THE ELECTRONIC SIGNATURE

Gramada Dragu Argentina
University "Titu Maiorescu " Senior Lect. Voiculescu Madalina Irena Phd. University "Titu Maiorescu" Faculty of Economics

Cuvinte cheie : digital signatures, electronic commerce, secured devices to generate electronic signatures

Article refers to significance and the digital signature in electronic commerce. Internet and electronic commerce open up many new opportunities for the consumer, yet, the security (or perceived lack of security) of exchanging personal and financial data is still a major concern amongst all kinds of users. We believe that only digital signature technologies based on public-key cryptography can guarantee the necessary security and consumer confidence.

The exigency in the conclusion of a written legal document, ad validitatem or ad probationem, is satisfied by the electronic document with an incorporated electronic signature, based on the acknowledged certificate and generated with a signature creation device.

The Internet has become a commercial means, with its own legal regulations. The new technologies allow for more widely spread and cheaper access, storage and transmission of *information*. The current economy is built around the information, and especially around the information on the internet, and the promotion of **electronic commerce** is connected to an appropriate legal approach.

The digital information can be transformed into new social and economic value, creating immense opportunities for the development of new products and services. The information becomes thus a **key-resource** for the digital economy.

The electronic signature is a new challenge, given the EU integration aspirations. It comprises electronic data which are attached to or logically associated to other electronic formatted data, and serves as an identification method.

Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender had access to the private key (and therefore is likely to be the person associated with the public key used), and the part of the message that has not been tampered with. On the question of authenticity, see also message digest. [575]

The international practice and the attempts to regulate the issues related to the yet fragile security of the electronic documents have found a remedy: the Certification Authority. Mainly this body should be a public service (the city hall, the government) or a private service (company).

The American Bar Association ABA has described the in "Guidelines for Digital Signatures", the *conditions* an electronic signature should comply with so as to be accepted legally, the technical means to implement the electronic signatures as well as the imposed requirements of the Certification Authority (to be in the possession of the financial resources to maintain the operations as per the declared obligations, to have the capacity, within reasonable limits, to take the risk of the responsibility towards the subscribers, to the individuals and companies that rely on the certificates it issues)[576].

The International Chamber of Commerce has recommended the use of a cyber notary as an important element, also called trusted third party, in the safe management of the electronic documents. Recently, the CyberNotarySM project, supported by Scrivener Notaries, Notaries Society, The Union of International Latin Notary and ABA considered the trusted third party as well as the authentification, encryption and the digital signatures in detail.[577]

The legal value o the electronic signature

The electronically written document that comprises the extended electronic signature has the judicial value of a privately signed written document. If the document is acknowledged by the opposing party, (the party with whom the contract has been concluded with), in the event of litigation, the document will be given the status of an authentic judicial document. The legal regulation applicable to the electronic signature is treated under **Law 455/2001** and the **Technical and methodological regulations** regarding its execution.

The exigency in the conclusion of a written legal document, ad validitatem or ad probationem, is satisfied by *the electronic document with an incorporated electronic signature,* based on the acknowledged certificate and generated with a signature creation device.

The lack of acknowledgement of any of the parties of the written document or of the signature will force the court to which the litigation has been submitted to instruct for the verification of the contested facts, by means of the

[575] http://en.wikipedia.org/wiki/Public-key_cryptography

[576] Digital Signature GuidelinesTutorial- American Bar Association Section of Science and Technology Information Security Committee- www.abanet.org/scitech/ec/isc/dsg-tutorial.html

[577] National Conference Of Lawyers & Scientists- www.aaas.org/spp/sfrl/committees/ncls/

specialized technical appraisal. The expert will request the qualified certificates, documents that identify the author of the documents, the signatory or the owner of the certificate.

The party who will call to its defense an extended electronic signature must make proof that the signature:

Is connected only to one sole signatory;

Provides for and is sufficient for the identification of the signatory;

Is created through means controlled solely by the signatory;

Is connected to the electronic data that it relates to, so that any ulterior modification of the former is identifiable.

Technical aspects

The private key is a unique digital code, generated by a hardware and/or special software device, with whose support the electronic signature is created. *The public key* is the pair of the private key, indispensable to the verification of the electronic signature. *The document print* is obtained with the hash-code function. The electronic signature is configured through an algorithm by overlaying the private key and the document print.

How to electronically sign a contract?

The party who initiates the endeavor uses his/her *private key* to sign the contract and sends it, and the addressee of the offer decrypts the transmitted document with the *public key of the addressor*. The acceptance of the sent offer is made if the contract is signed by the addressee with his/her private key and sent to the addressor, who will be informed of the acceptance through the public key of the addressee.[578]

Certification services

Providing electronic certification services consists of issuing a certificate or furnishing ancillary services to the electronic signature. Making such services available to customers is not conditioned by a previous authorization, as it takes place in a free and loyal competitive environment. The future supplier of certification services will inform the Authority for the Regulation and Supervision of the Certification Services Providers (ARSCSP), in writing, of the intention to act as an electronic signature certifier 30 days prior to the inception of such activities. All the information related to the security and certification procedures in use will also be transmitted.

