doi: 10.17586/2226-1494-2025-25-2-311-320

Integration of enhanced qualified electronic signature to the fast healthcare interoperability resources (FHIR RU-core) protocol

Nikolai A. Gorbunov[1]✉, Valeria O. Kuleshova[2], Viktoriia M. Korzhuk[3]

[1] "Netrika Medicine" LLC, Saint Petersburg, 191015, Russian Federation
[1,3] ITMO University, Saint Petersburg, 197101, Russian Federation
[2] CSRI Elektropribor, Saint Petersburg, 197046, Russian Federation

[1] gorb-2157@mail.ru✉, https://orcid.org/0009-0004-2973-9594
[2] valeria.kuleshova@yahoo.com, https://orcid.org/0000-0003-1377-6003
[3] vmkorzhuk@itmo.ru, https://orcid.org/0000-0002-0240-9067

Abstract

The article discusses how to use the Russian profile of the Fast Healthcare Interoperability Resources (FHIR) RU-core protocol for medical information systems developing. An enhanced qualified electronic signature has been used for information protection for a long time; however, it is currently being implemented for the first time with the FHIR RU-core protocol to protect medical information systems. The goal of the research is enhanced qualified electronic signature integration for organizations developing secure software for medical information systems. To reach the goal, the following tasks are solved: previous works including foreign ones are analyzed and the table with different variants of FHIR protocol using is presented; the step-by-step plan of an enhanced qualified electronic signature integration has elaborated. A software code has been created to ensure the safe transmission of sensitive medical data to meet the challenge of implementing an enhanced qualified electronic signature. Russian standards were used to implement cryptographic protection of information in various medical information systems. To ensure secure data exchange, an enhanced qualified electronic signature was incorporated into the domestic version of the FHIR protocol. The use of Russian version of the protocol and certificates result in the correct exchange of medical documents. New functionality for medical information systems was standardized through the application of the Russian profile of FHIR protocol. Medical information systems deployed in the certified data processing centers are now using the FHIR RU-core protocol. The medical community easily uses FHIR RU-core, which is the most advanced tool for domestic medical systems. The method is aimed at integrating health information systems safely to develop regional services for doctors, patients, and digital health care organizers. The scientific novelty and relevance of the research lies in the field of adaptation international experience of using FHIR protocol under Russian circumstances and refinement of an enhanced qualified electronic signature integration method without capacity loss. The practical result demonstrates that the use of the Russian enhanced qualified electronic signature satisfies the information security requirements of new medical information systems and allows sensitive data to be transmitted without loss of quality and speed. It has been concluded that a systematic approach to using the Russian profile of the FHIR RU-core protocol for new medical information systems, with the aim of implementing digital healthcare, is highly recommended. This article is a valuable resource for medical information systems software architects and developers, as well as information security specialists.

Keywords

medical information systems, Russian FHIR protocol, electronic signature integration

Acknowledgements

Funding from the research project "Autonomous Intelligent Systems" No. 623106 at ITMO University.

For citation: Gorbunov N.A., Kuleshova V.O., Korzhuk V.M. Integration of enhanced qualified electronic signature to the fast healthcare interoperability resources (FHIR RU-core) protocol. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 2, pp. 311–320. doi: 10.17586/2226-1494-2025-25-2-311-320

УДК 004.056

Интеграция усиленной квалифицированной электронной подписи с ресурсами быстрого взаимодействия в сфере здравоохранения FHIR RU-core

Николай Александрович Горбунов[1]✉, Валерия Олеговна Кулешова[2], Виктория Михайловна Коржук[3]

[1] ООО «Нетрика Медицина», Санкт-Петербург, 191015, Российская Федерация
[1,3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
[2] АО «Концерн «ЦНИИ «Электроприбор», Санкт-Петербург, 197046, Российская Федерация

[1] gorb-2157@mail.ru✉, https://orcid.org/0009-0004-2973-9594
[2] valeria.kuleshova@yahoo.com, https://orcid.org/0000-0003-1377-6003
[3] vmkorzhuk@itmo.ru, https://orcid.org/0000-0002-0240-9067

Аннотация

Введение. Рассматривается возможность использования российского профиля протокола Fast Healthcare Interoperability Resources (FHIR) RU-core для разработки медицинских информационных систем. Усиленная квалифицированная электронная подпись применяется для защиты информации уже длительное время, однако, совместно с протоколом FHIR RU-core для защиты медицинских информационных систем — впервые. В работе предложен процесс внедрения усиленной квалифицированной электронной подписи для организаций, разрабатывающих безопасное программное обеспечение для медицинских информационных систем. Для достижения цели были решены следующие задачи: проанализированы русские и зарубежные научные работы, и составлена таблица возможностей использования протокола FHIR, выработан пошаговый план внедрения усиленной квалифицированной электронной подписи. **Метод.** Для решения задачи внедрения усиленной квалифицированной электронной подписи был разработан программный код, который позволяет передавать чувствительные медицинские данные безопасно. Проведена реализация криптографической защиты информации при помощи российских стандартов интеграции различных медицинских информационных систем. В отечественной версии протокола FHIR встроена усиленная квалифицированная электронная подпись для защищенного обмена данными. Корректный обмен медицинскими документами возможен при использовании российских версий протокола и сертификатов. Проведена стандартизация применения российского профиля протокола FHIR RU-core для медицинских информационных систем с новым функционалом. Протокол FHIR RU-core был внедрен в медицинские информационные системы, развернутые в аттестованных центрах обработки данных. Стандарт FHIR RU-core является наиболее инновационным инструментом для отечественных медицинских систем, так как находится в открытом доступе, и удобен для применения медицинским сообществом. Метод ориентирован на безопасную интеграцию медицинских информационных систем для развития региональных сервисов для врачей, пациентов и организаторов цифрового здравоохранения. **Основные результаты.** Полученные результаты заключаются в адаптации международного опыта использования протокола FHIR для российской действительности и в уточнении метода внедрения усиленной квалифицированной электронной подписи без потери пропускной способности в медицинских информационных системах. Практический результат показывает, что использование российской усиленной квалифицированной электронной подписи удовлетворяет требованиям информационной безопасности для новых медицинских информационных систем и позволяет передавать чувствительные данные без потери качества и скорости. **Обсуждение.** Сделан вывод о необходимости внедрения системного подхода к использованию российского профиля протокола FHIR RU-core для новых медицинских информационных систем с целью дальнейшего развития цифрового здравоохранения. Результаты работы могут быть ценным ресурсом для архитекторов и разработчиков программного обеспечения медицинских информационных систем, а также специалистов по информационной безопасности.

Ключевые слова

медицинские информационные системы, российский протокол FHIR, интеграция электронной подписи

Благодарности

Финансирование выполнено за счет средств научно-исследовательской работы «Автономные интеллектуальные системы» № 623106 в Университете ИТМО.

Ссылка для цитирования: Горбунов Н.А., Кулешова В.О., Коржук В.М. Интеграция усиленной квалифицированной электронной подписи с ресурсами быстрого взаимодействия в сфере здравоохранения FHIR RU-core // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 2. С. 311–320 (на англ. яз.). doi: 10.17586/2226-1494-2025-25-2-311-320

Introduction

Public and private Medical Information Systems (MIS) are forced to constantly transfer large volumes of private information, namely personal data[1]. The source [1] has confirmed how to generate a list of personal data processed in MIS. When discussing the transfer of medical data, it is important to emphasize the importance of the Fast Healthcare Interoperability Resources (FHIR) protocol. In digital health, the exchange of medical information and the interoperability of healthcare resources can be achieved through the use of the standard protocol FHIR according to [2].

[1] Федеральный закон России № 152 от 27.07.2006 «О персональных данных». Federal Law of Russia no. 152 at 27.07.2006 “About personal data”.

One of the well-known companies in Russia engaged in secure integration for MIS in the Information Technology (IT) sector is "Netrika Medicine". In fact, this company is a Russian IT solution provider and developer. It is involved in developing web portals that are compliant with the latest FHIR standards. The company facilitates access for doctors and medical institution workers in Russian regions to an integrated electronic medical record[1]. Many new tools for practical work have been developed by doctors who work in private and public medical organizations, clinics, and diagnostic centers. MIS is where these tools are utilized to achieve new goals and issues. User web portals enable a significant increase in the speed and accuracy of disease diagnosis as well as facilitating doctor-patient interactions. Patients are no longer required to collect certificates, extracts, test data, ultrasound, etc. before receiving advisory or medical assistance due to this fact, which greatly simplifies their lives.

During the project, the specialists at "Netrika Medicine" solved multiple problems. Electronic versions of medical documents can be obtained from MIS used in healthcare institutions and provided to doctors in other institutions through a graphical interface. In addition, the system statistical indicators were expanded by significantly enhancing the databases.

When creating the interaction between web portals and the integrated electronic medical record module, the initial focus was on the development of various types of MIS. To utilize this opportunity, FHIR was selected as the most advanced standard for exchanging medical data[2]. Health Level Seven International is working on the development of the FHIR protocol.

The Table 1 below shows how the FHIR protocol has been utilized in previous scientific works.

The FHIR protocol global significance lies in its ability to enhance the interaction between diverse health systems. This allows MISs, which are developed by non-cooperative corporations, to effectively cooperate, share data, and interpret general information.

It is important to emphasize the ideological similarities of the decisions when comparing the integration of Enhanced Qualified Electronic Signature (EQES) with FHIR RU-core and existing solutions in the United States of America (USA). The algorithm GOST R 34.10-2012[3] is the sole distinguishing factor of EQES which is applicable to MISs operating in Russia. MISs operating in the US employ the Digital Signature Standard algorithm in the EQES. The main similarity of EQES integration with Russian and American MISs is in the introduction of EQES into the structure of the FHIR protocol. The aim of this integration is unambiguous identification of authorship as well as confirmation of the integrity of the signed data.

The FHIR standard-based MIS types and properties vary among the sources presented in the Table 1. However, they demonstrate the consistency and necessity of utilizing a universal FHIR protocol in any MIS. After analyzing six articles on the FHIR protocol, we have determined that it is used in all MIS. Moreover, FHIR protocol universality and user-friendliness make it convenient for MIS developers. It serves as a basis for further research on the idea of utilizing its Russian version.

By using FHIR, interaction with various MIS can be completely unified. This fact allows for the storage of an integrated electronic medical record through a specific

Table 1. Implementation of the FHIR protocol

Study title	Research feature
FHIR profile-based patient decision aid system [3]	It uses the FHIR standard for semantic compatibility with different systems
FHIR profile-based patient decision support system [4]	It uses the FHIR standard to create a decision support MIS for patients
FHIR medical data management platform [5]	It uses the FHIR standard to provide clinical decision support
FHIR profile-based model for collecting clinical study data [6]	It uses the FHIR standard to achieve interoperability of metadata and clinical trial data
FHIR profile-based pharmacogenomics clinical decision support service [7]	It uses the FHIR standard to combine pharmacogenomics clinical decision support service with clinical decision support system
FHIR profile-based practice guidelines [8]	It uses the FHIR standard to improve practice guidelines through the use of patient-specific recommendations
FHIR profile-based approach to clinical decision support system integration in critical care [9]	It describes the experiences of nurses and doctors using a FHIR profile-based clinical decision support system

[1] Программные продукты ООО «Нетрика Медицина» [Электронный ресурс]. URL: https://n3med.ru/ (дата обращения: 20.05.2024). Software products of the company "Netrika Medicine", URL: https://n3med.ru (accessed: 20.05.2024).

