

The method of identity verification when signing electronic documents based on biometric means of identification

V Pysarenko¹, L Dorohan-Pysarenko¹, N Kantsedal¹

¹Poltava State Agrarian Academy (PSAA), Poltava, Ukraine

vyacheslav.pusarenko@pdaa.edu.ua,

Abstract. The development of global communications in business and everyday life has led to the emergence of a new plane of relationship, the subject of which is the electronic data exchange. In this exchange of data involved bodies of state power, local self-government, public administration, commercial and non-profit organizations, as well as citizens in their official and personal relationships. The problem of protecting electronic documents with the help of electronic-digital signature is extremely widespread in our time. As the era of the Internet and electronic technologies has come to an end, problems with the security of electronic document circulation, including those in public administration, are beginning to emerge. The issue of the preservation of electronic documents from copying and forging requires for its solution specific means and methods of protection. One of the means of such protection is a biometric digital signature, which undoubtedly confirms the authenticity of the information in the document, its details and the fact of signature by a particular person. The technology of electronic document circulation with the use of biometric digital signature in the public administration is not implemented today, which significantly reduces its quality and the development of electronic document circulation in general. The development is devoted to the possibilities of use and benefits of the introduction of electronic document circulation using the method of identity verification when signing electronic documents based on biometric identification tools.

1. Introduction

The essence of the problem and its solution. The purpose of this article is to solve the issues of organization of electronic document circulation in the authorities using the method of identity verification when signing electronic documents on the basis of biometric means of identification, namely, the biometric digital signature, the advantages of practical use of such a type of digital signature, and proposals for legislative and regulatory acts that determine the organizational principles for using a biometric digital signature in Ukraine.

Despite the existence in Ukraine of a certain legal and regulatory framework for electronic document management, there are many unresolved issues in improving the organization of electronic document management in government. Improvement and updating of the legal framework of Ukraine, creation of special legal norms will facilitate effective implementation and functioning of electronic document circulation.

Comprehensive use of electronic digital signature, namely biometric, will enable not only to simplify and speed up the circulation of documents between business entities, but also to create conditions for the development of export-import operations, e-commerce, electronic banking services, full-scale distance learning and provision of medical services from application of the latest information

technologies. In addition, the introduction of a biometric digital signature will establish an organizational and technical basis for the provision of electronic information services by public authorities, local governments, public administration, legal and physical entities with the use of the Internet. The reliable functioning of electronic document circulation will be a guarantee of Ukraine's information security.

This paper demonstrates the practical feasibility of organizing electronic document circulation in government using the method of identity verification when signing electronic documents on the basis of biometric of identification means - a biometric digital signature.

2. Review of literature

The management activity that is generally carried out and reproduced through and through the management of government records in government agencies is a dynamically functioning link in the process of ensuring interconnection and interoperability and the interconnection between the management and the managed systems.

The activation of the efforts of Western scholars at one time to develop scientific aspects of document management and coordination of scientists from different countries made it possible to recognize document management as a general management function, however, there was no complete agreement on understanding the management of documentation as a scientific category.

There was an understanding of the concept of managing documentation and information in their inextricable link, based on the combination of information technology capabilities and the benefits of traditional documentation.

In the scientific literature, the problematic aspects of the introduction of electronic document management systems are insufficient, which is due to the lack in Ukraine of the approved legislative framework for electronic documents functioning until 2004 in Ukraine. In the works of scientists, mainly only theoretical foundations of automated documentation are considered [1, 2, 3]. The adoption in 2003 of the laws of Ukraine "On electronic documents and electronic document circulation" [4] and "On electronic digital signature" [5] facilitated the introduction of integrated electronic document management systems. However, the theoretical and practical aspects of the implementation of such implementation need further development.

In order to regulate legal relations in the field of information technologies, the Verkhovna Rada of Ukraine adopted several Laws of Ukraine, which entered into force: "On mandatory copy of documents", which defines the legal principles of functioning of the system of mandatory copy of documents and regulates information relations related to replenishment national information fund of Ukraine [6]; "On the National Program of Informatization", which defines the general principles for the formation, implementation and adjustment of the National Informatization Program [7]; "On Telecommunications", which establishes the legal basis for activities in the field of telecommunications and defines the powers of the state regarding the management and regulation of the said activities, as well as the rights, responsibilities and principles of liability of individuals and legal entities involved in the activity or use telecommunication services [8]; "On the National System of Confidential Communication", which regulates social relations related to the creation, operation, development and use of the National Confidential Communication System [9]; "On Information Protection in Information and Telecommunication Systems", which regulates relations in the field of information security in information, telecommunication and information-telecommunication systems [10].

The Law of Ukraine "On the Uniform State Demographic Registry and Documents Affirming the Citizenship of Ukraine, Definition of a Person or Its Special Status," which defines the legal and organizational foundations for the establishment and functioning of the Uniform State Population Register and the issuance of identity documents, confirm the citizenship of Ukraine or a special the status of the person, as well as the rights and obligations of the persons to whom such documents have been issued [11].

Only in December 2017 the Cabinet of Ministers of Ukraine approved the resolution "On Approval of the Regulation on the National System of Biometric Verification and Identification of Citizens of

Ukraine, Foreigners and Stateless Persons" [12], which regulates the implementation and functioning of the national system of biometric verification and identification of citizens of Ukraine, foreigners and stateless persons, as well as defines its structure and purpose. The document states that this is an automated system created for the sake of national security, economic prosperity and human rights, which ensures the establishment of a person of a foreigner and stateless person who enter Ukraine, depart from Ukraine, exercise control over their observance of the rules of stay in the territory of our state.

The terms used in this Regulation are defined and have the following meanings:

- biometric data (parameters) - digitized fingerprints, digitized face image;
- data center - fault-tolerant integrated centralized system (software and hardware complex);
- workstation - a complex of hardware and software;
- fixing of biometric data (parameters) of a person - the process of collecting biometric data (parameters) of a citizen of Ukraine, a foreigner and stateless person (hereinafter - a person), making and storing in the departmental information systems of subjects of the national system;
- biometric identification - "one to many" search by recognizing and comparing one or two biometric data (parameters) of a person with biometric data (parameters) of persons in departmental information systems of subjects of the national system;
- biometric verification - search by principle.

3. The purpose and objectives of the study

The purpose of our study is to develop organizational measures for the implementation of electronic document circulation in public administration using a fundamentally new method of identity verification when signing electronic documents based on biometric identification tools. This issue will require further research by scientists from different countries, as existing legislation does not streamline the issue of electronic document circulation using biometric digital signatures.

4. Finding the best solutions for the implementation of electronic document and document management in public administration using a biometric digital signature

In the world, standards are becoming increasingly important. The main reason for this is the changes related to the globalization of the world financial market, the erosion of borders along the way of the movement of capital, goods, ideas and information. Scientific and technological progress, the rapid development of information technology and their active implementation - all this contributed to the process of development and implementation of international standards in all areas of human activity, in particular. in the management of documentation [17].

The use of electronic documents has been used in many areas of public administration, local government and public administration. The use of electronic document management systems can achieve enormous economic benefits, but the introduction of electronic document management systems can not be forgotten about security. One of the most important requirements for any electronic document management system is to ensure the security of electronic exchange of documents. Currently, systems of secure electronic document circulation are becoming increasingly popular. This is due to an increase in the number of confidential documents in public authorities, local self-government, other organizations of different forms of ownership and an active transition to electronic circulation of documents.

The legal protection of databases in the countries of the European Union is based on Directive 96/9 / EC dated March 11, 1996, which has received direct effect in the territory of the member states of the EU from 01.01.1998 [18]. In the European Union, databases are protected by a special legal institution - sui generis, that is, special protection if qualitative or quantitative investments are made in their selection, certification or submission.

The essence of special protection is that nobody can do:

- the transfer of a database or significant parts thereof to any other means of communication or the production of a copy (copy) in any form and at any time (paragraph A of paragraph 2 of Article 7 of the Directive);

- communication of the database to the public in any way or to enable the database to be used by various means (paragraph B, paragraph 2, Article 7 of the Directive);
- multiple systematic extraction or reuse of non-essential parts of the database and which compromise the intelligent interests of the compiler due to unforeseen use of the database, for example, with the help of the program (Clause 5, Clause 2 of Article 7 of the Directive).

In Ukraine, which is preparing for joining the EU, there is a need for regulatory documents regarding electronic document circulation and electronic digital signature, to bring the requirements of the European Union. However, the use and development of Ukrainian scientists is possible to ensure EU requirements. A new scheme of organization of electronic document circulation in the authorities is proposed using the method of identity verification when signing electronic documents based on biometric means of identification - a biometric digital signature.

5. Strategy for the development of organizational measures for the implementation of electronic document management in public administration with the use of a fundamentally new method of identity verification when signing electronic documents based on biometric means of identification

For the organization of electronic documentation in public authorities, local self-government using the method of identity verification when signing electronic documents based on biometric means of identification, it is necessary to prepare and issue joint orders of the chairman of the regional state administration and the regional council and, respectively, district state administrations and district councils for implementation in work institutions of electronic document circulation, using the method of identity verification when signing an e-mail Throne documents based on biometric identifiers, where:

- to indicate the specialists who will be obliged to include on the outgoing electronic documents, biometric data of the persons who signed the paper version of this electronic document and conduct identification of the biometric data of the persons who signed the incoming document (hereinafter the specialist);
- define one e-mail address in each institution from which the original electronic information will be sent and on which electronic documents will be received;
- oblige the relevant units to equip the automated workplace (APM) specialist with appropriate equipment and software.

5.1 Preparation for implementation

Provide an automated workplace for a specialist in the documentation department - a personal computer that needs to be password protected, a fingerprint scanner, such as ZK 6000-USB, connect the Internet and the e-mail of a Ukrainian provider.

Prepare a list of government officials with electronic addresses to which electronic documents will be sent, and their phone numbers for the contact.

Identify a list of positions and prepare lists of government officials who have the right to sign documents.

Install a fingerprint identification software on a personal computer, such as an automated dactyloscopic identification system, for example, "DACTO-2000".

Move the cursor over the scanner icon to the personal computer monitor and click on the left mouse button and prepare the scanner for work.

5.2 Creating a fingerprint database

Start preparing for the creation of a fingerprint database by filling out a fingerprint card specialist (hereinafter referred to as dactyloscopic card) on persons in the list, namely:

- registration number (identification number, card number);
- surnames;
- name;
- surname;
- positions;

- place of work;
- citizenship;
- date of birth;
- place of birth;
- information about registration at the place of residence.

The index finger of the left and then the right hand of the responsible person alternately placed on the scanner window. The reader scans your finger quickly and automatically. The fingerprint image is encoded before transferring to a computer via a usb port. For example, the ZK 6000 uses an optical fingerprint sensor for high quality and reliability. The fingerprint recognition algorithm has an unmatched ability to identify even the hardest fingers. The data stream received from the sensor is subjected to software processing to restore the fingerprint image and extract it from the necessary for further comparison with the information template. The restored image typically has a size of 25x14 mm, which is equivalent to the number of pixels of 500x280. The imprints of the index finger of the left and right hands are made in order to be able to use one of them in the case when the responsible person confuses his hands, or illness or other reasons will not allow the use of imprints from one hand.

The database will be completed when the dactyloscard is completed on all officials listed.

In order to ensure secrecy and due to the limited amount of memory, it is not desirable to store full fingerprints in the fingerprint recognition system. Of course, they can be stored in a safe place as a backup to access them in special cases, but for normal operation of this system, full-size image fingerprints are not required. In normal operation of the system from the image is extracted a unique set of data on the imprint. The extraction is performed using the pattern recognition process or using the principle of details (minutiae).

Authorities exchange their databases, creating in each institution a complete, common database, which is replenished with changes in staffing and the recruitment of new employees.

The database is stored on the server of the institution with the right of access only by the appropriate specialist.

5.3 Preparation and sending of outgoing electronic documents

An electronic document is prepared, the paper version of which is submitted and signed by the corresponding person in person.

In the absence of the head and signature on a paper document or the person who substitutes it, the paper document indicates his position and surname, and the electronic document supplements his electronic image of the papery patterns of fingers.

The signed paper document, together with the electronic document, is forwarded to the specialist for registration and dispatch.

The expert, having removed from the datacard of databases, the scanned fingerprint of the official who signed the paper document imposes it on the electronic document in the place where the signature is usually held and preserves it.

The electronic document is sent to the addressee by e-mail.

A paper document is stored in the institution in accordance with the requirements of normative documents regarding the terms of the storage of documents, and the electronic document is transferred to the electronic file of the control card of the document.

5.4 Procedure for processing received incoming electronic documents

Before sending an e-mail to the specialist e-mail address specified by the institution, an electronic document is copied to the file, and the specialist, using the automated fingerprint identification system, for example "DAKTO-2000", carries out the identification of the electronic image of the papillary fingerprints on the incoming electronic document with the database in order to identify the person who signed it.

If the print corresponds to the post and the name of the official who signed the document, it is printed on paper and handed over to the management for familiarization. Further work with a paper document

and its electronic copy shall be carried out in accordance with the regulations and the document and control system in force in the institution.

In the event that the imprint does not correspond to the position or name of the official who signed the document, the electronic document is postponed to the "Unidentified" folder for detailed examination by the head of the documentation department and the identification of the reasons (failure of the system of identification or unreliability of the information).

Introduction of electronic document circulation using the method of identity verification when signing electronic documents based on biometric means of identification in comparison with electronic document circulation using electronic digital signature have significant advantages.

6. Conclusion

In the above studies, an analysis of the conditions and constraints that provide the necessary quality of electronic document circulation in public administration using the method of identity verification when signing electronic documents based on biometric means of identification, namely, a biometric digital signature, is carried out.

As can be seen from the foregoing, the method of identity verification when signing electronic documents based on biometric means of identification:

- more efficient due to high reliability at use and low level of error;
- does not require the creation of a serious infrastructure for the proper functioning of the digital signature, the creation and approval of standards that ensure the compatibility of the keys to digital signature and digital signature, and standards that provide a specified level of stability of the digital signature keys and digital signature;
- easy to use in the absence of open and closed keys and the need for special software for generating electronic digital signature keys provided by the key certification center;
- Convenience - there is no need for each of the subscribers to conclude an agreement on the provision of electronic digital signature services in the form of an agreement on subscription with the center of certification of keys, and to provide directly to the CSC personally the documents confirming the information included in the key certificate and access to the special resource of the key certification center each time receipt of a signed and encrypted document in order to verify the validity of the certificate of the subscriber who signed it;
- cost-effectiveness - affordable software and fingerprint identification devices, no need to create and maintain a network of key certification centers.

Consequently, the approval of the regulatory framework for electronic document circulation is a positive precondition for the use of primary media in electronic form. However, for the widespread introduction of these systems, further improvement of the normative and methodological base is required in accordance with the proposed recommendations.

Comprehensive use of electronic digital signature will enable not only to simplify and speed up the flow of business between business entities and to strengthen the competitiveness of domestic enterprises, but also to create conditions for the development of export-import operations, e-commerce, electronic banking services, full-scale distance learning and provision of medical services from application of the latest information technologies. In addition, the introduction of an electronic digital signature will establish an organizational and technical basis for the provision of electronic information services by public authorities and local self-government bodies to legal entities and individuals through the use of the Internet. The reliable functioning of electronic document circulation will be a guarantee of Ukraine's information security.