Voluntary accreditation

The certification services suppliers who wish to be accredited suppliers can apply for an accreditation from the ARSCSP. Acquiring the voluntary accreditation implies complying with the conditions required for the issuing of qualified certificates and the use of the secured devices to generate electronic signatures, accredited by an accreditation agency agreed by the authority. The validity of the accreditation is 3 years and can be renewed.

The qualified certificate mentions

That the certificate has been issued as a qualified certificate;

The identification data of the supplier, its citizenship (individuals) or nationality (juridical bodies);

Name of signatory or the pseudonym, as well as other relevant attributes;

The personal identification code of the signatory;

The verification data of the signature;

The exact indication of the validity of the qualified certificate;

The identification code of the qualified certificate;

The extended electronic signature of the supplier that issues the qualified certificate;

The limits to the use of the qualified certificate of the value limits of the operations it can be used for.

Certificate suspendibility:

At the request of the signatory, after checking his/her identity;

At the final court request;

The information in the certificate no longer coincides with the reality.

Certificate cancellation:

At the request of the signatory, after checking his/her identity;

At the death or when an interdiction has come into effect on the signatory;

At the final and irrefutable court request;

The essential information in the certificate no longer coincides with the reality.

The encroachment upon the confidentiality of the signature creation data;

[578] Atreya, Mohan ; Hammond, Benjamin - Digital signatures - McGraw-Hill - New York, 2002

The fraudulent use of the certificate;

Upon the proof that the certificate has been issued based on false or erroneous data.

The obligations of the certificate supplier:

To comply with the declared security and certification procedures;

To provide the access to all the necessary information for the correct and safe use of its services (the steps to take for the creation and the validation of the electronic signature, the prices charged, the ways and concrete conditions to use the certificates, the obligations for the owner of the certificate and for the supplier, the existence of an accreditation, the contractual conditions to issue the certificate, the ways to solve litigation, other information required by the authority);

To keep an electronic register of the issued certificates accessible on-line as well (date and time of the issuing/expiry of the certificate, suspension and cancellation policy mentions, as well as their potential causes);

To keep the secret of the information given in relation with their professional activity and not to disclose it unless the owner of the certificate accepts to have them published to third parties; as per art. 196 Penal Code, lack of compliance with this obligation has penal consequences for the disclosure of a professional secret, unless the information is transmitted to a public authority when the latter acts to perform its public and legal competencies;

Not to collect personal data from other persons than the one who requested the certificate and only in the measure that the information is useful for the issuing and preservation of the certificate; the use of a pseudonym does not allow the supplier to disclose the real identity of the owner, unless agreed so for reasons related to the public interest.

The supplier of qualified certification services should possess the financial means to cover legal damages that may arise in the course of its activity. The insurance is made either through an insurance contract with an agent or through a letter of credit from the specialized financial institution.

Conclusions

Implementing the technologies, as with any new technologies, is a step towards their security. The option to « react » in the information domain is justified by the existing risks to the security.

Law 455/2001 translated the *Directive norm no. 99/93/EC of the European Union Council and the European Parliament* into the Romanian legal system.[579] It is a step forward. May it be fruitful!!

BIBLIOGRAFIE

1. Arias Martha-INTERNET LAW - The EU Law on Electronic Signatures and its Recent Report-www.ibls.com/internet_law_news_portal_view.aspx?id=1920&s=latestnews

2. Atreya, Mohan ; Hammond, Benjamin – "Digital signatures "- McGraw-Hill - New York, 2002

3. Digital Signature GuidelinesTutorial- American Bar Association Section of Science and Technology Information Security Committee- www.abanet.org/scitech/ec/isc/dsg-tutorial.html

4. http://en.wikipedia.org/wiki/Public-key_cryptography

5. Gramada Argentina-"Tehnologia informaţiilor şi comunicării în România si locul ei în lumea "societăţilor informaţionale" a UE"-AnaleleUniv Titu Maiorescu-Ed Titu Maiorescu- 2006

6. Mihai NADIN- "Noua ordine computerizată "
www.comunic.ro/article.php/Noua_ordine_computerizat%C4%83_-_Interviu_cu_Mihai_NADIN/438/

7. Roger.Clarke -Requirements for Message Transmission Security
www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html Privacy Implications of Digital Signatures

8. National Conference Of Lawyers & Scientists- www.aaas.org/spp/sfrl/committees/ncls/

9. www.webopedia.com/TERM/E/encryption.html

10. www.anu.edu.au/people/Roger.Clarke/DV/DigSig.html

[579] Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions- Brussels-
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF