] Janácek, J., Ostertág, R.: Problems in practical use of electronic signatures. Submitted to IFIP WG 9.6/11.7 SCITS-II working conference

[5] Stanek, M.: Útoky na cipové karty. 1. medzinárodná konferencia Bezpecnost informacných systémov vo financnom sektore, Bratislava 1998