Collective Based on EC-GDSA Digital Signature Protocol to Protect the Doctors' Medical Conclusion of the Consilium

Hanna Nelasa[1][0000-0002-3708-0089]

[1]Zaporizhzhia National Technical University, Zhukovsky str., 64,Zaporizhzhia, 69063, Ukraine

nelasa@zntu.edu.ua

Abstract. Modification digital signature protocol EC-GDSA on elliptic curves to collective form for telemedicine is proposed. This form may be used for security authentication of general conclusion of the doctors' concilium. Computational algorithm is given.

Keywords: telemedicine, cryptography, collective digital signature protocol, elliptic curve, EC-GDSA

1 Introduction

The fundamental task of each state is to ensure the right of its citizen to health and safety. There is a high concentration of technical and human resources in large cities and metropolitan areas in Ukraine. In such a situation, qualitative, timely and qualified medical care is not available to the majority of the population living in rural areas, what leads to a deterioration of the health of the population and average life expectancy decrease. The main task of modern medicine is to raise the quality of life of the population, increase the level of availability of medical services at the expense of the latest medical technologies. Increasing demands of Ukrainian people regarding the quality of medical goods and services compel the society look for new ways and forms for its satisfaction, or at least to improve existing ones. One such way is telemedicine.

Telemedicine is a complex of actions, technologies and measures used during the medical care using the means of remote communication for the exchange of information in electronic form. Medical assistance with application of telemedicine involves the opportunity of providing the patient with medical services for counseling, diagnosis, treatment using means of remote communication in the form of information exchange in electronic form, including by sending electronic messages, holding videoconferences [1]. Telemedicine services have already been developed and popularized abroad.

Telemedicine services are very comfortable and the most effective in remote areas. On-line consultation with physicians is much cheaper than a trip to a doctor and allows one to get a consulate faster. Implementation of telemedicine technologies will

also reduce the number of physical visits to the medical institution by patients, as well as early discharge from the hospital and further undergo certain procedures and monitoring of a health status at home.

Conditionally, telemedicine can be divided into three general directions related to medical education, the interaction “doctor-to-doctor” and the interaction “doctor-to-patient”. An important aspect here is the issue of transmission, processing, analysis, storage, protection of medical information and safe identification of the users of telemedicine services. So, telemedicine is a direction of medicine simultaneously combines telecommunications, information technologies and medical education.

In order to provide telemedicine services, it is necessary to comply with the requirements of the Law of Ukraine [2], the Order of the Ministry of Health of Ukraine [3] and the requirements of the current legislation on information security.

Confidential medical information is transmitted through computers and open networks, and requires the protection and authentication.

The urgency of the issues of protection of telemedicine information and ensuring the proper level of cryptographic security is undoubted. This is due to the fact that the latest medical technologies and measures, including telemedicine counseling, are being implemented and used in the practice of healthcare institutions. The provision of telemedicine services should ensure the preservation of personal, medical and other secrets provided by the legislation of Ukraine, as well as the confidentiality of personal data. Particularly, software used for telemedicine counseling should provide the appropriate level of protection of information and its authenticity by using an electronic digital signature.

Mandatory services to be provided to clients and owners are services such as integrity, integrity, authenticity, availability, confidentiality and reliability. The quality of providing the specified services and the level of guarantees to a large extent is determined by the methods, mechanisms and protocols of cryptographic protection of information. In order to provide the specified services with the necessary level of guarantees, it is necessary to use asymmetric and symmetric cryptographic transformations as well as cryptographic authentication protocols and the establishment of keys based on them.

Immediate implementation of medical information systems (telemedicine, electronic medical cards, "mobile medicine", cloud technologies, etc.) to the practice of the physicians will lead to increase in the competitiveness of domestic health facilities and their financial and economic security.

Directions of activity of large medical clinics and centers of private and state ownership concerning telemedicine are connected with “virtual clinics”, telemedicine consultations, “another thought” service and a consultation of the physicians.

2 Formal problem statement

The following main types of telecommunications are used for the transmission of medical data: stationary and mobile telephony; Internet (IP - protocol); GSM and CDMA networks (SMS). Individual telemedicine is often used for mobile communi-

cation and wireless Internet (GPRS, CDMA, 3G, 4G). The protection of transmitted medical information in home telemedicine systems is carried out with the help of various software and hardware, primarily cryptographic, by encryption.

The development and convenient implementation of digital signature cryptographic protocols based on elliptic curves can be a tool allows medical personnel transmit and receive relevant messages and medical information with adequate cryptographic stability and the required speed when telemedicine tools are used.

