ORIGINAL ARTICLE

Development of the pharmacological product identification system with guaranteed reliability

Irina V. Spichak[1], Roman P. Gahov[2], Pavel V. Cherkashin[2], Vladimir E. Poryadin[1], Igor S. Friz[2]

[1]Department of Management and Economics of Pharmacy, Belgorod State University, Belgorod, Russia, [2]Department of Information Systems, Belgorod State University, Belgorod, Russia

Abstract

Background and Objective: The article is a considerate system, designed for marking and the identification of goods and the subsequent monitoring of their movement. The system designed to provide a guaranteed authenticity of the markings applied to a controlled product. The system's reliability is based on the principles of symmetric and asymmetric key encryption and on "point-to-point" encryption of the markers, as well as on the technology of a secure communication channel. **Materials and Methods:** The article considers an algorithm for creating an encrypted token and transmitting data over closed channels. Special attention is paid to the key formation with the special PBKDF2 library, the generation of 512-bit hashes according to the GOST R 34.11-2012 and the subsequent formation of a symmetric cipher GOST R 34.12-2015. This encryption algorithm allows to view the marker on the medicine package as an encrypted message in the precision time protocol. The author also considers the use of encrypted secure sockets layer and transport layer security protocols when communicating between client devices and infrastructure devices that provide the functioning of a monitoring system. **Results:** In addition, the article highlights the federal grain inspection service Federal State Information System for Monitoring the Movement of Drugs (FSIS MMDP) system which is created by the Federal Service for Supervision in Health Care, its organizational and legal base and the possibility of integration of these systems. **Conclusion:** As a result of the research it was established that protocols for data exchange and coding of markers, which allow to make reliable operation of the system for monitoring the movement of medical products and to design a unified system for monitoring the movement of goods, or the definition of their owner and also the study showed possible vulnerabilities of the system FSIS MMD.

Key words: Anti-counterfeiting, communication channels, cryptographic protection against counterfeit medicines, GOST R 34.11-2012, GOST R 34.12-2015, pharmaceuticals, pharmacological product, public-key cryptography, secure sockets layer, symmetric encryption, transport layer security

INTRODUCTION

There are no products marking system with high resistance to cryptographical attack in the Russian Federation today. Apart from that, there are also similar systems which are vulnerable to replication.

Therefore, the creation of a modern system is relevant and considered by many market participants as relevant.

According to the annual statistics, economic damage from counterfeit drugs was comparable to the state's expenses for the purchase of essential medicines. In 2014, more than 4000 tons of counterfeit drugs were destroyed on the territory of the Russian Federation. Counterfeit drugs cause irreparable harm to the health of the population, as well as a huge setback to the reputation of manufacturers. The situation aggravated by the rapid growth of the popularity of "online pharmacies," in which counterfeit drugs are most often found.[1]

Address for correspondence:
Irina V. Spichak,
Department of Management and Economics of Pharmacy, Belgorod State University,
Belgorod - 308 015, Russia.
E-mail: gahov@bsu.edu.ru

Received: 04-07-2017
Revised: 29-07-2017
Accepted: 12-08-2017

As part of counteracting the trafficking of counterfeit drugs, the Government of the Russian Federation has initiated the creation of a federal state information system for monitoring the movement of drugs Federal State Information System for Monitoring the Movement of Drugs (FSIS MMD). The launch of the pilot phase is planned in 2017.[2] So in our project, we will rely on the system as the basis of the state policy in this matter. Legislative and legal acts and normative documents of the Russian Federation, the algorithm for the operation of cryptosystems with public key (PK) (GOST R 34.10-2012), transport layer security (TLS) and secure sockets layer (SSL) protocols (open SSL cookbook), algorithms, GOST R 34.11-2012, and GOST R 34.12-2015.

MATERIALS AND METHODS

To solve our research problems, we divided our work into two: The study of the regulatory, legal, and organizational measures aimed at preventing the trafficking of fake and counterfeit drugs; the studying of the methods of cryptographic protection of information and building secure communication channels.

First, we examine the regulatory, legal and organizational means of preventing the trafficking of counterfeit drugs.

In particular, the Federal Law No. 294 of December 26, 2008, "On the Protection of the Rights of Legal Entities and Individual Entrepreneurs in the Conduct of State Control (Supervision) and Municipal Control," tightens the responsibility for the production, sale and import of counterfeit, inferior, unregistered drugs, or biological supplements. The law provides for punishment for forgery of packaging, documentation or labeling of medicinal products.

