Application of new data formats for electronic document management in government bodies

V Pysarenko[1], L Dorohan- Pysarenko[1], N Kantsedal[1]

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

vyacheslav.pusarenko@pdaa.edu.ua

Abstract. Increasing the volume of information around the world and the rapid development of the latest information technologies led to the emergence of new opportunities for their use in the life of society, in the work of the authorities and local self-government. The introduction of computer technology for the processing, transferring, storage and use of information have led to the creation of documents on fundamentally new media, which caused the emergence of such concepts as an electronic document or document in electronic form. Analyzing the current state of the organization of processes of electronic document circulation in the activities of the public administration bodies of Ukraine as a component of e-government, it should be noted that there is a need for further study of the problem issues of the implementation of electronic document circulation, namely the order of application of electronic documents and the composition of their identity and legal registration, in order to provide legal force electronic documents and make it possible to use them on a par with paper documents. The development is devoted to the possibilities of using a new type of biometric digital signature in electronic documents of public administration bodies. The advantages and disadvantages of using this type of digital signature are analyzed. The directions of introduction of alternative means of identification of the person with the signing of electronic documents are indicated.

1. Introduction

Management acts as one of the most complex and most responsible areas of practical intellectual activity of people. It is always carried out to achieve specific goals and objectives, and their implementation is through the adoption and implementation of many managerial decisions that must be fully justified, timely, with the necessary completeness of the content and consistent with previously adopted decisions.

Ukraine's preparation for joining the EU requires changes to the current legislation and the development of new legal acts on the implementation of electronic document management.

In clause 9 of the International treaty of the Directive of 13 December 1999 No. 1999/93 / EC on the legal framework for the regulation of electronic signatures within the Community, it was stated that "... electronic signatures are planned to use in a wide variety of circumstances and applications that should expand the scope of the use of new services that are related to electronic signature, or use them. The definition of such goods and services should not be limited to the issuance and management of certificates. It should also include other goods or services that use or supplement the electronic signature, such as registration services, referral services, computer or consulting services related to electronic signature"[1].

The EU position on the legal regulation of electronic document circulation documents includes the achievement of some results - it is mainly the development of similar laws in the independent states that differ significantly in legal systems and traditions. The purpose of the European Community is not to

create the same legislation, but to promote the development of investment activity, trade, so, despite the presence of its harmonization, it is only one of the means of achieving the main goal.

The advantage of electronic document management systems for working with documents is among other things the ability to protect documents from unauthorized access by using an electronic digital signature.

Another issue for electronic document management and electronic document circulation is the need to secure the legal validity of electronic documents.

Due to the fact that the Law of Ukraine "On Electronic Digital Signature" [2], which regulates the use of electronic digital signature, was finally adopted, it became possible to provide electronic documents with legal status.

This Law defines the legal status of an electronic digital signature and regulates the relations arising from the use of an electronic digital signature, but the effect of this Law does not extend to relations arising from the use of other types of electronic signature, including the digitized self-handwritten signature image, or papillary fingerprint.

According to the Law an electronic digital signature is a props of an electronic document intended to protect it from forgery, a cryptographic tool that makes it possible to verify the absence of distortions in the text of an electronic document, and, where appropriate, to identify the person who created such a signature.

The digital signature infrastructure provides:

- the possibility of identification of the person who expressed his will through the preparation of an electronic document (the authorship of the document) or confirms the fact of familiarization with the document (visa on the document, notary's stamp, mark of inspection, etc.);
- the possibility of ensuring the confidentiality of the workflow.

An electronic digital signature in an electronic document is equivalent to a self-signed signature in a document on a paper carrier as confirmed by the current legislation.

An electronic digital signature can be obtained as a result of a cryptographic transformation of information using a private key. Of course, the complexity of the mathematical apparatus of two-key cryptography, through which the mechanism of electronic digital signature is implemented, is large.

The electronic document management system of the executive body must comply with the requirements of Clause 3.7 of the Technical Specifications (TU U 30.0-33240054-001: 2005) [Electronic document management executive authority. Specifications. TU 30.0-33240054-001: 2005], on the complex of means of protection of information from unauthorized access [3].

The key features of a digital signature are the ability to provide legal force by e-mail. The digital signature itself provides the status of an electronic document to files that contain informational content. In addition, digital signature allows you to transmit electronic documents in the same form and bring to court their authorship.

For the proper functioning of the digital signature, it is necessary to create a serious infrastructure that has received recognition in the world called "public key infrastructure" or PKI (public key infrastructure) - in the international terminology. All developed countries of the world, including Ukraine, form similar national infrastructures.

The creation of a fully-fledged digital signature infrastructure today requires the introduction of amendments to the digital signature law, which establish:

- the duty of state authorities, state organizations, their officials to accompany documents digitally and to admit them to circulation, to accept documents from citizens and their associations in electronic form, accompanied by a digital signature;
- requirements to certification centers that carry out the certification of public key digital signature, which are used to ensure the legal significance and / or confidentiality of document flow between the parties, if at least one of these parties is a state authority;
- the duty of the state authorities to certify the public key of a digital signature for use in the document circulation between this body and a citizen or organization at the request of that citizen or organization;

- the duty of public authorities to disclose and officially publish their public keys of digital signature;
- the responsibility of the certifying centers of the public keys of the digital signature for mistakes in the certificate of keys, as well as state authorities and their officials for compromising their own private keys of digital signature;
- standards that ensure the compatibility of the digital signature keys and standards that provide a specified level of stability of the keys of the digital signature;
- requirements for the development and implementation of alternative standards based on accepted algorithms and data formats in foreign countries and ensure compatibility with the existing international digital signature infrastructure;
- requirements for the development of open-source software that implements standards of digital signature in a standard manner.

In accordance with the Law of Ukraine "On Electronic Digital Signature" [2], in the absence of the possibility of overlaying and verifying an electronic digital signature with the help of an enhanced certificate (due to the lack of accredited certification centers that have the right to issue such certificates), to provide legal status to electronic document signed by electronic digital signature, the participant of the electronic circulation may act within the framework of an agreement on the recognition of an electronic digital signature, the validity of which is certified without the use of an enhanced certificate. Since the number of participants in electronic document management in public administration is large enough and the conclusion of agreements between the authority and each of them is a rather complex and inconvenient process, it may be appropriate to provide contractual basis for electronic document circulation on the basis of the accession agreement. Such a contract is made by one party - the initiator of the document circulation (coordinator), the rest of those who wish to join the system join it by providing the coordinator of the completed form-card (the mechanism of signing the contract may be determined separately). After the conclusion of the agreement the parties act in accordance with it and signed by electronic digital signature the electronic documents have a legal status. Thus a certain corporate network of electronic circulation is organized.

To provide subscribers of the corporate network of electronic document circulation with electronic digital signature services, each subscriber uses the services of the Center of Certification of keys. For this the subscriber concludes an agreement on the provision of electronic digital signature services in the form of an accession agreement with the Key Certification Center. At the same time, each subscriber (or his authorized person) must arrive at the Center of Certification of keys personally with documents confirming the information entered into the key certificate or transmitted by courier delivery (the order of certification and the list of documents are determined by the relevant documents of the Certification Center keys).

Thus for the implementation of secured electronic document circulation each subscriber must:

- Install on your computer a special software for generating electronic digital signature keys provided by the key certification center, and generate a pair of electronic digital signature keys and a couple of encryption keys. The personal digital signature key remains with the subscriber, and the public key in the form of the application for certification is provided to the Center of Certification of keys;
- to carry out the certification of its public key at the Center of Certification of keys, while providing all necessary documents confirming the information entered into the certificate of the key;
- install on your computer a special software for overlaying and verifying the electronic digital signature provided by the key certification center.