[2] Рыжиков М. Введение в HL7 FHIR. EverCare. 2016 [Электронный ресурс]. URL: https://evercare.ru/vvedenie-v-hl7-fhir (дата обращения: 20.05.2024). Ryzhikov M. Introduction to HL7 FHIR. EverCare. 2016. URL: https://evercare.ru/vvedenie-v-hl7-fhir (accessed: 20.05.2024).

[3] Национальный стандарт РФ ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». National standard of the Russian Federation GOST R 34.10-2012 "Information technology. Cryptographic protection of information. Electronic digital signature generation and verification processes".

web portal and also directly from any medical institution information system.

EQES meets the security requirements because it provides the highest level of protection and legal significance. This is identical to a handwritten signature. EQES is used to transmit confidential information to banks, courts, tax authorities, medical institutions, and other organizations with strict security requirements. This is confirmed by the fact that only accredited certifying centers are entitled to create EQES certificates. The format and storage of EQES keys require additional requirements. The organization EQES private key must be written to a token that is held solely by the owner. Cryptographic means are utilized to create EQES, which confirms authorship and document integrity without the need for additional agreements between the parties. It is widely accepted that the EQES is a universal tool for electronic document processing worldwide.

Synchronization using two cryptographic transformation principles can make integration compatibility with international health systems possible.

The FHIR RU-core protocol is the model used by the Russian Federation for transferring sensitive personal data in healthcare[1]. The interaction of information systems in Russian healthcare requires unified understanding of data which it serves as a basis for.

Method

The article aims to develop a distinctive approach for utilizing Russian EQES in the FHIR RU-core protocol when constructing MISs to expand integration capabilities[2].

This goal requires the integration of cryptographic information protection tools in the Russian national standard for exchanging medical records among MISs. The integration task has arisen because the Russian version of the FHIR protocol utilizes domestic cryptographic information protection tools in a distinct manner. This scientific article was created through the use of logical inference, system analysis, search and cognition, and methodological design.

The research uniqueness lies in its method for integrating EQES into the FHIR RU-core protocol which will enable data exchange in various MISs. Transferring manipulations that were previously unused in the FHIR protocol for MIS is now possible thanks to this new method. The use of cryptographic information protection tools for transferring personal data makes it unique by adhering to the general principle. However, at the same time, we emphasized the use of the Russian tools for exchanging medical records.

The relevance of the study lies in the necessity to integrate EQES certificates into the FHIR RU-core framework. Systematic work resulted in the standardization of indicators for the use of the Russian profile of the FHIR RU-core protocol in a new MIS created to implement new functionality.

Using the inalienability principle of the organization component and production needs, the FHIR RU-core protocol was incorporated into MIS that is currently deployed in several data processing centers certified for various information security requirements [10].

It becomes possible due to the Russian version of the tool for exchanging medical records meeting the following information security requirements:

- Government decree on the protection of personal data[3];
- Order of the Federal Service for Technical and Export Control of the Russian Federation regarding the protection of information in state information systems[4];
- Government decree on the categorization of critical information infrastructure facilities in the Russian Federation[5].

Scientific articles on healthcare MIS confirmed the advantages of adding EQES to the FHIR RU-core protocol, indicating that MIS without EQES is not very useful [11]. The MIS subsystems are continuously being developed, which includes updating the list of information security requirements [12]. The development of various MIS resulted in the need to establish a coordinated data exchange protocol. In Russia, the FHIR RU-core standard is the most advanced and developed tool for MIS. Both, MIS software developers and representatives from the medical industry are interested in this standard. This protocol is a necessary addition to the system of medical standards. In fact, HL7 FHIR is currently the only standard with a large professional community and a profound comprehension of medical records. Its primary advantage is a resource diagram that is well-designed to describe all required entities including patients and doctors, immunizations, treatment plans, etc.

[1] Манифест FHIR Ru. FHIR RU-core [Электронный ресурс]. URL: https://fhirru.github.io/core/docs/manifest/basic.html. (дата обращения: 20.05.2024). Manifesto FHIR Ru. FHIR RU-core, URL: https://fhirru.github.io/core/docs/manifest/basic.html (accessed: 20.05.2024).

[2] Федеральный закон России № 63 от 06.04.2011 «Об электронной подписи». Federal Law of Russia No. 63 at 04.06.2011 “About electronic signature”.

[3] Постановление Правительства России от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных». Decree of the government of Russia No. 1119 at 11.01.2012 “About approval of requirements for the protection of personal data during their processing in personal data information systems”.

[4] Приказ ФСТЭК России от 02.11.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Order of the FSTEC of Russia at 11.02.2013 No. 17 “About approval of the requirements for the protection of information that does not constitute a state secret contained in state information systems”.

[5] Постановление Правительства России № 127 от 08.02.2018 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». Decree of the government of Russia No. 127 at 02.08.2018 “About approval of the rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as the list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values”.

