# THE ELECTRONIC SIGNATURE (E-SIGN) IN THE INFORMATION SOCIETY

*Virgil Chichernea*[1]

**Abstract**

This paper deals with the legislative and technical aspects, concerning the electronic signature and examples regarding the implementation of the e-sign software security solutions in the information society. One of the major problems the IT developers for complex systems have to deal with, is to provide the security of data and the information administered by these systems, as well as to certify their authentication by the electronic signature. The certification procedures and the encryption algorithms, used for the electronic signature are needed in today's information society.

*Keywords: e-sign, software security, information security, Decision Support System(DSS).*

## 1. The information security

The objectives of the information security policies are meant to respect the following:

- confidentiality: The access to data must be restricted for those entitled to see the data;
- integrity: the information must be concise and up to the point. All the systems, the assets and networks must be administered properly, according to the instructions;
- availability : the information must be available and also directed to those entitled to receive it, when necessary.

Among the technical methods in order to meet these goals we mention: firewall, users' control access, encryption of the files which circulate through the extranet of the organization, the infrastructure of public keys for the implementation of the electronic signature, e-mail security and e-documents by using e-sign, Web secured applications, by using the SSL security protocols, the security of the Intranet/Extranet networks of the organisations, the encryption of files on the personal computers to ban the access of the unauthorized persons. The security policies are different, according to the situation it faces. In this respect, there were elaborated security policies regarding: the distance users, Extranet, passwords.

The most important indicators of the information security are the following:

- The indicator - the rate of the security breaks within the organisation( BSO);
- The indicator - the index of the damages seriousness (IGP) ;
- The indicator - the on-line security threat (ASO);
- The indicator - the encountered security problems (IP);

[1] Virgil Chichernea, Professor ph.d., Romanian-American-University, Bucharest, email: Chichernea.virgil@profesor.rau.ro

- The indicator - the barriers to the information security (BSI);
- The indicator - the instruments for the information security (ISI);

**2. Electronic signature(E-sign)**

The electronic signature is a unique, personal code, consisting of information in electronic format, generated and stocked on a secured tool, which is attached to the computer, from which the signature is being issued. In the context of providing the security of the internet applications (e-commerce applications, banking transfer, submitting offers for contracts etc.), e-sign represents the base that offers the safety and the confidentiality of transactions, also hindering their fraud. The electronic signature can be used in every field of activity, saving time and money, by sending the informaton electronically, regardless of their nature. The major applications for electronic signature, in Europe are the following:

- personnel e-banking (consumer banking) is used in many countries of the E.U., including Romania;
- e-government applications based on both, simple certification and qualified certification.

The effect made by using the electronic signature is assimilated to the holograph signature and the stamp on an existing document. Each person can use the electronic signature if previously got a certificate issued by The Certification Authority, which legalize the link between the electronic signature and its owner, as a person.

The electronic signature is not a scanned signature, an icon, a photo, a hologram, a smart card, it is a structured row of bytes, generated according to a certain rule, with a probability of regeneration under a certain limit, which makes it being acceptable, concerning the risk. The general requirements for a signature are the following:

- must be genuine, made by the document's author;
- must not be falsified, it must prove the document was not made by the so-called signer;
- must not be reused, must not be replaced, on another document, by a wrongly intended-harmful person;
- must not be altered, once the document is signed, it cannot be modified;
- must not be disowned, meaning the signer is not entitled to not recognize its authentication.

The electronic signature benefits of legality, having the same value as the holograph signature and it meets cumulatively the next conditions:

- it is attached only to the signer;
- it offers the identification of the signer;
- it is created by means controlled exclusively by the signer;
- it is attached to the electronic document to which it refers, so that each modification of the document, after signing, must automatically infirm the signature.

Law no. 455/2001 regarding the electronic signature and the Law no. 589/2004 regarding the juridical regime of the notaries' electronic activity, as well as the norms to enforce

these laws, represent the legal framework existing in Romania at present. The electronic signature is attached to an electronic document, which is edited or made by using the applicable software, as in the following examples:

- MS Word documents (contracts, documents, notifications etc.);
- Spread-sheet Excel (financial reports, salary register, orders etc.);
- pdf documents ( which is superior from the point of view of the security of information integrity );
- expert programs for content /document management;
- documents resulted by processing the fiscal and accounting data( income tax declarations, documents of payment for the state Budget etc.).

**Electronic Signature (E-Sign) In The Information Society**

**1. Technical issues in creating the electronic signature**

The electronic signature is based on a specialized and complex technology, which includes the following components:

**Hash-code** - function that returns the physical footprint of an electronic document;

**Private key** - a unique digital code, generated by a specialized hardware and/or software device. In the context of the digital signature, the private key represents the data required to create the electronic signature, as defined in Law no. 455/2001;

**Public key** - digital code, the pair of the private key needed to verify the electronic signature. In the context of the digital signature, the private key represents the data required to create the electronic signature, as defined in Law no. 455/2001;

**The mechanism of creating the electronic signature**: a hash code function is applied on the document, thus obtaining the document's print. By an algorithm, the private key is applied over the document's print, which operation results into the electronic signature;

**The mechanism of verifying the electronic signature** is based on the use of the public key, hash-code function and the electronic signature received. The verification of the signature is an automatic operation.

