DOI: 10.53477/2668-6511-22-11

ELECTRONIC SIGNATURE, TOOL FOR OPTIMIZING THE MANAGEMENT OF INFORMATION IN ELECTRONIC FORMAT

Lucian SCÎRTOCEA,
Ph.D. Candidate, National Defense University „Carol I", Bucharest, Romania.
E-mail: lucian.scirtocea@yahoo.com

***Abstract*:** *The development of the IT & C field produces changes in the way of organizing and functioning of all civilian organizations as well as for those in the military field. The way of managing information in electronic format is a concern of specialists in both military and civilian fields in terms of optimizing the process of managing information in electronic format due to the large volume of files and documents currently operated.*

Keywords: *information security; computer and communications system; electronic signature; information management; information in electronic format; informational management.*

Introduction

The electronic signature is a mathematical application used to guarantee the authenticity of an electronic message or document.

In national legislation, the notion of electronic signature is used for an electronic data package that is logically connected with another electronic data package and also as a tool to authenticate and identify a document or message in logical association with the person who signed it (Low no 455/2001 – electronic signature, art. no. 4).

In 1999 the European Directive no. 1999/93 defines the electronic signature in as an authentication *method*" (Directive 1999/93/EC, art. no. 2 (1), 6).

Through The *eIDAS Regulation* (Regulation (EU) No 910/2014), stated in the EU Member States, regarding availability of agreed electronic security means, the *electronic signature* is mutually recognized between them, electronically signed documents having the same trust and validity as those printed on paper and signed manually (handwritten) thru writing instruments. Therefore, the concept of the electronic signature stays similar to that provided in the *Electronic Signature Directive* (Directive 1999/93/EC).

In 2014, the Regulation adopted at the EU level introduces the new concept of *"Qualified electronic signature*", which would represent a, high-*performance electronic signature created by an electronic signature generator authorized by a certificate specific to an electronic signature*" (Regulation (EU) No 910/2014, art. 3, 84).

The advanced electronic signature must be qualified in the following *criteria* (Regulation (EU) No 910/2014, art. no. 36, 104):

- to be linked to the signatory;
- to be able to identify the signatory;
- the user of the electronic signature (the signatory) has to have at hand the necessary tools to create the electronic signature with a high level of trust, under his sole control;
- any subsequent modification of the electronic signature data is detectable.

Having regard to the specialized legislation, the European Union Regulation states that a qualified electronic signature has the legal effect equivalent to a *handwritten signed signature*

(Regulation (EU) No 910/2014, art. no. 25, 100) and that a qualified electronic signature based on a qualified certificate issued in one of the State Member will be recognized in all other States Member.

According to the same regulation, advanced electronic signatures are qualified as ,,*trust services*"[1].

The legal framework of these electronic signatures is not stipulated by the eIDAS Regulation adopted at the European Union level but will be included in the national legislation.

1. Conceptual delimitations

Digital electronic signatures use internationally authorized cryptographic algorithms and are widely used in online operations (organizational management, banking, online payment services, etc.) as well as in other situations to protect the authenticity and integrity of data.

Another term used in this specific field is that of the digital signature which is often used as a larger field of application of electronic signatures and which refers to any electronic data bearing the intention to sign. It should be noted here that not all electronic signatures are digital signatures.

There are specific legislative packages on electronic signatures adopted at the level of several economically developed countries through which electronic signatures have legal significance and where it is demonstrated that the computerization of a state is closely correlated with economic and social growth by ensuring data security in that state.

Electronic (digital) signatures were used as the electronic equivalent of holographic signatures and introduced into public key encryption systems by Diffie and Hellman in 1976 (Diffie, Hellman, 1976), in the absence of a cryptographic scheme for this purpose.

Digital signatures are based on *asymmetric cryptography* (IBM, documentation cryptography, n.d.). The digital signature combines data authentication with the authentication entity. They provide an additional confidence in ensuring the security of messages transmitted through an insecure communication channel. Properly implemented, a digital signature gives the certainty that the message has been sent by the legal, original sender.