According to the order No. 5539 of August 7, 2015 "On approval of the procedure for the implementation of selective quality control of medicinal products for medical use", requirements are set for the implementation of selective quality control of medicinal products for medical use. Within the framework of selective control, the compliance of medicinal products with the requirements of a pharmacopeia article or normative documentation is confirmed within the Federal Service for Surveillance of Healthcare (Roszdravnadzor) and its territorial subdivisions. In case of detection by selective quality control, the whole series of drugs must be withdrawn from sale. The application of the FSIS MMD increases the effectiveness of the execution of this order because the system provides information on the location of each drug from the series.[3]

Decision of the Commission of the Customs Union No. 769 of August 16, 2011 "On the adoption of the technical regulations of the customs union" on the safety of packaging ("TR TS 005/2011") establishes uniform security requirements throughout the territory of the customs union the rules for labeling and handling of pharmaceutical packages.[4]

Resolution No. 686 of the Government of the Russian Federation of July 6, 2012 "On approval of the regulation on the licensing of the production of medicinal products," establishes the procedure for licensing activities for the production of drugs. This procedure affects such an important component as obtaining reliable information about registered drugs.[5]

Based on the requirements of Order No. 866 of the Ministry of Health of the Russian Federation of November 30, 2015, "On the approval of the concept of the creation of a federal state information system for monitoring the movement of medicinal products from the manufacturer to the end consumer using marking" (FSIS MMD), a mechanism was developed for the continuous monitoring of drugs, using individual and group coded labeling and identification of packages of drugs. The purpose of this system is to ensure effective quality control of drugs in circulation and to prevent their falsification. To identify the series and package of a specific drug, the system prescribes the use of specialized graphic markers, such as quick response (QR) code and data matrix (DM), containing the unique identifier of the unit of the medicinal product or lot, as well as the other identifiers required for identification. The functioning of this system also simplifies the monitoring of the shelf life of drugs and simplifies the process of removing the expired/defective ones from the market.[6]

RESULTS

Thus, a set of regulatory, legislative and organizational measures applied by the state aimed at raising the level of drug safety in the Russian Federation, as well as attracting the country's population to protect their own rights and interests. The means of accomplishing these tasks is the FSIS MMD, which is able to control the turnover of medical products in the pharmaceutical market of the country and the entire customs union, thus supporting the interests of all market participants, from suppliers and consumers to the fiscal authorities of the state.

This order describes the system security requirements and its organizational structure, which is shown in Figure 1.

An analysis of the above documents shows that the system provides for an exchange between its participants through the inter-agency electronic interaction system of inter departmental electronic interaction (SIEI). Its use presupposes the protection of all slavish documentation using an electronic digital signature (DS).

However, in the current form, the system remains vulnerable to unscrupulous participants. Open package