Concilium is a meeting of several doctors of one or different specialties. Concilium may be necessary to establish the state of health of the examinee, diagnosis, determination of medical forecast, tactics of further examination and treatment, expediency referral to a specialized department or other, profile, medical institution.

The key difference between the doctors' congress is the collective responsibility for the content of the medical conclusion. To ensure the authenticity of such a document in the telemedicine system, authors are encouraged to use the collective digital signature protocols. In contrast to multiple signatures [4], where signing and checking of an electronic document is important for the sequence of signatures / signatures of each participant and, in addition, the size of the signature increases proportionally to the number of participants.

For the time being in Ukraine, with the aim to ensure the functioning of telemedicine networks, it is planned to use the specialized software, which corresponds to: the DICOM standard. One of the advantages of the DICOM standard is the integration of visual data with medical data in a single file, which is why the formation of a DICOM file/package is crucial. A separate DICOM file includes, in addition to the title and image (which may contain three-dimensional information) a set of graphic and text data (relative to a patient).

The high speed of IT development forces government authorities to learn how to use them to improve the efficiency of work and be prepared for rapid change. Germany is one of the leading countries in the field of Internet development in applying cryptographic primitives and protocols and is guided by the US and EU standardization system. In this regard, it is important for Ukraine to study the German experience and determine the possibilities for its application in terms of cryptographic protection of information in general and in particular in the medical sphere.

The goal of the work is modifying the EC-GDSA electronic digital signature protocol into a collective form for the purpose of cooperation with clinics in Germany and other countries to create telemedicine services for the physician consultation and "second opinion" services, as well as its software implementation in the form of client-server application.

3 Literature review

Theoretical and theoretical foundations concerning the functioning of telemedicine systems, as well as information security in computer networks and systems, are considered in the works of domestic scientists, Godlevsky L.S. [5], Kovalenko O.S.[6], Lyakh Yu.E. [7], Martsenyuk V.P. [8, 9], Mayorov O.Yu. [10], Minzer O.P. [11], Khimzon I.I. [12]. Questions about the approaches to protecting data protection in

medical systems using cryptosystems, and increasing the reliability of cryptographic keys are also considered by such foreign experts asYudin O.K. [13], Venkatasubramanian K.K.[14], Cherukuri S. [15] and many others.

There is a problem of collective responsibility for the contents of a document (in this context, a medical conclusion) in telemedicine systems. From an IT point of view, it can be solved with a multiple signature[4]. But in this case the order of signers and verificators is important. And the size of the signature increases proportionally to the number of signers.

To eliminate these shortcomings, a new approach to the formation of a collective public key based on users' public keys was proposed [16]. Based on this approach, collective digital signature protocols are developed, including those based on modern electronic digital signature standards in different countries [17-21]. These protocols use a common (collective) public key, which is formed on the basis of the individual public keys of the group of users. The practice of electronic digital signature systems enables the use of standard open source directories and / or standard public key certificates (Internet accessibility), which facilitates the practical application of a new approach to generating a collective electronic digital signature.

At this time, cryptography on elliptical curves[22-24], the principles of which were independently proposed by N. Koblicz and V. Miller, have been widely used to offer open-source cryptographic protection systems. In Ukraine, the research of electronic digital signature on elliptical curves is also engaged in a large number of specialists, including I.D. Gorbenko, M.M.Savchuk, G.Z. Khalimov V.I. Dolgov, V.K. Zadiraka, O.O. Kuznetsov, A.V. Bessalov and others.

4 Threat analysis

Telemedicine systems, as well as other information and telecommunication systems have problems with the security of information. This is tied to the fact that telemedicine and telecommunication services are perceived separately from information security services, but should be considered complexly.

To a greater extent teleconsultation is carried out between doctors, and much more rare between a doctor and a patient. In the first case of telemedicine consultation, the opportunity of mutual exchange of electronic messages with files of various formats is very important (results of diagnostic examination, results of analyzes conducted, etc.). In this case, the most practical in terms of efficiency and economic feasibility is the sharing of files that are confidential, so the necessary protection measures should be applied to this information. In telemedicine systems, which include local networks (central subsystem with workstations, servers and data warehouses), to remotely interact with its users, remote connections of the global network are used.