To sign and encrypt electronic documents, you need to use your private key, and to use for checking and decrypting documents received from other system participants, use the certificates of keys of these subscribers.

Each time, upon receipt of the signed and encrypted document, verify the validity of the certificate of the subscriber who signed it. To do this, you need to go to the particular resource of the Center of Certification of Keys - the table of valid certificates. If the signer's certificate is not valid at the time of the creation of the document - such a document is not valid.

In this methodology for the encryption and for decoding by the sender and the recipient the same key that they have agreed to use before the interaction is used. If the key has not been compromised, then the decryption automatically performs the identification of the sender, since only the sender has a key that can encrypt the information, and only the recipient has a key that can decrypt the information. Since the sender and the recipient are the only people who know this symmetric key, when the key is compromised, only the interaction of these two users will be compromised. The problem that will be relevant to other cryptosystems is the question of how to safely distribute symmetric (secret) keys.

2. Review of literature

Scientists interpret the concept of a digital signature - in different ways. A.V. Tkachev considers electronic digital signature as a legal category and believes that the use of such expressions in normative documents as an analog of a personal signature and equivalent to a personal signature of a person is undesirable, as it entangles the participants of the legal relationship and can create procedural difficulties in identifying persons, who used an electronic digital signature to certify computer documents [4].

The solution of the problem of the authorship of a paperless document can be achieved only with the use of an electronic digital signature, defined by L. A. Sysoevu as "... a tool that allows using cryptographic methods to reliably establish authorship and authenticity of a document" [5].

In the Law of Ukraine "On Electronic Digital Signature", which defines the legal status of an electronic digital signature and regulates the relations arising from the use of an electronic digital signature, the terms "electronic signature" are used as data in electronic form, which are added to other electronic data or logically from they are linked and intended to identify the signer of this data, and the "electronic digital signature" as the type of electronic signature obtained as a result of the cryptographic transformation of the electron collection s data included with this set, or logically combined with it and allows you to confirm its integrity and to identify signer. An electronic digital signature is superimposed using a private key and verified using the public key [2].

The reason for this is that an electronic digital signature allows you to set only the fact of its creation using a particular private key, as opposed to a personal signature that carries information about the distinctive signs of the author. The conclusion about the identity of the author of the document with the owner of the private key is based on the assumption that he is known only to its owner, but this provision can be refuted. Therefore, the idea of an electronic digital signature as an analog of a handwritten signature, according to many experts in the field of law, is based only on the similarity of the functions performed by these types of signature certificates.

The analysis of the scientific literature presented in this review revealed several unresolved issues regarding the effectiveness of the use of electronic digital signatures and their use when signing electronic documents in public administration.

3. The purpose and objectives of the study

The purpose of our research is to develop and use electronic digital signature documents, namely, the biometric digital signature, which continues to be of interest to scientists from different countries of the world and today. Despite the adoption of several legislative acts in this area, many problems remained unresolved and required additional regulation both at the legislative and regulatory-methodical levels.

4. Finding the best parameters for the process of using a biometric digital signature on electronic documents

The purposeful formation of the database of information resources necessary for the management of institutions and organizations has put the problem of document management, which is why modern document science pays great attention to studying the possibilities of advanced information technologies for their use in document management.

The basic concepts of document studies were borrowed from international standards and dictionaries, manuals issued by archivists from Australia, the United Kingdom, Canada, and the United States, as

well as from legislative acts regulating the organization of work with service documents in these countries and the theoretical works of international and national professional organizations.

A fundamentally new method of identity verification is offered at the signing of electronic documents based on biometric means of identification.

The advantages of biometric identifiers based on unique biological and physiological peculiarities of a person, which uniquely identify a person, have led to the intensive development of the appropriate means. Biometric identifiers use static methods based on the physiological characteristics of a person, that is, on the unique characteristics given to him from birth - drawing papillary lines of fingers. The general signs of patterns allow to differentiate the imprints by types and, in case of their differences, to conclude that there is no identity. To obtain the same definite conclusion about individual identity, in addition to the coincidence of standard features, it is necessary to coincide with a specific quantitative and qualitative set of distinct features, which include the beginning and end of the lines, the merging and splitting of lines, bridges, islets, hooks, points, specks, dashed lines, bends of lines etc.