At the regional level, HL7 standard of FHIR RU-core has already been implemented by almost all leading medical system developers in one or another of their solutions for MIS. The research examines the possibility of implementing the FHIR RU-core protocol in the MIS of "Netrika Medicine" to address new challenges and demands. The "Netrika Medicine" software currently has multiple components, including laboratory and instrumental tests, prescriptions, telemedicine consultations, various types of appointments, but the most significant one is the secure integration of MIS. The software has been successfully used in over 20 regions in Russia.

One of the research tasks is to assist the medical community in attaining long term goals for the digitalization of healthcare. Our method is primarily focused on the safe integration of medical information systems and the development of regional services for doctors, patients and healthcare providers. It is necessary to resolve the contradiction between the level of technological development and the problem of developing a scientific and methodological apparatus.

The Russian EQES was utilized to ensure safe integration with the state unified healthcare system[1]. MIS components were responsible for the functions and structures of services of Federal Register of Medical Organizations (FRMO)[2], federal register of medical workers[3], which were posted on the portal for the operational interaction with participants. The implementation of these components involved using enhanced EQES for information interaction.

The implementation of information interaction with the FRMO subsystem has been achieved through the use of CryptoPro Cryptographic Service Provider (CSP) and EQES. If an EQES certificate is available, the following data about medical organizations will be transmitted:

- obtaining basic information about a medical organization;
- obtaining information about buildings;
- obtaining a range of divisions and departments of a medical organization;
- obtaining information about the staffing schedules of a medical organization;
- obtaining information about the medical equipment of a medical organization;
- obtaining information about mobile units;
- obtaining information about households.

The innovation of the method lies in the introduction of a certificate into the FHIR RU-core protocol. Previously, these solutions were not used due to the need to adapt the domestic FHIR protocol to the method.

The EQES integration improves the system by promoting digitalization of healthcare. Doctors and MIS owners are able to obtain information about patients, their stories of diseases, treatment methods, and other information in a quick and qualitative manner. The management of departments and healthcare facilities can enhance their control over staff performance. EQES enhances data storage security by protecting it from unauthorized access, modification and destruction.

The software code for EQES integration into MIS required the creation of a function that connected a cryptographic information protection tool — CryptoPro CSP and the use of an EQES certificate to uniquely identify authorship and ensure the integrity of transmitted data.

Generating and sending an Object Identifier (OID) to the FRMO using a certificate and the GOST algorithm is the main aspect of the method. The method can be schematically presented in the form of an algorithm, where I means the counter required to set the limit of password submission attempts. The limit is three. The algorithm is presented in Fig. 1. If you enter a PIN code

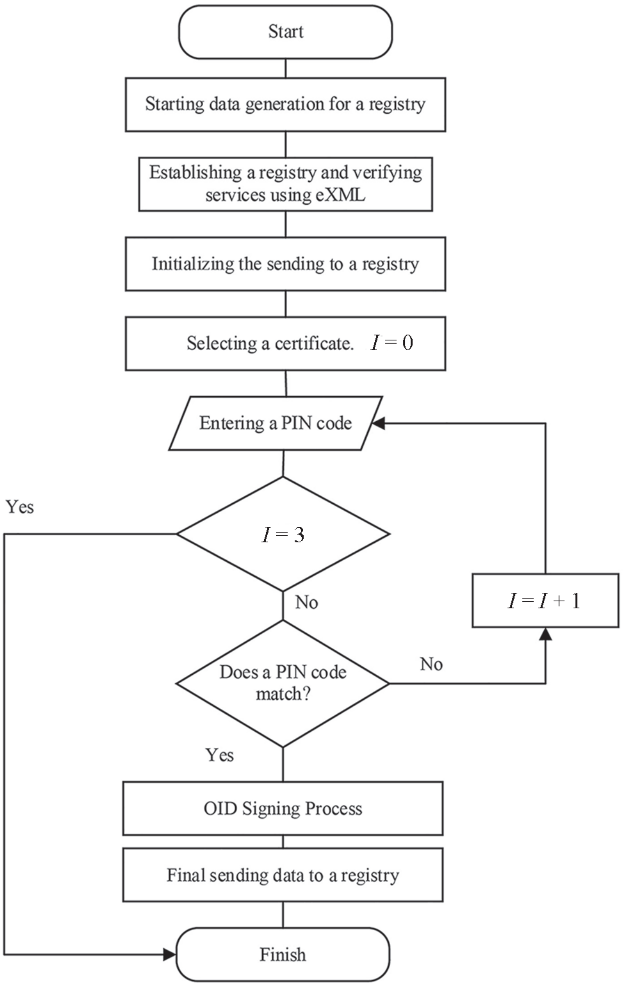
Start
Starting data generation for a registry
Establishing a registry and verifying services using eXML
Initializing the sending to a registry
Selecting a certificate. $I = 0$
Entering a PIN code
Yes
$I = 3$
No
$I = I + 1$
Does a PIN code match?
No
Yes
OID Signing Process
Final sending data to a registry
Finish

Fig. 1. Algorithm of signing with EQES data for sending to a medical organization

[1] Единая государственная информационная система в сфере здравоохранения [Электронный ресурс]. URL: https://egisz.rosminzdrav.ru/#firstPag (дата обращения: 20.05.2024). Unified state information system in the field of healthcare, URL: https://egisz.rosminzdrav.ru/#firstPag (accessed: 20.05.2024).

[2] Федеральный регистр медицинских работников [Электронный ресурс]. URL: https://portal.egisz.rosminzdrav.ru/materials/4133 (дата обращения: 20.05.2024). Federal register of medical organizations, URL: https://portal.egisz.rosminzdrav.ru/materials/4133 (accessed: 20.05.2024).