Separate clinical and informational security when providing telemedicine services. Clinical security in telemedicine is related to telemedicine systems, to what extent they affect and to the extent that they are safe for the life and health of people involved in the provision of telemedicine services (patient, doctor, engineer, etc.). Information security is about medical and personal secrets, it is the security of network

infrastructure, as well as information and telemedicine systems from interference (intentional or accidental, internal or external), theft of medical or personal information, blocking processes that impede the work of users.

Loss and falsification of medical data may occur as a result of the negative impact of software, computer viruses, improper performance and equipment failure, negligent or intentional user actions. The threat and disadvantage of access to telemedicine systems are DoS attacks directed at intermediate and end nodes, as well as failures in equipment, damage to communication channels, substitution of an authorized object, listening of communication channels; loss of data (in full or in part), systematic falsification that is typical of most remote access systems.

Information security is provided through the use of the following telecommunication and hardware-software solutions: corporate medical networks, closed channels (Virtual Private Network); cryptographic protection and electronic digital signature; spam and antivirus protection; application of authorized access to servers, separate databases, workstations, etc .; transmission of information in anonymous form; the use of international standards (DICOM, SCP-ECG, etc.) in the transmission of information.

Security policy should be formed depending on the particular situation and tasks, in order to protect the personal data of a patient, it is proposed to use a variety of cryptographic algorithms, to use electronic digital signature for the transmission of medical information.

Regarding the ways of organizing telemedicine services within the hospital itself, it is possible to carry out diagnostic manipulations (e.g., ECG) by middle medical personnel, and the reading of the diagrams and the diagnosis are performed by qualified doctors in the functional diagnostic department. In case of the need for telemedicine counseling involving simultaneously two or more doctors-consultants, a telemedicine consultation (concilium) is carried out.

5 The modified method of digital signature based on EC-GDSA

In the event that a doctor encounters a complicated case in the process of treating patients in his medical practice, he usually needs additional advice (advice) from another specialist (the " another opinion" service) or several colleagues (a physician's consultation) at his or her medical institution, or else, within the city, country or abroad. In those cases where distance is a critical factor, remote counseling is provided through telemedicine.

Germany is one of the most developed states of the European Union with a high level of development of the market of telemedicine services, which is potentially the most ready to introduce new technologies.

Let's consider the national standard of electronic digital signature of Germany EC-GDSA [table 1], and we modify it to a collective form for the purpose of organizing the interaction of several doctors in consulting patients.

Let's illustrate the diagram of the deployment of the software complex (Figure 1), which ensures the authenticity, confidentiality and integrity of the medical conclusion when carrying out the consultation of physicians.

Table 1. - The EC-GDSA Digital Signature Standard

Formation of a digital signature	**Verification of digital signature**
Input: secret key d, public key $Q = d^{-1} \times P$, general system parameters. **Output:** digital signature $\langle r, s \rangle$ for message M.	**Input:** public key Q, general system parameters, digital signature $\langle r', s' \rangle$ for message M'. **Output:** The signature is valid or not.
1. $h = H(M) \bmod n$; **2.** Choose random $k \in \{1,...,n-1\}$; **3.** $k \times P = (x, y)$; **4.** $r = \pi(x, y) \bmod n$; **5.** $s = (kr - h)d \bmod n$.	**1.** $h = H(M) \bmod n$; **2.** $w = (r')^{-1} \bmod n$; **3.** $u_1 = h'w \bmod n$; **4.** $u_2 = s'w \bmod n$; **5.** $(x, y) = u_1 \times P + u_2 \times Q$; **6.** $v = \pi(x, y)$; **7.** $r' \overset{?}{=} v$

The system consists of:
- *Server* - leading doctor;
- *Client* - doctors - consultant from 1 to l.

Diagnostic equipment is directly connected to the host's doctor's server.

Consider the modification of the current EC-GDSA Digital Signature Standard for the implementation of a collective signature, which may be useful for ensuring the safe authentication of a general medical conclusion when the consultation is carrying out.

The protocol consists of three parts: the generation of a public key, the formation of a collective signature, the verification of the collective signature.

The designation:

P - the base point of the elliptic curve (the general parameter of the cryptosystem);
l - number of signatories (consultants);
n - the order of the cyclic subgroup of the elliptic curve points;
d_i - the secret key of the *i*-th signer (doctor-consultant);
h – the hash of the document (medical conclusion);
Q - general public key (point of the elliptic curve);
Q_i – share of the public key of the i-th doctor-consultant (EC point).

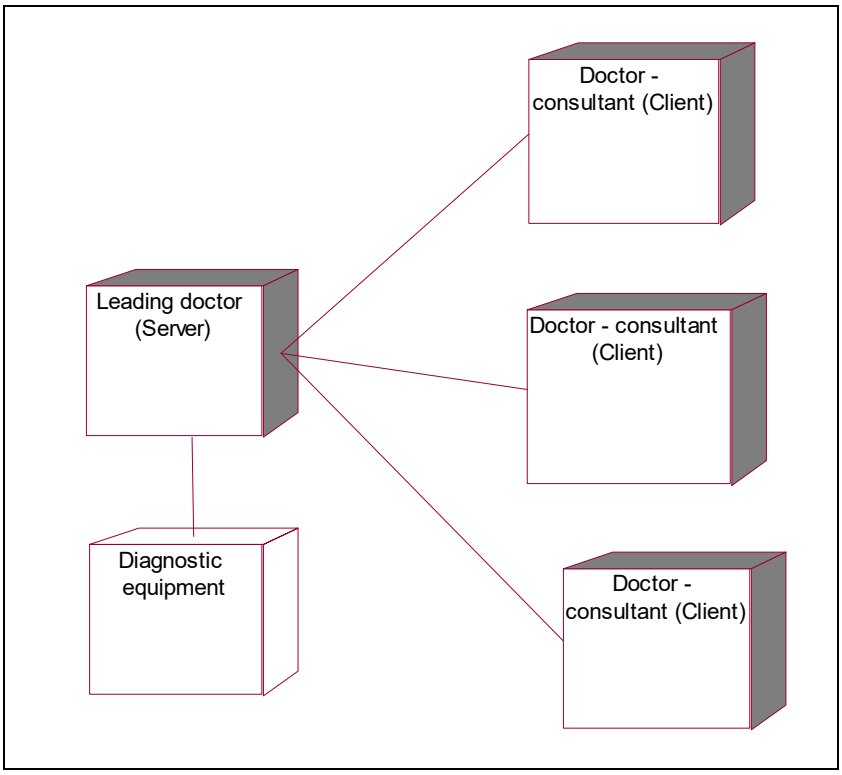

Fig. 1. - Diagram of the deployment of a software for concilium

Part 1. Generation of a public open collective key.

1. The leading doctor (Server) initiates the calculation of the general public key (point *Q*). After that, each doctor-consultant (Client) calculates the share of the public key, which is then transferred to the leading doctor.

$$Q_i = d_i^{-1} P .$$

2. The leading doctor (Server) calculates the total secret key Q, as the sum of the shares of the public keys of the group of *l* signers (consultants of the concilium).

$$Q = \sum_{i=1}^{l} Q_i = \sum_{i=1}^{l} d_i^{-1} P \cdot$$

Part 2. Formation of a collective signature.

1. A leading physician (Server) calculates a hash of a document (medical conclusion) and transmits it to all doctors-consultants (Client).

2. Each i-th subscriber (doctor - consultant, Client) calculates a point as follows:

a) selects a random parameter (random variable) k_i, $1 < k_i < n$;

b) calculates the point $R_i = k_i P$

c) sends it to the *Server*.

3. The leading doctor (Server) calculates the total point R as the sum of R_i:

$$R = \sum_{i=1}^{l} R_i = (X_R, Y_R)$$

4. The leading doctor (Server) calculates the first part of the collective signature

$$r = \pi(R) = X_R \bmod n$$

and sends it to all signers.

5. Each subscriber (doctor-consultant, *Client*) calculates its part s_i:

$$s_i = (k_i r - h) d_i \bmod n$$

using its private key d_i, and sends it to Server

6. The leading doctor (Server) calculates the second part of the collective signature

$$s = \sum_{i=1}^{l} s_i \cdot$$

7. Collective signature is a pair of numbers – (r,s).

Part 3. Checking the collective signature.

1. The verifier calculates the hash of the document (medical conclusion).
2. The verifier calculates the values:

$$w = (r')^{-1} \bmod n,$$
$$u_1 = h' w \bmod n,$$
$$u_2 = s' w \bmod n.$$

3. and, using an open collective key Q, forms a point

$$(x, y) = u_1 P + u_2 Q$$

and calculates the value

$$v = \pi(x, y) = x \bmod n.$$

5. If $r' = v$, then the signature is authentic, in the other part it is forgery.

Justification of the correctness of the submitted protocol.

Since the value of r is determined by the formula $r = \pi(R) = \pi(\sum_{i=1}^{l} k_i P)$ when forming a signature, and when checking the signature verifier $u_1 P + u_2 Q$ is the point R, then

$$u_1 P + u_2 Q = h'wP + s'wQ = h'wP + s'w\sum_{i=1}^{l} d_i^{-1} P = w(h' + s'\sum_{i=1}^{l} d_i^{-1})P =$$

$$r^{-1}(h' + \sum_{i=1}^{l}[(k_i r - h)d_i]\sum_{i=1}^{l} d_i^{-1})P = r^{-1}(h + \sum_{i=1}^{l} k_i r - h)P = \sum_{i=1}^{l} k_i P = R$$

as a result we have:

$$v = \pi(u_1 P + u_2 Q) = \pi(R),$$

which corresponds to the value r when the signature is formed.

Note that the Server function can act as a separate individual of the protocol, and one of the consultants. In this case, it combines Server and Client functions, which does not interfere with the correct operation of the protocol. If the number of participants equals two, we have the implementation of the "another opinion" service, which from the point of view of technical implementation is a special case of a concilium.

6 Conclusion

Thus, modern economic, scientific and social changes, rapid development and introduction of innovative technologies, and a significant increase in data exchange information processes require timely response to changes in the medical sphere, and oblige comprehensive protection and confidentiality of medical data in modern telemedicine systems.

The authors carried out an analysis of threats and modern methods of protecting confidential medical information. The analysis of possible variants of confidentiality and identification of the authorship of electronic communications for the provision of telemedicine services, as well as analysis of critical, in terms of information security, elements and communication channels infrastructure of telemedicine systems.

It is established that in the context of the reform of the health care of Ukraine, a significant reduction of the bed fund, important issues are the improvement of medical diagnostic processes, the implementation of information and telecommunication technologies, the organization of interaction between medical, preventive and specialized health care institutions through telemedicine , remote provision of qualified medical services, maximum utilization of the intellectual potential of the best clinics.

In the case of the need for telemedicine counseling with the participation of several consultants, a telemedicine consultation is conducted. It has been established that some issues, including those concerning the practice of the use of a collective digital signature in domestic health care institutions, for example, for the consultation of physicians, remain unresolved. Germany is one of the most developed states of the

European Union with a high level of telemedicine market development, potentially the most ready to introduce new technologies. Therefore, the possibility of modifying the current EC-GDSA electronic digital signature standard for Germany for the implementation of a collective signature is considered, which may be useful for ensuring the safe authentication of a general medical conclusion when physician consultation is carrying out.

The development of software for the proper level of cryptographic protection of information in telemedicine, the implementation of the EC-GDSA collective digital signature protocol, including to solve the problem of conducting a consultation of doctors, can also be used for cooperation with medical institutions in Germany and other European countries and the world to create a telemedicine service "second thought". For this purpose, the analysis and research of modern digital signature standards based on cryptographic transformations in the groups of points of elliptic curves has been carried. The proposed collective digital signature protocol is based on the EC-GDSA standard using a method similar to another one used in the collective signing protocol DSTU4145.

A software package with a client-server architecture is developed. It allows to ensure the preservation of the authenticity, integrity of the non-contradiction of electronic medical documents by protecting them with collective digital signature methods, based on the standards DSTU4145, EC-GDSA. To develop the project, the C ++ programming language and the Miracle cryptographic library were selected, which includes the functions of long arithmetic and the implementation of the arithmetic of elliptic curves defined over the simple and extended finite fields of Galois.

References

1. Vladzimirskiy A.V., Telemedicine: Curatio Sine Tempora et Distantia. Digital Printing, Moscow, 663p. (2016)
2. Information Law System "League of Law": Law of Ukraine 18.09.2017 No. 7117 "On Increasing the Availability and Quality of Medical Services in Rural Areas". http://search.ligazakon.ua/l_doc2.nsf/link1/JH5HP00V.html (2017)
3. Ukraine. Ministry of Health. On Approval of Regulatory Documents on the Application of Telemedicine in the Healthcare: Order dated 19.10.2015, No. 681., A Collection of Regulatory and Policy Documents on Public Health 1, pp. 12-26 (2016)
4. Min-Shiang Hawng, Cheng-Chi Le. Research issues and challenges for multiple digital signature, Int. J. of Network Security, vol.1 (1), pp.1-7 (2005).
5. Godlevsky L.S., Dets V.V., Stepanenko K.I. [and others]: Perspectives for the introduction of telemedicine technologies for the elderly in the Odessa region. Biophysical standards and information technologies in medicine. Proceedings of sciences conf. – Odessa, Astroprint, pp. 48-52 (2004)
6. Kovalenko O.S., Buryak V.I.: Standardization of medical information systems with taking into account pan-European integration. Clinical informatics and telemedicine (1), pp. 35-41 (2004)
7. Lyakh Yu.E., Vladzimirskiy A.V.: Introduction to telemedicine. Essays on biological and medical informatics, Donetsk: Lebed, 101 p. (1999)
8. Martsenyuk V. P. Development and application of information system of recording (selfrecording) patients for consultation of university clinics specialists / V. P. Martsenyuk, P.

R. Selskyy, A. V. Semenets // Ukrainian journal of telemedicine and medical telematics. – 2013. – Vol. 11, No. 2. – P. 173–178.
9. Martsenyuk V. P. Performance of telemedicine technology usage for increasing quality of treatement and diagnostical work of primary care / V. P. Martsenyuk, P. R. Selskyy // Actual problems of pharmaceutical and medical science and practice. – 2013. – Vol. 12, No. 3. – P. 53–54.
10. Mayorov O. Yu., Bilov L.B., Nezhensky C.A.: Information systems of public health services (hospital information systems) - a tribute to the fashion or necessity (feasibility study of the introduction of the program complex "C-Hospital®"). Clinical informatics and telemedicine, vol.1, (1), pp. 1-12 (2004)
11. Mintser O.P., Bolgov M. Yu.: Information mapping of medical diagnostic process at the level of data logic. Ukrainian Journal of Telemedicine and Medical Telematics, vol. 5 (2), pp. 128-138 (2007)
12. Khimzon I.I.: Development and research of the efficiency of new information technologies for the management, processing and accounting of medical documentations in the conditions of the hospital department: abstract for the sciences degree of dr. Tech. Sciences: special 05.13.02 "Mathematical modeling in scientific researches". National Academy of Sciences of Ukraine, Institute of Cybernetics V.M. Glushkov, Kyiv, 30 p. (1995).
13. Judin O.K., Korchenko O.G., Konakhovych G.F.: Protection of information in data transmission network, Kyiv: "NVP" INTERSERVICE ", 716 p (2009)
14. Venkatasubramanian K. K., Banerjee A., Gupta S. K. S. PSKA: Usable and secure key agreement scheme for body area networks // IEEE Transactions on Information Technology in Biomedicine. 2010. Vol. 14, No 1. Pp. 60-68.
15. Cherukuri S., Venkatasubramanian K., Gupta S. K. S. BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body // Proceedings of Workshop on Wireless Security and Privacy. 2003. Pp. 432-439.
16. Moldovian D.H., Moldovyan N.A. Two-key cryptosystems with a new mechanism of digital signature generation // Information Security Management. 2006. Vol. 10. No. 3. pp. 307–312.
17. Hortinskaya, L.V., Moldovian, N.A., Kozina, G.L.: Implementation of protocols of collective signatures on the basis of GOST 34.310-95 and DSTU 4145-2002 standards. Legal, normative and metrological provision of the information security system in Ukraine. Kyiv, NTUU "KPI", No. 1.,pp. 82-86 (2008)
18. Nelasa H.V., Kozina G.L., Moldovian N.A.: Collective digital signature protocols on elliptic and hyperelliptic curves. Radio Electronics, Computer Science, Control. 1(19) Zaporizhzhia, ZNTU, pp. 127-133 (2008)
19. Kozina, G.L., Moldovian, M.A., Nelasa, H.V.: Crypto Protocols: Digital Signature Schemes. Zaporizhzhia, ZNTU, 158 p. (2014)
20. Shovgenyuk R.V., Software of cryptographic protection in telemedicine. Master's thesis, supervisor associate professor Nelasa H.V., ZNTU, 224 p. (2017)
21. Nelasa H., Shovhenyuk R., Korolkova O.: Collective digital signature EC-GDSA based protocol for telemedicine. II All-Ukrainian Scientific and Practical Conference "Prospective Directions of Modern Electronics, Information and Computer Systems" (MEICS-2017) Dnipro, 22 November 24, pp. 123-124 (2017)
22. Koblitz N. A Course in Number Theory and Cryptography. Berlin, Heidelberg, New York: Springer, 1994.
23. Malhotra K., Gardner S., Patz R. Implementation of elliptic-curve cryptography on mobile healthcare devices // Networking, Sensing and Control. 2007. Pp. 239-244.
24. Liu A., Ning P. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks // Information Processing in Sensor Networks. 2008. Pp. 245-256.