The biometry allows uncontested identification of the person, and this information cannot be tampered or repaired.

Biometric identifiers provide very high rates: the probability of unauthorized access - 0.0001%, the identification time - a few seconds.

5. The strategy of solving the tasks of information security of electronic document circulation in the authorities

At the moment, reliable information security is one of the main criteria for selecting systems for storing and processing critical information. This is due to the probability of unauthorized access to such systems, as they have extensive information interaction with adjacent control systems through the Internet.

Therefore, providing information security should be the most crucial stage in their development.

Protection based on the biometric parameters of the human body, in particular, the fingerprint, has several indisputable advantages: ease of use, convenience, and reliability.

The analyzed characteristics of a person can not be lost, transmitted, forgotten, and extremely difficult to fake. They are practically not subject to wear and do not require replacement or restoration. The entire identification process takes a little time and does not require effort from those who use this access system. Research has also shown that the use of a fingerprint for personality identification is the most convenient of all biometric methods. The probability of error in identifying a user in this way is much smaller than in other biometric methods. Also, the fingerprint identification device does not require much space on the keyboard or in the mechanism. Nevertheless, it is necessary to carry out the corresponding work on the creation of a secure network for the transmission of biometric data and the infrastructure of informational interaction of state authorities among themselves, with local authorities, with consumers of management services.

6. Conclusion

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

- more efficient - high reliability with use and low level of error;
- does not require - the creation of a severe infrastructure for the full functioning of the digital signature, the creation, and approval of standards that ensure the compatibility of digital signature keys and standards that provide a certain level of stability of the digital signature keys;
- easy to use - the lack of open and closed keys and the need for special software for generating EDS keys provided by the key certification center;
- convenience - there is no need for each of the subscribers to conclude from DSK an agreement on the provision of EDS services in the form of an agreement on the admission and directly to the CSCE personally documents confirming the information provided in the critical certificate and

access to the exclusive resource of the CSK each time upon receipt of the 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.

In addition, it is necessary to clearly define at the legislative level what is a biometric digital signature, namely, a digital representation of the biometric characteristics of the person (fingerprint), a set of personal data collected on the basis of fixing its characteristics, which are of sufficient stability and substantially different from similar the parameters of other persons. To amend the Law of Ukraine "On the Uniform State Demographic Registry and Documents Affirming the Citizenship of Ukraine, Identifying a Person or Its Special Status" [6] regarding the possibility of its use.

This comparison shows a significant advantage of the method of identity verification when signing electronic documents using a biometric digital signature based on biometric identification means - a biometric digital signature.

References

[1] 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.

[2] Law of Ukraine "On electronic digital signature" on May 22, 2003 № 852-IV. *Supreme Council of Ukraine*. 36 (2003), Art. 276.

[3] J. Chyrskyy Digital Signature: legal aspects of. *Handbook secretary and office manager*. 1 (2007), 26-31.

[4] L. Tkachev Pravovoy status of computer documents: Basic characteristics. Moscow, 2000, p. 8.

[5] L.L. Sisoeva Problems electron organization vyzyrovanyya documents in electronic document systems. *Deloproyzvodstvo*. 2 (1998), 47.

[6] 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 (BPD),* 51 (2013),716

[7] M. Dutov, Legal problems of electronic document management. *Law of Ukraine*. – 6 (2002),122-124.

[8] Law of Ukraine on electronic documents and electronic document circulation. *Information from the Verkhovna Rada of Ukraine dated September 5*, 36 (2003), Article 275

[9] Shahverdov V.A. Digital signature in office automation and workflow systems / V.A. Shahverdov // *Records Management and Document Management at the Enterprise.* 8 (2003), 30-38.

[10] 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.*