Digital signatures are legally equivalent to handwritten signatures, stamps and seals with the mention that a handwritten signature can be reproduced on a certain document by certain interested persons while electronic (digital) signatures, which are based on a cryptographic algorithm and bind an electronic identity to an electronic document cannot be copied on another document. Verifying with certainty the authenticity of the digital signature is very easy and no specialized staff is needed to do this.

The use of the electronic signature ensures the following functions regarding the security of information transmitted through IT & C, as follows:

– *authentication*; digital signatures can be used to guarantee the authenticity of the messages sender. When the ownership of the secret key of the digital signature is assigned to a certain user, a digital signature shows that the message was sent by that sender and not another;

– *integrity*; It is necessary for the sender and the recipient to trust that the messages sent / received have not been changed. If a message is digitally signed, any change to the message cancels its signature;

[1] Trust Services' are a concept defined in Regulation 910/2014 to include electronic services, consisting of the creation, verification, validation and preservation of e-Signatures, e-Seals or time stamps, e- registered delivery services and certificates for website authentication. This concept goes beyond that of 'certification services' under the E-signature Directive (Directive 1999/93/EC) as it encompasses delegated and cloud-based signature services. A Trust Service Provider (TSP) will now be able to manage an electronic signature remotely on the signatory's behalf, if its procedures ensure that the signatory remains in sole control.

– *non-repudiation* ensures that a person or organization, regardless of the activity profile, cannot deny the issue of a document/information once signed.

2. Requirements and characteristics of electronic signatures

Requirements:

– it must be easy to implement only by the person signing the message;
– it must be easy to check by correspondents;
– it must have an appropriate validity; the signature cannot be forged until it is no longer necessary for the purpose for which it was created.

Features:

– does not represent a scanned signature, an icon or a picture.
– ensures the authentication of digital messages;
– eliminates the work with papers and their related costs;
– optimizes the necessary resources in managing documents in printed format;
– protection of communications within both military and civilian organizations.

3. Classification of digital electronic signatures

There are two distinct categories of digital signatures:

– *digital signatures with message retrieval;*
– *digital signatures with annex.*

By using digital signatures from the first category, the message can be retrieved directly from the digital signature. The simplest example of construction is by reversing the role of the public and private key in the case of the RSA scheme.

Digital signing of documents is done either by using *asymmetric cryptography*, but there are also constructions that use only *hash cryptographic functions* (ENISA, 2013).

Attached digital electronic signatures are those from which the message cannot be retrieved but is additionally sent as an attachment to the digital signature. These can be easily built by applying a hash function to the message and encrypting the obtained hash.

Due to the efficiency in signing large messages, these signatures are the most used in practice. At the same time, any digital signature with message retrieval can be easily converted into an attachment signature.

A hash function takes a group of characters (called a key) and maps it to a value of a certain length (called a hash value or hash) (Google 2021, hash function, March 26, 2018).

The *160 - bit SHA-1* function, which resembles the MD5 algorithm, was designed by the National Security Agency (NSA) to be part of the DSA[2] (Digital Signature Algorithm). Along the way, however, cryptographic weaknesses of SHA-1 were discovered, and the standard was not approved for most cryptographic uses after 2010.

The hash functions are used as a file identifier, to check passwords, files or messages integrity, to perform certain specific protocols, and so on.

[2] DSA (Digital Signature Algorithm) – The digital signature algorithm is a standard of the United States government for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use under the Digital Signature Standard (DSS), specified in FIPS 186 and adopted in 1993. A minor revision was issued in 1996 under the name FIPS 186 -1 [1]. The standard was extended in 2000 as FIPS 186-2 [2] and in 2009 as FIPS 186-3 [3].

One of the main applications of a common hash function is to allow searching fast data in the *scatter tables*[3].

Digital signatures can also be classified according to the signing algorithm used (one-time algorithms or multiple-time algorithms).

Another classification of electronic signatures is based on the level of trust as follows: low level used for low risk documents, advanced level used for medium risk documents, and qualified electronic signature which is an advanced electronic signature based on a qualified digital certificate and provides the highest level of trust in accordance with the European Regulation eIDAS 910/2014 (Regulation EU 910/2014), recognized in all States Members and created by a professional, competent and qualified provider of reliable IT security services.

4. Digital certificate

The digital electronic signature is provided by a *digital certificate*.

In cryptography, a digital certificate, also known as a *public key certificate*, is an electronic document used to prove ownership of a public key.

According to the *legislation* (Decision no. 1259, 2001) in force, a Qualified Digital Certificate is nominal and identifies a natural person acting either in his own name or as a representative of a third party, legal person.

Qualified digital certificate (Law no. 455/2001, art. no. 18, 7): represents the proof that the certificate has been issued as a qualified certificate including the identification data of the certification service provider, the name of the signatory, the personal identification code of the signatory, the verification data of the electronic signature, the validity period of the qualified certificate, the identification code of the certificate, the electronic signature of the certification service provider, any other information established by the regulatory and supervisory authority specialized in the field.

Similar to the concept of identity card, where the obligation to issue such documents belongs to a single authority at national level, based on documents submitted by the applicant, a digital certificate is issued by certain organizations called *certification authorities*. Such an authority, in order to be accredited, must meet strict requirements and criteria in accordance with national law, so that a digital certificate issued by that authority represents a high degree of trust.

Digital certificates are generally *used for*:

– authentication and encryption of information between servers and web browsers;

– authentication and encryption of connections in a local network - LAN;

– authentication and encryption of messages sent by email within a local network or between third parties;

– authentication and encryption of connections between servers.

Digital certificates can be of several *types*:

– *certificates for internal use* – are used in local networks belonging to military or civilian organizations and cannot be used in relations with third parties because they are not issued by accredited certification authorities;

– *certificates with domain authentication* – when issuing such a certificate, the certification authority verifies only the fact that the person who submitted the issuance request owns the respective domain;

[3] *A scatter table or hash table* is a data structure that implements the interface of an associative array, namely: it allows storing pairs (key, value) and performing three operations: adding a new pair, searching and deleting the pair after the known key.

– *fully authenticated certificates* – are granted by a certification authority only after thorough checks on the organization and the domain holder;

– *certificates for signing software applications* – are used by software companies to digitally sign software codes to prevent their compromise with malware applications when downloaded from the Internet;

– *certificates with extended validation* – represent digital certificates with the highest possible level of trust.

In the mail-specific encryption (use of email services) the holder of a certificate is usually a person or organization. However, in *Transport Layer Security/TLS*[4], although the subject of the certificate is usually a computer or other electronic device, TLS certificates can identify organizations or individuals in addition to their primary role in identifying electronic devices.

5. The role of electronic signature in optimizing information management in electronic format

The information management in electronic format within organizations, including those with military specifics, is the future way of managing them. The process of migrating information from paper to electronic format is the key to optimizing the activities carried out within organizations. An important role in the implementation of these IT&C infrastructures necessary for the information management in electronic format has the electronic signature through its following characteristics:

– the electronic signature ensures advanced security in the process of authentication of documents managed in electronic format;

– the electronic signature and certificates that are issued for the authentication of electronically managed documents are recognized at European and national level;

– the electronic signature service can be used in any Microsoft Office application;

– civilian organizations and military structures choose to use the electronic signature for security and efficiency reasons, its implementation brought savings in their budgets;

– reduction of costs related to the printing of documents, the equipment necessary for the process of printing them as well as those related to the physical management of these documents (transport, logistics, security of these documents, etc.);

– ensuring the confidentiality of electronically managed data; the electronic signature guarantees the confidentiality of the transmitted data. Digital documents cannot be opened by unauthorized persons;

– the role of electronic signatures is to increase the security and trust of the activities carried out in an organization with a certain specificity, demonstrating that the messages transmitted through electronic files are unchanged;

– electronically signed documents with a qualified electronic signature are impossible to falsify. When a document is certified with an electronic signature, it is known with certainty who the signatory is;

– the electronic signature can be used for issuing the various documents necessary for carrying out specific activities in Romania as well as in the EU;

[4] A.N.: Transport Layer Security (TLS) and Secure Sockets Layer (SSL), its predecessor, are cryptographic protocols that allow secure communications over the Internet. The term "SSL" used here refers to both protocols, except in cases explicitly specified in the context. Using SSL technology provides a greater degree of privacy and security than an encrypted web connection. This reduces the risk of information being intercepted.

– in the event of litigation, the validity of electronically protected documents is easy to prove. According to the legislation governing the field of digital signatures, the legality of these documents cannot be challenged;

– employment contracts concluded at the level of both civilian and military organizations can be signed with the help of electronic signatures, thus increasing the speed of approval and entry into force of these categories of documents provided for in labor legislation;

– unlike documents managed in printed format, electronically signed documents can be printed, but the printed paper has no legal value. Thus, electronically signed documents are also managed in electronic form.

6. Limitations on the use of electronic signature

From the aspects presented above, the use of electronic signature has many advantages, but its implementation within organizations has a number of disadvantages (limitations and costs), as follows:

– the occurrence of initial costs regarding the provision of equipment used in the process of implementing electronic signatures (means of authentication such as tokens, PCs, computer networks);

– the existence of specialized staff involved in the management of these categories of equipment used in the authentication process as well as the implementation of this system, which involves additional staff remuneration costs;

– in the absence of such specialized personnel, capable of implementing and managing such infrastructure, these services must be outsourced to private companies with this specific, which involves additional costs for the operation of organizations as well as military-specific structures;

– possible security vulnerabilities in the security policy of the military structures within the Romanian Army in the situation when this specific infrastructure is outsourced to companies that have not been carefully selected and/or verified.

Conclusions

The electronic signature is a useful tool for any person or organization, including the military, in order to streamline and optimize the activities carried out, related to the way of managing files in electronic format because the electronic signature provides legal tools for authenticating documents and guarantees the confidentiality of protected data.

I consider that the existence of some infrastructures (specialized personnel and specific technique) in the Romanian Army, for managing this field, is useful and will determine the increase of the decision making speed for fulfilling the specific missions.

The training of personnel with responsibilities in this field is essential in the new global context in which information is transmitted in electronic format within the specific networks used at the level of military structures in conditions of security and with maximum operability.

The way of transmitting information in printed format with handwritten signatures and stamps, transported by mail or couriers between military units of different echelons has run its course and these activities will have to be replaced by information and communication infrastructures, ensured from a security point of view, which will manage documents in electronic format, authenticated through the cryptographic infrastructure specific to electronic signatures.

BIBLIOGRAPHY:

Decision no. 1259 of December 13. 2001. Regarding the approval of the Technical and Methodological Norms for the application of Law no. 455/2001 regarding the electronic signature.

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

ENISA. September 20th, 2013. Recommended cryptographic measures, Securing personal data,

Google. 2021. Hash function, March 26, 2018, URL: https://www.techopedia.com/definition/19744/hash-function, accessed in November 2021.

IBM, n.d, documentation cryptography, https://www.ibm.com/docs/ro/i/7.1?topic=concepts-cryptography

Law no. 135/2007 on archiving documents in electronic form.

Law no. 455/2001 regarding the electronic signature of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

European Parliament and the Council. 2014. Regulation (EU) No 910/2014 of the European Parliament and of the Council.

WHITFIELD, Diffie; HELLMAN, Martin E. 1976. "New Directions in Cryptography", IEEE, Transactions on information theory, Vol. IT-22, No. URL: https://ee.stanford.edu/~hellman/publications/24.pdf