References

- [1] A.N. Kurbatsky Automation of document processing. *Minsk*, (1999), 20.
- [2] F.F. Butinets, S.V.Ivakhnenkov, T.V. Davidov, T.V.Shahraichuk Information Systems of Accounting: Textbook. *Ed. prof. FF Buttons; 2nd species, processing. and add – Zhytomyr*. (2002), 544.

- [3] M. Bilukha Electronic Documents in Accounting. *Accounting and Audit*. 5 (2003).
- [4] Law of Ukraine on electronic documents and electronic document circulation. *Information from the Verkhovna Rada of Ukraine dated September 5, 2003*. 36 (2003), Article 275.
- [5] Law of Ukraine "On electronic digital signature" on May 22, 2003 № 852-IV. *Supreme Council of Ukraine*. 36 (2003). Art. 276.
- [6] Law of Ukraine "On mandatory copy of documents" dated April 9, 1999 № 595 XIV. *Bulletin of the Verkhovna Rada of Ukraine dated June 11, 1999*. 22 (1999), Article 199.
- [7] Law of Ukraine "On the National Program of Informatization" dated February 4, 1998 № 74/98-BP. *Bulletin of the Verkhovna Rada of Ukraine*. 27-28 (1998), 181.
- [8] Law of Ukraine "On Telecommunications" dated November 18, 2003 № 1280-IV. *Bulletin of the Verkhovna Rada of Ukraine*. 12 (2004), 155.
- [9] Law of Ukraine "On the National System of Confidential Communication" of January 10, 2002, № 2919-III. *Bulletin of the Verkhovna Rada of Ukraine*. 15 (2002), 103.
- [10] Law of Ukraine "On Protection of Information in Information and Telecommunication Systems" dated July 5, 1994 № 80/94-VR. *Bulletin of the Verkhovna Rada of Ukraine*. 31 (1994), 286.
- [11] The Law of Ukraine "On the Uniform State Demographic Registry and Documents Affirming the Citizenship of Ukraine, Identifying a Person or Its Special Status" of November 20, 2012 № 5492-VI. *Bulletin of the Supreme Council*. 51 (2013), 716.
- [12] Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Regulation on the National System of Biometric Verification and Identification of Citizens of Ukraine, Foreigners and Stateless Persons" dated December 27, 2017, № 1073. *Official Bulletin of Ukraine dated January 12, 2018*. 4 (2018), 152, article 178, code of the act 88680/2018.
- [13] The Law of Ukraine "On Protection of Personal Data" of June 1, 2010 № 2297-VI. *Bulletin of the Verkhovna Rada of Ukraine*. 34 (2010), art. 481.
- [14] Resolution of the Cabinet of Ministers of Ukraine "Some Issues of Documenting Management Activity" of January 17, 2018, № 55. *Official Bulletin of Ukraine dated 23.03.2018*. 23 (2018), 24, article 770, act code 89399/2018.
(Law of Ukraine "On electronic trust services" dated October 5, 2017, № 2155-VIII. *Bulletin of the Verkhovna Rada*. 45 (2017), 400.
- [15] Resolution of the Cabinet of Ministers of Ukraine "On Approval of the Procedure for the Use of Electronic Trust Services in State Authorities, Local Self-Government Bodies, Enterprises, Institutions and Organizations of State Ownership" of September 19, 2018, № 749. *Official Bulletin of Ukraine dated October 5, 2018*. 76 (2018), p. 23, article 2528, code of act 91594/2018.
- [16] Federal Law of 27.07.2006 № 149-ФЗ "On Information Based Information Technology on Information Protection". *Reference Legal System CONSULTAN*.
- [17] A.A. Vaishnurs Present and prospects of legal protection of databases in Russia, the USA and the European Union. *Lawyer*. 12 (2003). 45.
- [18] Electronic document management system of the executive authority Specifications TU U 30.0-33240054-001: 2005 [*Electron. resource*]. - Method: URL: <<http://www.stc.gov.ua>>.- header. from the screen.
- [19] Directive 1999/93 / EC of the European Parliament and of the Council of 13 December 1999 on the system of electronic signatures within the Community.