**The secured mechanism of creating the electronic signature** is the device required to create the electronic signature, which meets the following conditions:

- The data necessary to create the signature, used to generate it, to appear only once and their confidentiality to be ensured;
- The data necessary to create the signature, used to generate it, to not be deducted;
- The signature to be shared against forgery using technical means available at the moment of its generation;
- The data necessary to create the signature to be effectively protected by the signatory against unauthorized persons;
- To not modify the data in electronic form, which must be signed and to not prevent them from being presented to the signatory before the completion of the signing.
- The minimum length of the private key used by a signatory to create the extended electronic signature must be:
  - 1024 bits for the RSA/DSA algorithm;
  - 160 bits for the DSA algorithm based on elliptic curves

**2. Certification – products and services**

The Regulatory and Supervisory Authority has been established at national level in order to supervise the activity of the Providers of Certification Services (ARSFCS). The said authority endorses the Providers of certification services given the compliance with the requirements necessary to issue qualified certificates and to use secured devices to generate the electronic signature, approved by a regulatory authority agreed by ARSFCS. The certification term is of 3 years and it can be renewed. The main products offered by the Providers of certification services, authorized by ARSFCS, are:

- Qualified certificate – ensures the authenticity and lawful recognition of the documents sent in electronic format; it guarantees the message's reliability; it ensures the safety of transmission by means of encryption.
- Server certificate – allows 128 bits SSL encryption (the most powerful in the world – for Microsoft and Netscape browser versions) and authentication of users based on digital certificates, identification of domain, safety and reliability of SSL transmission to third parties.
- Document management and archive solutions;
- Secure devices to create electronic signatures (DCSC) - they are cryptographic devices allowing the generation, storage and use of the digital certificates of qualified signature. Included accessories: extendible USB cable, CD installation drivers;
- Signing and encryption software – specialized software ensuring the signing and encryption of any type of files and documents in electronic format;
- IPSec?VPN – allows the acquirement and use of digital certificates and IPSec to ensure a scalable, controllable and secured VPN;
- Hosting in secure conditions with qualified certificate:
    - Windows LogOn;
    - Secure e-mail;
    - Data encryption;
    - Solutions for secure transactions, communications and information

Legal and natural persons have to meet the following requirements to receive such certificates:

- To submit information necessary for the desired type of certificate;
- To generate or to purchase a pair – private key/public key. The private key cannot be deducted, under any circumstances, from its pair public key;
- To prove the functionality of the pair – private key/public key.
- To protect the private key from theft, damage, content adjustment or other compromises; it is forbidden to duplicate the private key;
- To suggest a distinct name or pseudonym for identification;
- To submit to the supplier's examination: the application regarding the supply of a certificate; the agreement to comply with the obligations, as client, and its public key;

In order to issue qualified certificates, the providers of certification services must meet a series of requirements imposed by ARSFCS, including the requirement to keep all information concerning a qualified certificate for a period of minimum 10 years from the

date of certificate termination, especially to be able to provide proof of certification in a possible litigation.

**Maintaining qualified certificates implies:**

- To stipulate that the certificate has been released as qualified certificate;
- To mention the identification data of the services' provider, namely the citizenship (natural persons) or nationality (legal entities);
- Name of the signatory or their pseudonym and other relevant information;
- Personal identification number of the signatory;
- Verification dates of the signature;
- Accurate indication of the qualified certificate's validity period;
- Identification code of the qualified certificate;
- Extended electronic signature of the service provider issuing the qualified certificate;
- The limits of the qualified certificate's use or the value limits of the operations for which it can be used.

**The certificates can be suspended as follows:**

- Upon the request of the signatory, after prior verification of their identity;
- As effect of a definitive legal decision;
- The information provided for the certificate is no longer valid.

**The certificates can be terminated under the following circumstances:**

- Upon the request of the signatory, after prior verification of their identity;
- Given the death of the signatory or if the signatory is under legal restrictions;
- As effect of a definitive and final legal decision;
- The information provided for the certificate is no longer valid;
- The confidentiality of the signature's creation data has been infringed;
- Unlawful use of the certificate;
- Evidence that the certificate has been issued based on false or incorrect information;

The providers of qualified certification services must have the financial resources to cover losses that may arise in the exercise of their activity. The insurance is concluded either through underwriting an insurance policy from an insurance company or by a letter of guarantee from a specialized financial institution. The liability for the enforcement of the provisions under Law no. 455/2001 and related regulations is in the charge of ARSFCS.