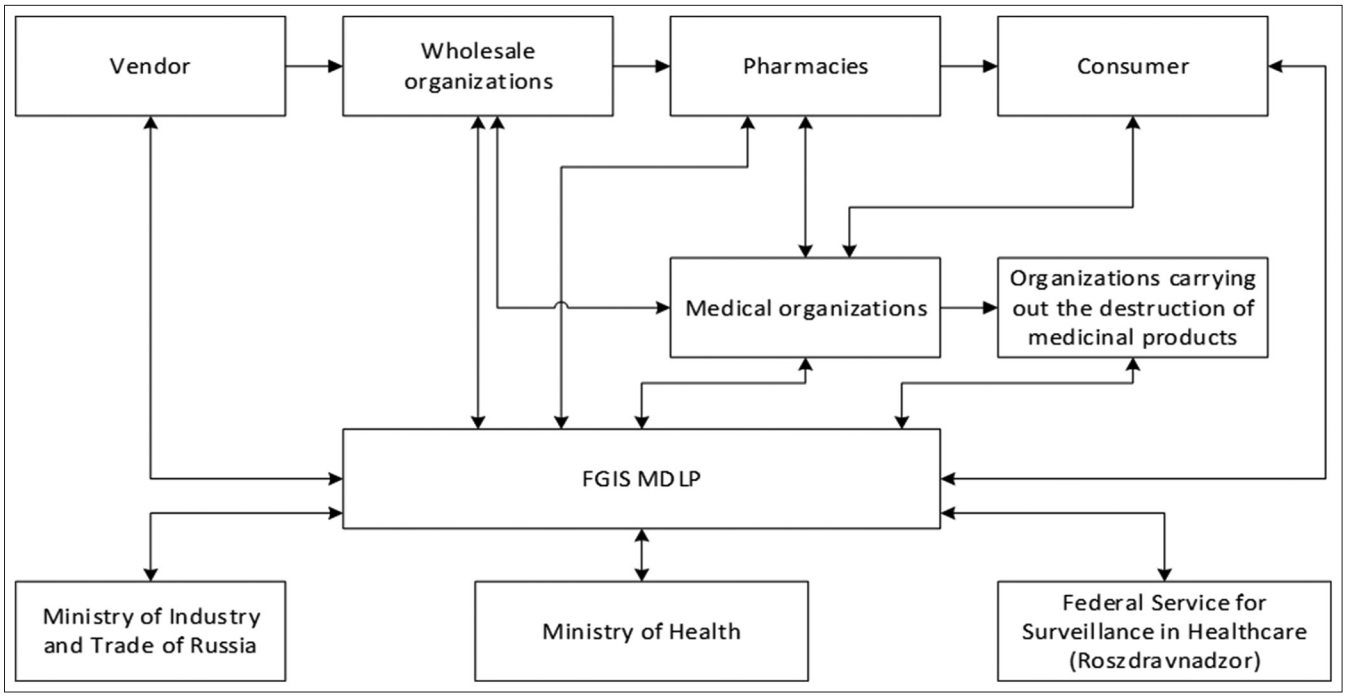

Figure 1: Organizational structure of federal grain inspection service MDLP functioning

transmission and individual codes, allow you to decipher the algorithm of your group and introduce counterfeit along the route of the drug, like the so-called "man-in-the-middle" (MITM). Adding a control hash of the DS obtained by the individual drug code and group code also does not give a full guarantee, as there is a vulnerability of any hash to collisions. In addition, sending it along with the encoded data in an open form leads to the possibility of carrying out a crypt analytical attack.[7]

To top it off, there remains the unsolved problem of vulnerability for the attack of the MITM communication channel between the consumer and the monitoring server.

The following actions are taken to address the identified vulnerabilities:

- Based on the materials studied, we developed a cryptographic protection protocol for digital markers applied to a medicinal product;
- We have developed a protocol for data exchange between the monitoring server by the consumer and the manufacturer.

First, the information security of the subsystem will significantly increase from the use of secure communication channels, such as SSL, TLS, and secure shell, which increases the system's resistance to MITM attacks, which are especially critical when responding to applications on the mobile platform. In addition, a specific protocol was developed for the data exchange considering each package of drug or a group of packages in a container as a separate message sent by the manufacturer to the server. At each stage, there should be an opportunity to verify the reliability of this

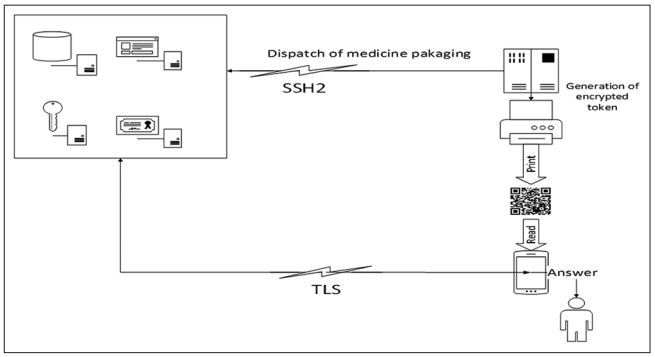

Figure 2: Scheme of exchanging data

message. This protocol is based on the principle of "end-to-end" protection. The general scheme of exchanging data on this protocol is depicted in Figure 2.

Data exchange under this protocol allows any end user device (consumer smartphone or control device in the warehouse) to verify the authenticity of the drug and its expiration date.

Each message, actually, applied to the packaging in the form of a QR or DM marker is a set of fields, shown in Table 1.