[3] Федеральный регистр медицинских работников [Электронный ресурс]. URL: https://portal.egisz.rosminzdrav.ru/materials/4135 (дата обращения: 20.05.2024). Federal register of medical workers, URL: https://portal.egisz.rosminzdrav.ru/materials/4135 (accessed: 20.05.2024).

three times in a row incorrectly, the use of the EQES will be suspended until unlocked.

Documents must be signed to upload information about medical workers and institutions to the federal services. Cryptographic Message Syntax format is required for the signature to be EQES. EQES should be formed using the algorithms of GOST R 34.10-2012. Before FHIR RU-core is implemented, it is important to create separate files for the signatures of medical professionals and organizations (each electronic signature must correspond to a separate file).

The limited validity of signature certificates is a potential cause of difficulties with using EQES. The closed key is valid for one year. Due to the current demographic situation, there is a severe shortage of IT specialists in the field, which could make it challenging to support and maintain the EQES.

Automated complex debugging testing was performed by generating and sending the object identification to the FRMO using the certificate and algorithm of GOST R 34.10-2012.

When discussing the quality of data transmission, it is important to emphasize that EQES, which is part of the FHIR RU-core structure, ensures the integrity of transmitted data. The speed is significantly faster than manual processing. Without using EQES as part of the FHIR RU-core structure, scalability in actual health applications is not achievable due to the absence of legally legitimate EQES analogues. The process of integrating EQES into the FHIR RU-core structure may require further development after being certified by the quantum cryptographic regulator.

Software implementation

Information interaction is ensured using cryptographic measures of information security in the developed program code[1]. EQES certificates provide:

- formation of a qualified electronic signature using GOST R 34.10-2012 algorithms;
- verification of a qualified electronic signature using GOST R 34.10-2012 algorithms.

Thus, the Russian EQES implemented in the HL7 FHIR RU-core protocol meets information security requirements. The unique source process is presented below.

After entering the Internet portal, the user was redirected to a URL generated on the portal side. The URL contains the following data:

- *client_id* — the identifier of the client system (mnemonic of the Unified Identification and Automation System (UIAS) indicated in capital letters);
- *client_secret* — the request signature in Public-Key Cryptographic System #7 (PKCS#7) detached signature format. In UTF-8 encoding from the values of four HTTP request parameters: scope, timestamp, clientId, and state (without delimiters). <*client_secret*> must be encoded base64 URL safely. The certificate used to verify the signature must be pre-registered in the UIAS and linked to the health committee of the client system in the UIAS. UIAS uses certificates in the X.509 format and interacts with the algorithms for generating an electronic signature and cryptographic hashing using GOST R 34.10-2012 and GOST R 34.11-2012[2];
- *redirect_uri* — the link that the user is directed to after being given permission to access the resource;
- *scope* — access area, i.e., rights requested. For example, if a client system requests access to information about employees of an organization, then the access scope should be as in http://esia.gosuslugi.ru/org_emps with the necessary parameters. If the access scope id_doc (user data) is requested, then there is no need to specify the OID of this user as a parameter;
- *response_type* is the type of response that is expected from the UIAS, and it has a value code if the client system needs to receive an authorization code;
- *state* — a 128-bit request identifier that is randomly generated and meets the universally unique identifier standard to prevent interceptions;
- *timestamp* — the time of the authorization code request in the format yyyy.MM.dd HH:mm:ss Z (for example, 2013.01.25 14:36:11 +0400), it is necessary to record the beginning of the time period during which the request with this data is a valid identifier (<*state*>);
- *access_type* takes the value “offline” if access to resources is required and when the owner cannot be called (in this case, a refresh token is issued). The value is “online” — access is required only if the owner is present.

The program structure for implementing EQES into the FHIR RU-core protocol is presented above. Since the integration platform was created with C Sharp (C#), the programming language choice was predetermined.

Below is an example of obtaining a list of medical organizations that are available. Request type: POST. Listing 1 and 2 show the request and the generated response.

Listing 1. Request

```
URL-запроса: [base]/term/ValueSet/$expand?_
format=json
Header: Authorization: [GUID-токен]
BODY-запроса:
{"resourceType": "Parameters",
    "parameter": [{
        "name": "system",
```

[1] Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». Order of the FSB of Russia at 10.07.2014 No. 378 “About approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems using cryptographic information protection tools necessary to fulfill the requirements established by the government of the Russian Federation personal data protection for each security level”.

[2] Национальный стандарт РФ ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования». National standard of the Russian Federation GOST R 34.11-2012 “Information technology. Cryptographic data security. Hash function”.

```
        “valueString”:”urn:o
id:1.2.643.2.69.1.1.1.84.2”
    }
   ]
}
```

Listing 2. Response

```
{
    “parameter”:[{
        “name”: “return”,
        “resource”: {
            “id”: “0da121d9-eeb4-4695-9b3a-
            cb64c3fe9b4a”,
            “url”: “urn:o
id:1.2.643.2.69.1.1.1.84.2”,
            “meta”: {
                “versionId”: “0e277f6e-
                ed52-405a-afd6-
                5683a19b7b8c”,
                «lastUpdated»: «2024-05-
                28T11:02:16.547447+03:00»
            },
            «name»: «Медицинские работники
            медицинских организаций»,
            “status”: “active”,
            “contact”: [{
                “telecom”: [{
                    “value”: “”,
                    «system»: «email»
                }]
            }],
            «version»: «0»,
            «expansion»: {
                «contains»: [{
                    «code»: «1.2.643.5.1.13
                    .13.12.2.78.8000»,
                    «display»: «СПб ГБУЗ
                    \»Стом. пол. №11\””,
                    “version”: “0”,
                    “contains”: [{
                        “code”: “mr”,
                        “display”: “Создано
                        записей: 2”
                    }]
                }],
                “parameter”: [{
                    “name”: “total”,
                    “valueString”: “1”
                }],
                “timestamp”: “2024-05-
                28T14:04:25.07663+03:00”
            },
            “publisher”: “”,
            “experimental”: true,
            “resourceType”: “ValueSet”
        }
    }],
    “resourceType”: “Parameters”
}
```