## 4. Encryption algorithms and electronic signature

Cryptography is the science of secret writing and is used in secure messaging, authentication, services and mechanisms used in electronic networks and Internet. This science is a branch of mathematics that studies mathematical foundations used by cryptographic methods. A cipher is defined as turning a clear message into a coded message or cryptogram. This system, called a cryptosystem or cryptographic system consists of:

- M – clear text (clear message);

- C – ciphered text (ciphered message);
- Two reversed functions denoted by E() (encryption cipher and D() (reversed cipher);
- An algorithm generated the Ke and Kd keys so that:

C = E Ke (M) = E Kd (C)

There are two types of cryptographic systems: symmetric systems and asymmetric systems. Symmetric cryptographic systems (with secret key) use the same key, both for message encryption and decryption. Asymmetric cryptographic systems (with public key) use distinct keys for encryption and decryption (but connected to one another). The most common and studied symmetric cryptographic systems are: DES (Data Encryption Standard) and AES (Advanced Encryption Standard) and the best known cryptography system is RSA (Rivest Shamir Adleman). Cryptanalysis is the art of "breaking" ciphered texts without knowing the key used for the decryption process and those practicing cryptanalysis are called cryptanalysts.

Hash functions play an important role in authenticating the content of a message sent in communications. The objective of these functions is to create a value h = H (M), called the summary (digest), with a role in the digital signature procedure, the value H (M) being very difficult to forge.

Three entities are involved in the digital signature procedure:

- M – initial message (message to be “digested”)
- h – H(M) the digest calculated by the hash function;
- S – Sign (H(M)) digital signature

Hash functions have several common features:

- When M is known, it very simple to calculate h= H(M);
- When h is known, it is impossible to calculate M so that H(M) = h;
- When M is known, it is very difficult to find another M’ (even impossible) so that H(M) = H(M’)
- It is impossible to find two random messages so that H(M) = H(M’) – feature called resistance to collision;

One of the fundamental requirements for such a function is that modifying a single bit on input to produce a series of changes in output bits. Usually one way functions are used, which receive on input a block of message with length m and provide on output compressed message of a shorter length.

**5. Implementation of e-sign software security solutions**

In Romania, e-sign software security solutions have been implemented in the following fields of activity: banking, communication, insurance, government.
Also, internet banking solutions have been implemented for several banks, offering highly appreciated services, out of which we may note:

- MultiCash BCR used to perform banking operations while ensuring the transactions’ safety and confidentiality by means of electronic signatures;

- BRD-NET – ensures the transactions' safety by means of an encryption system, using the 128 bits SSL protocol. The system automatically disconnects the user after 5 minutes of inactivity;

- BT 24, which uses SSL on 128 bits and authenticity certificates used by Microsoft.

- ING OnLine uses the following protection methods: firewall, 128 bits SSL, transaction oriented security services, digital certificates loaded on smartcard.

- The Electronic Payment System, created by TRANSFOND SA, which is used by all credit institutions operating on the inter-banking market in Romania, the Ministry of Finance, the Bucharest Stock Exchange, The National Securities Clearing, Settlement and Securities Deposits, VISA MASTERCARD and the Companies and Financial Investment Services. The electronic payment system has three components namely: gross settlement system in real time, called ReGIS, automated clearing house system, called SENT, registration and settlement system for transactions in government securities, called SAFIR. The advantages of the new electronic payment system are largely operational in nature, including: better risk management and liquidity, payments can be initialized and completed during the same banking day, and in many cases, only within a few hours.

- MEDICOVER Company has implemented for medical laboratory services (Synevo) a system that allows user authentication on the portal based on qualified certificates to secure access to the patients' medical test results. Through this system the patient goes to the doctor, the doctor submits the application for test online after authentication by qualified certificate, the laboratory receives the application online, the patient goes to the laboratory and takes the prescribed tests, then the doctor can see the results of the tests with the help of the authentication process.

- The National Institute of Hydrology has implemented an integrated access control and attendance solution to present information in real-time to the NIH management on the employees' activity and also to improve security within the organization.

**Bibliography**

1. Ion Ivan, Marius Popa – Entitati text – dezvolatre, evaluare, analiza. Editura ASE, Bucuresti, 2005
2. Victor Valeriu Patriciu, Monica Ene_Pietrosanu, Ion Bica, Costel Cristea – Securitatea informatica in UNIX si INTERNET, Editura Tehnica, Bucuresti, 1998.
3. Virgil Chichernea -Sisteme informatice in economie. Strategii de informatizare, Editura Prouniversitaria, 2006
4. http:// ars.mcti.ro
5. http://en.wikipidia.org
6. http://crs.nist.gov/fispubs
7. http://infosec.jmu.edu/ncisse/conference 2000