Under Medical Equipment and Technology Association (META), the medical product packaging has (individual number, serial number, drug code, manufacturer's code, date of issue, etc.) some of this listed data on the package are for visual comparison by the buyer, all these data are known only to the licensee of the drug and the control server. The number of bits allocated for useful information depends on the type of marker used. The maximum capacity of DM is 2 kb and about 3 kb (2953 bytes) of QR code. For the system to function, the

exporter/manufacturer must have his personal private key. The most reliable way to store this is by encoding this key in hardware, for example, in (programmable logic integrated circuit). This scheme will be included in the marking equipment. The key is the private key of the manufacturer in encoding algorithm. Figure 3 demonstrate the algorithm of encrypted marker generation.

In this scheme, META is the data for each individual drug package (individual number, serial number, medical product code, manufacturer's code, release date, etc.).

PK is a public key, the formation of which occurs when the drug is released.

The PK used not only as an element that allows you to calculate the key for encryption but also as a checksum (hash) for verification of metadata.

A private key is the key for encryption generated by a secret algorithm.

E_META - Encrypted by private key metadata (encrypted META).

Table 1: Message fields in binary form

Salt	Meta		Alignment
128-bit	16256 - bitmax for DM	23496 - bitmax for QR	0-15 - bit

DM: Data matrix, QR: Quick response

Card_ID is the identifier of the circuit card that points to the key stored in it; this mapping is secret and is known only to the division which is supervising federal information help system for monitoring the movement of drugs (FIHS MMD).

As the scheme show, the algorithm designed to use the most up-to-date domestic encryption standards such as the block encryption algorithm "Grasshopper" - GOST R 34.12-2015, which assumes the use of a 256-bit key.[8]

In the same way, an algorithm for obtaining the hash's "Stribog" (GOST R 34.11-2012) is used which can also generate 512-bit hashes.[9]

To generate the encryption key, the functions of the PBKDF2 library are used.

The algorithm assumes that a set of metadata is sent to the FSIS center from the plant at the time of marking. At the time of the verification of the marking, the Card_ID, PK, and encrypted metadata are sent to the server. The server determines the private key on the PK and decodes the metadata, after which the data are searched in its database. Further, the server sends a response to the user that also contains some data on the package (name, serial number, and manufacturer) that will make it possible to visually verify the authenticity of the medicine.[10]

This algorithm ensures that the packaging of the medicinal product that is checked at each stage of the movement on the pharmaceutical market is the same package that began its