The received response means that a Medical Organization (MO) is available to the user from OID 1.2.643.5.1.13.13.12.2.78.8000.

Experimental study

The ‘Experimental study’ includes information about the experiment. The characteristics of the test stand are given in relation to the computer system and the software used. Table 2 presents the steps.

“Netrika Medicine”, an IT company that operates in over twenty regions of our country, created the first real example of using the FHIR protocol in health care. In particular, these are such software products as Access Management System, Patient Flow Management, Telemedicine, Patient Portal, and Integrated Electronic Medical Card.

The benchmarks are presented in this section: Case No. 1, Case No. 2, Case No. 3.

The experiment is described in the process of updating information in the Regional Segment (RS) of the FRMO. Table 2 presents the experimental steps.

The experiment requires logistics support.

The experiment should be carried out on personal computers with the following indicators:

- Intel Celeron Processor G1850 2.90 GHz or comparable;
- RAM volume should not be less than 4 GB;
- disk subsystem should not be lower than 80 GB;
- network adapter with at least 100 Mbit;
- Windows 10 and higher, MacOS X 10.10 and higher;
- Google Chrome browser, version 45.0 and higher;
- Google Chrome Advanced REST Client browser plugin with URL version 7.43 and higher;
- CryptoPRO EQES Browser Plug-in;
- CryptoPRO CSP software version 5.00.

The following test cases were used:

Test case No. 1. Medical Organization Data

OID MO: 1.2.643.5.1.13.13.12.2.41.3842

Name of MO: “Kamchatka MO”

Test case No. 2. Obtaining Complete Data of a MO

Request type: GET

URL: [base]/fhir/term/get_resource?_format=json&system=1.2.643.2.69.1.1.1.86.2&code=1.2.643.5.1.13.13.12.2.41.3842

Test case No. 3. Updating MO Data in Register of Medical Organizations (RMO) with Data from FRMO. New Division of the MO

OID MO: 1.2.643.5.1.13.13.12.2.41.3842

Name: Outpatient department

Type of unit: Outpatient

Type of unit: Outpatient clinics (including mobile ones)

Buildings and premises: <arbitrary buildings and premises>

Scheduled visits per shift (Total number): 33

Attached Residents (Total Number): 300

Form of medical care: Planned

Conditions for providing medical care: Outpatient

Medical services provided by the unit: <voluntary services>

Updating the information of the RS FRMO with the data from FRMO Uniform State Health Information System (USHIS) is presented in Table 2.

Table 2. The experimental steps

No	Steps	Results
1	Open the RS FRMO directory, OID 1.2.643.2.69.1.1.1.86.2. Find an MO from test case No. 1. Open a directory entry to view details	In the graphical user interface of the reference data in directory 1.2.643.2.69.1.1.1.86.2, in the MO data from the test case No. 1, there is no data about the department from the test case No. 3
2	Check if the structure of the medical organization contains the unit from test case No. 3. Execute the request from test case No. 2 in the mail application	In the resulting JSON object of the MO, obtained as a result of executing the request of test case No. 2, in the “departs” information block there is no data about the department from test case No. 3
3	Add a new division to the federal system FRMO USHIS for Moscow Region from test case No. 1: ➢ Log in to the system. ➢ Open the MO card from the test case. ➢ Add a new department for the ministry using data from test case No. 3	The department from test case No. 3 is successfully created in the USHIS 2.0
4	Start the process of obtaining data from the FRMO: ➢ Launch and log in to the web application “FRMO”. ➢ Set parameters for synchronization from test case No. 3 and begin the process of synchronization. ➢ Wait for the data acquisition process to complete and the process status changes from “saving result” to “stopped”	The process of updating MO data from test case No. 1 is successfully launched and completed
5	Access the regulatory reference information web application. Open the RS FRMO directory, OID 1.2.643.2.69.1.1.1.86.2	In the graphical user interface of the reference data in directory 1.2.643.2.69.1.1.1.86.2, the MO data from test case No. 1 contains data about the new unit
6	Find a medical organization with an OID from test case No. 1. Open the directory entry to view details. Find the latest uploaded information. Check if the structure of the medical organization contains the unit from test case No. 3. Execute the request from test case No. 2 in a mail application	In the resulting JSON object obtained as a result of executing the request of test case No. 2, the information block “departs” contains data about new department

The experiment is run as Administrator. Role: Administrator. Updating the data of MO in the RMO with data from the FRMO: adding a unit.

Results

The MIS of “Netrika Medicine” is a real illustration of how cryptographic information security can be integrated into the HL7 FHIR RU-core protocol. The “integration platform”, “patient flow management”, “access management system”, “telemedicine”, “unified electronic medical card”, and “patient portal” have been deployed in more than 20 regions of the Russian Federation. A quantitative analysis is done to determine the rapid increase in MIS interactions through an integration platform. Starting from 2020, there has been a significant annual increase in the number of MIS operating on the HL7 FHIR RU-core standard. This rapid increase is shown in Fig. 2.

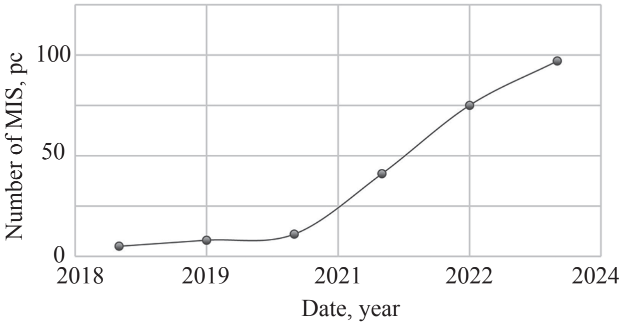

Fig. 2. A graph showing the annual increase in the number of MIS

Discussion

Practical suggestions for integrating EQES into the HL7 FHIR RU-core standard incorporate the design of a protected MIS. Furthermore, the types of certificates were identified and the necessity for additional information security measures when processing personal data was presented [13].

Moreover, FHIR RU-core is the only standard that is currently popular and has a large professional that is well-versed in medical records description. The key advantage is a clearly thought-out resource structure that enables to describe all the necessary entities: from patients and doctors to immunizations, treatment plans, etc. By combining the same resources in different ways, it is possible to create descriptions of completely different processes using the EQES certificate implemented in FHIR as if they were building blocks.

Limited funding for medical facilities is a potential limitation, as CryptoPRO CSP and EQES certificates will require extra costs. These restrictions are not a significant threat since data transfer to the ‘Unified Public Health System’ is currently mandatory.

Compatibility of the domestic and international versions of FHIR protocol in MIS is possible. To achieve this, it is necessary to acknowledge the initial structures and synchronize goals and objectives in the development of MIS.

Conclusion

The Russian Fast Healthcare Interoperability Resources (FHIR) community has existed for several years. During this time, many important decisions were made. The development of community-created content is currently underway. It is now possible to apply certain advancements. For example, a patient's card makes it possible to integrate Medical Information Systems (MIS) created by different vendors. Commercial companies that support the community and invest both financially and with expertise will have a positive impact on the speed with which all decisions and materials are described, worked out, and recorded. The Russian HL7 FHIR RU-core is faster, but requires appropriate legislation to be available everywhere.

FHIR is the only standard that has detailed descriptions of medical records. In 80 % of cases, the FHIR knowledge base satisfies Russian medical regulatory requirements and health care practitioners. There is a lack of global unifying motive for practical synchronization, which may prevent the Russian and international versions of different companies from being harmonized.

The security of Enhanced Qualified Electronic Signature integration into the FHIR structure is confirmed by the author's identification and ensuring the integrity of the information.

This should become a strong basis for the further digitalization of medicine in Russia.

In conclusion, it is crucial to emphasize that the materials that describe the systematization of the Russian FHIR RU-core protocol for new MIS have been validated for their novelty, relevance, methodological, and practical value. Thus, when developing MIS with new functionality, it is necessary to use the innovations presented in this article.

References

1. Gorbunov N., Kuleshova V., Korzhuk V. Personal data processed in medical information systems. *International Research Journal*, 2023, no. 9 (135), pp. 10. (in Russian). https://doi.org/10.23670/IRJ.2023.135.3
2. Mikhailenko O.V., Staykov G.B., Dorrer G.A. Using the fast healthcare interoperability resources health information exchange standard in digital healthcare. *ITNOU*, 2021, no. 1 (17), pp. 43–49. (in Russian). https://doi.org/10.47501/ITNOU.2021.1.043-049
3. Semenov I., Kopanitsa G., Denisov D., Yakovenko A., Osenev R., Andreychuk Y. Patients decision aid system based on FHIR profiles. *Journal of Medical Systems*, 2018, vol. 42, no. 9, pp. 166. https://doi.org/10.1007/s10916-018-1016-4
4. Semenov I., Kopanitsa G. Decision support system based on FHIR profiles. *Studies in Health Technology and Informatics*, 2018, vol. 249, pp. 117–121. https://doi.org/10.3233/978-1-61499-868-6-117
5. Semenov I., Osenev R., Gerasimov S., Kopanitsa G., Denisov D., Andreychuk Y. Experience in developing an FHIR medical data management platform to provide clinical decision support. *International Journal of Environmental Research and Public Health*, 2019, vol. 17, no. 1, pp. 73. https://doi.org/10.3390/ijerph17010073
6. Leroux H., Metke-Jimenez A., Lawley M.J. Towards achieving semantic interoperability of clinical study data with FHIR. *Journal of Biomedical Semantics*, 2017, vol. 8, pp. 41. https://doi.org/10.1186/s13326-017-0148-7
7. Dolin R.H., Boxwala A., Shalaby J. A Pharmacogenomics Clinical Decision Support service based on FHIR and CDS Hooks. *Methods of Information in Medicine*, 2018, vol. 57 (S 02), pp. e115–e123. https://doi.org/10.1055/s-0038-1676466
8. Owens D.K. Improving practice guidelines with patient-specific recommendations. *Annals of Internal Medicine*, 2011, vol. 154, no. 9. pp. 638–639. https://doi.org/10.7326/0003-4819-154-9-201105030-00010
9. Weber S., Crago E.A., Sherwood P.R., Smith T. Practitioner approaches to the integration of clinical decision support system technology in critical care. *The Journal of Nursing Administration*, 2009, vol. 39, no. 11, pp. 465–469. https://doi.org/10.1097/NNA.0b013e3181bd5fc2
10. Gorbunov N., Kuleshova V., Korzhuk V. Organizational and law aspects of medical information systems. *International Research Journal*, 2024, no. 4 (142), pp. 11. https://doi.org/10.23670/IRJ.2024.142.38
11. Vaganova E.V. Hospital information systems as the object of evaluation: factors and development tendencies. *Tomsk State University Journal of Economics*, 2017, no. 37, pp. 113–130. (in Russian). https://doi.org/10.17223/19988648/37/9

Литература

1. Горбунов Н.А., Кулешова В.О., Коржук В.М. Персональные данные, обрабатываемые в медицинских информационных системах // Международный научно-исследовательский журнал. 2023. № 9 (135). С. 10. https://doi.org/10.23670/IRJ.2023.135.3
2. Михайленко О.В., Стайков Г.Б., Доррер Г.А. Использование стандарта обмена медицинской информацией fast healthcare interoperability resources в цифровом здравоохранении // ИТНОУ: Информационные технологии в науке, образовании и управлении. 2021. № 1. С. 43–49. https://doi.org/10.47501/ITNOU.2021.1.043-049
3. Semenov I., Kopanitsa G., Denisov D., Yakovenko A., Osenev R., Andreychuk Y. Patients decision aid system based on FHIR profiles // Journal of Medical Systems. 2018. V. 42. N 9. P. 166. https://doi.org/10.1007/s10916-018-1016-4
4. Semenov I., Kopanitsa G. Decision support system based on FHIR profiles // Studies in Health Technology and Informatics. 2018. V. 249. P. 117–121. https://doi.org/10.3233/978-1-61499-868-6-117
5. Semenov I., Osenev R., Gerasimov S., Kopanitsa G., Denisov D., Andreychuk Y. Experience in developing an FHIR medical data management platform to provide clinical decision support // International Journal of Environmental Research and Public Health. 2019. V. 17. N 1. P. 73. https://doi.org/10.3390/ijerph17010073
6. Leroux H., Metke-Jimenez A., Lawley M.J. Towards achieving semantic interoperability of clinical study data with FHIR // Journal of Biomedical Semantics. 2017. V. 8. P. 41. https://doi.org/10.1186/s13326-017-0148-7
7. Dolin R.H., Boxwala A., Shalaby J. A Pharmacogenomics Clinical Decision Support service based on FHIR and CDS Hooks // Methods of Information in Medicine. 2018. V. 57 (S 02). P. e115–e123. https://doi.org/10.1055/s-0038-1676466
8. Owens D.K. Improving practice guidelines with patient-specific recommendations // Annals of Internal Medicine. 2011. V. 154. N 9. P. 638–639. https://doi.org/10.7326/0003-4819-154-9-201105030-00010
9. Weber S., Crago E.A., Sherwood P.R., Smith T. Practitioner approaches to the integration of clinical decision support system technology in critical care // The Journal of Nursing Administration. 2009. V. 39. N 11. P. 465–469. https://doi.org/10.1097/NNA.0b013e3181bd5fc2
10. Gorbunov N., Kuleshova V., Korzhuk V. Organizational and law aspects of medical information systems // International Research Journal. 2024. N 4 (142). P. 11. https://doi.org/10.23670/IRJ.2024.142.38
11. Ваганова Е.В. Медицинские информационные системы как объект оценки: факторы и тенденции развития // Вестник Томского государственного университета. Экономика. 2017. № 37. С. 113–130. https://doi.org/10.17223/19988648/37/9

12. Mavlyanova L.T. Protection of information on the Internet. *Oriental Renaissance: Innovative, Educational, Natural and Social Sciences*, 2022, vol. 2, no. 1, pp. 568–575. (in Russian)
13. Alsafwani N., Fazea Y., Alnajjar F. Strategic approaches in network communication and information security risk assessment. *Information*, 2024, vol. 15, no. 6, pp. 353. https://doi.org/10.3390/info15060353

Authors

Nikolai A. Gorbunov — Head of Department, “Netrika Medicine” LLC, Saint Petersburg, 191015, Russian Federation; PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0009-0004-2973-9594, gorb-2157@mail.ru

Valeria O. Kuleshova — PhD (Philology), CSRI Elektropribor, Saint Petersburg, 197046, Russian Federation, https://orcid.org/0000-0003-1377-6003, valeria.kuleshova@yahoo.com

Viktoriia M. Korzhuk — PhD, Associate Professor, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, sc 56875395200, https://orcid.org/0000-0002-0240-9067, vmkorzhuk@itmo.ru

Received 20.06.2024
Approved after reviewing 21.01.2025
Accepted 18.03.2025

12. Мавлянова Л.Т. Защита информации в интернет // Oriental Renaissance: Innovative, Educational, Natural and Social Sciences. 2022. V. 2. N 1. C. 568–575.
13. Alsafwani N., Fazea Y., Alnajjar F. Strategic approaches in network communication and information security risk assessment // Information. 2024. V. 15. N 6. P. 353. https://doi.org/10.3390/info15060353

Авторы

Горбунов Николай Александрович — руководитель отдела, ООО «Нетрика Медицина», Санкт-Петербург, 191015, Российская Федерация; аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0009-0004-2973-9594, gorb-2157@mail.ru

Кулешова Валерия Олеговна — кандидат филологических наук, преподаватель, АО «Концерн «ЦНИИ «Электроприбор», Санкт-Петербург, 197046, