METHODOLOGY OF RISK ASSESSMENT OF FORENSIC TECHNICAL EXPERTISE IN RECOGNIZING THE AUTHENTICITY OF AN ELECTRONIC DIGITAL SIGNATURE

Pavel Menshikov, Alex Tsirdava
•
Peter the Great St. Petersburg Polytechnic University, Russia
Vitta.spb@mail.ru
alex.tsirdava@yandex.ru

Abstract

The article discusses the issues of using an electronic digital signature as enhanced authentication of the signature owner, as well as preserving the integrity of the document content. Particular attention is paid to the issues of differences in the types of electronic signatures (ES). ES has long been part of the usual electronic document flow, it is used in the banking sector, in the field of entrepreneurial and commercial activities, as well as economic, thereby it has become a new way of data theft, which in turn has led to the development of new types of crimes. The article presents various methods of ES research that help to establish the fact of changes in a document by studying its hash functions. As a consequence, the article concludes that it is necessary to develop the expertise of an ES.

Keywords: electronic signature, electronic document management, hash function, cryptographic algorithm

I. Introduction

The legislator equalized the legal force of paper and electronic documents by approving and consolidating these provisions in the Federal Law "On Electronic Signature" [1]. An electronic document that is certified by an EP is absolutely equivalent and equivalent in the legal field to a paper carrier with the signature of a certain person and (or) the seal of the organization. Identification of the authenticity of a signature on paper has long been known and studied in the world of expert research, but the world of electronic documents has not yet been fully studied.

II. Methods

The signature examination is carried out using such a modern method as the study of the hash function, as well as using the method of studying the authenticity of the EP certificate. In order to check the documentation or confirm its compliance with the data, the EP expert first sends a request to the registry of the enterprise that provided this service to the owner of the document.

The hash function method is resorted to only if there are suspicions that corrections were made to the document during forwarding. Hash functions are a mathematical tool, the essence of which is to transform an information block according to an established system that creates strings of bits of various lengths. This process, in fact, is called hashing.

This technology allowed representatives of the criminal world to make transactions on behalf of third parties for the disposal of property without the consent of the owner, including:

-alienate the owner's property;

-to make profit on behalf of other persons in credit institutions;

-to change the owner of the organization illegally.

Specialists from the USA in 1983 submitted patent No. 4405829, which described the mechanism of the formation of the EP. The basis of this patent was a secret key, which consisted of three simple multi-digit binary numbers p, q and d, clothed in the form of three-bit strings, thereby simplifying the system of forming an EP [2].

III. Results

The formation of the public key was based on a pair of multi-bit binary numbers n and E. n was the product of p and q, and e was a separate multi-bit binary number given by the condition that ed=1mod(p-1) (q-1). In this form, an electronic document, depending on the value of H, that is, on the value of bit strings in the form of multi-bit binary numbers, forms the value of the secret key of the EP as the formula Q =s=Hdmodn. The next step is to check multi-bit binary numbers. The first verification multi-digit binary number is set by the parameter A=N. The second verification number B comes from manipulations with this number, for this they set the condition for which B is equal to a multi-digit binary number s, raised to the power of e modulo n: B =semodn. The last stage of the formation of the EP is the verification of the formed multi-digit binary numbers A and B; if the parameters of the compared MDCs A and B coincide, they conclude that the EP is authentic."

Thus, thanks to the automation of the process, it is possible in a matter of seconds not only to form an EP, but also to check the coincidence of the public and private keys by calculations based on the formula. There are still many different approaches to the formation of the EP, but the algorithm has not been changed and the principle of its operation is similar.

IV. Discussion

An EP is a complete analogue of an ordinary signature on paper, expressed using a public and private key based on hashing technologies, but it is embodied not in the form of a graphic image, but with the help of information and mathematical transformations over the content of the document. The main document that regulates the operation of the EP in the Russian Federation is GOST 34.10-2001. It is this document that defines all the processes that make up the introduction of EDS into electronic document management, including: key generation, the formation of the signature itself and its verification. Due to the formation and verification of the EP, three tasks are solved at once: preserving the integrity of the content of the electronic document, the authenticity of the information contained in the document, as well as confirming the authorship of the owner of the EP.

The EP provides an opportunity to determine the owner of the rutoken by converting information from the private and public EP key, thereby the EP is the main certifying requisites of the key owner. After the entry of Federal Law No. 63 "On Electronic Signature", the scope of conducting an electronic document of turnover and business activity was significantly simplified, but together with this, the EP became a modern tool for committing a crime.

To ensure the reliability of the EP, a verification key is used, which is a binary code decryptor. "Certifying centers (CC), namely, the authorized body that registers the EP is called, exercises control in this area. The EP is based on the identification of a person using a special key, which is presented in the form of a paper or digital document, this kind of data just warns the UC."[3]

Cryptographic tools are the foundation on which the EP tools are based, they are generated using a unique set of data created using a special random number sensor algorithm. This data set is formed by sequential calculations of the cursor movement or the applicant's movements on the touchpad. These tools can be installed on the computer of the owner of the signature in the form of software (software) or a special flash drive (rutoken).

The current Federal Law "On Electronic Signature" divides the EP into simple and enhanced. To confirm the owner of the signature, a simple EP requests the necessary passwords or access codes. A more complex access system is provided by Federal Law for enhanced EP, the law identifies strict requirements for qualified and unqualified enhanced EP.

So, to use a qualified EP, it is necessary to have a certificate of the verification key.[4] In turn, for an unqualified EP, it is sufficient to use any other authentication keys.[5] An unqualified EP is formed by converting information from the key of the EP, with the help of this type of EP it is possible to determine the person who signed the document, as well as the fact of changing the document.[6] Taking into account the statistics of forensic investigative practice, it can be concluded that access to the EP has become one of the key tools of personal data theft.

At the output, experts receive a hash document, which is an encrypted summary of detailed information about the document under study on which the EP was applied. Then, with the help of a computer program, decryption and subsequent reconciliation of hash function indicators are performed. Any deviation from the original encryption code can tell experts about the violation of the integrity of the documentation.

The EP examination turned the idea of computer-technical research objects upside down, becoming a unique kind, since during the general computerization, the identification of various economic entities also switched to digital format, therefore this area requires considerable attention and research. Nowadays, most organizations have begun to use electronic document management everywhere, which has significantly increased the speed of interaction between organizations, thereby leading to increased cases of criminal attempts in this area, which makes the examination of the EP one of the most relevant studies.

Nowadays, the issue of a new technological exchange of information is becoming more acute, and to protect such information, it is necessary to develop two aspects: methods of computer data research and qualified personnel training.

References

[1] Ivanov M.A., Rostovtsev A.G., Makhovenko E.B. Introduction to public key cryptography. St. Petersburg, Mir i Semya, 2001.

[2] Kapustina A.G. "Federal law on electronic signature - what's new?" // Information protection INSIDE – 2011 - No. 3 -pp. 20-22.

[3] Fanina M.N. "Computer-technical expertise in electronic transactions."// International Journal of Humanities and Natural Sciences. – 2020. - No. 12-2 (51) – pp. 100-102.

[4] Shestakova E.V. "Digital law." // Right of Access - 2020.

[5] Shestakova E.V. "Policy and regulation of personal data processing." // Right of Access - 2017.

[6] Khairusov D.S. /Comparative legal analysis of the use of electronic signatures in the documents of the UIS units under the new law// Actual problems of the activity of the UIS units: collection of materials of the All-Russian Scientific and Practical Conference, Voronezh, 2011.

[7] Bondarenko Yu.A. "Features of the investigation of fraud committed using an electronic signature." // Humanities, socio-economic and social sciences. – 2020. – No. 3 - pp. 60-63.