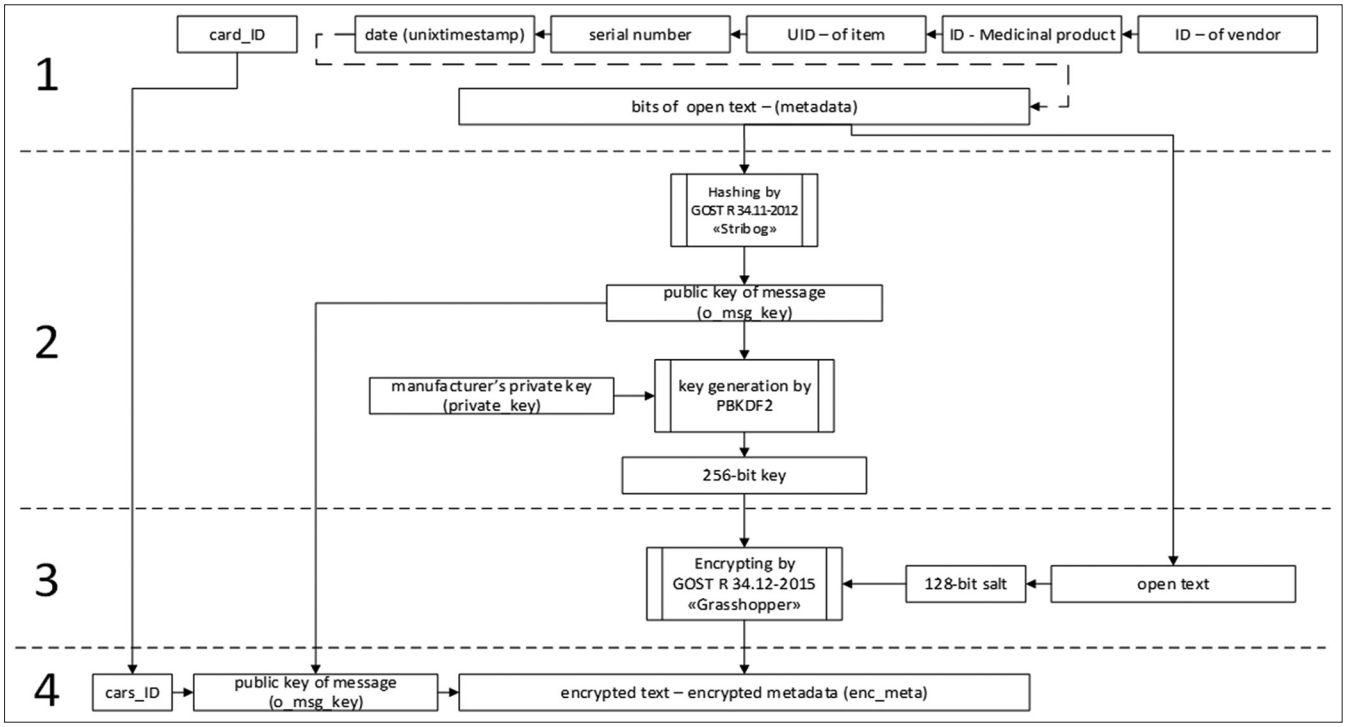

Figure 3: Scheme of the generation of the encrypted marker

movement from the manufacturer.[11] From a cryptographic point of view, protection is difficult to circumvent. Since at any of the stages (except the first one in which an attacker should be excluded organizationally), the attacker does not have a complete set of data to select a combination capable of the collision, or the selection of data to calculate the key or encryption algorithm.

It should be noted such a feature of the system has the need to ensure that the packaging of the medical product will not be opened on the way to the consumer, and stored in the proper conditions. Furthermore, an important task is the protection of algorithms and keys that are in charge of the supplier, hypothetically, not being a person interested in forging their products, because it carries reputational risks, but is capable of applying them for the purposes of unfair competition.

CONCLUSION

From an economic point of view, this system is not commercial and intended for use in government regulation aimed at improving public welfare. It's application for commercial purposes faced with the problem of organizing and regulating the interrelations of its various participants. A private company can voluntarily label its products, but a tangible positive effect is possible only in the case of mandatory labeling of its products by all market participants. However, in cases when it comes to expensive goods that are subject to individual registration, the application of this system is appropriate, and it becomes a guarantee that a reliable quality product delivered from the seller to the buyer. An example of such a product is used in weapons, jewelry, and so on. The increase in the cost of medical products faced by producers theoretically compensated for by eliminating unfair competition in the market.

REFERENCES

1. DSM Group. Russian Pharmaceutical Market-2013. Moscow: DSM Group; 2013. p. 29.
2. The market of medicines and new opportunities of federal service for surveillance in healthcare. gmpnews.ru. № 15; 2015 [Electronic resource].
3. Russian Federation. Laws. Federal Law. No. 294 from December, 26 'On the Protection of the Rights of Legal Entities and Individual Entrepreneurs in the Exercise of State Control (Supervision) and Municipal Control'; 2008.
4. Decision of the Commission of the Customs Union of August 16, 2011 No. 769 'On the Adoption of the Technical Regulations of the Customs Union' On the Safety of Packaging'; 2011.
5. Russian Federation. Decisions of the Government. Resolution No. 686 of the Government of the Russian Federation of July 6, 2012 'On Approval of the Regulation on the Licensing of the Production of Medicinal Products'; 2012.
6. Russian Federation Ministry of Health. Orders. No. 66 from November 30, 2015. "On approval of the Concept of creation of the Federal State of information system for monitoring the movement of drugs from the manufacturer to the end user".
7. Petrov AA. Komp'yuternaya Bezopasnost'. Kriptograficheski Ye Metody Zashchity. [Computer Security. Cryptographic Protection Methods]. Moscow: DMK; 2000. p. 448.
8. GOST R 34.11-2012 (National Standard of the Russian Federation)Information technology. Cryptographic protection of information. Hashing function. 34.11. 2012.
9. GOST R 34.12-2015 (National Standard of the Russian Federation)Information technology. Cryptographic protection of information. Block ciphers. 34.12. 2015.
10. Spichak IV, Poryadin VE, Razdorskaya IM, Spichak AS. Pharmacy competitiveness optimization using information technologies. Int Bus Manage 2015;9:1595-7.
11. Ivan R. Open SSL C Book. London: Feisty Duck Digital; 2016. p. 99.

Source of Support: Nil. **Conflict of Interest:** None declared.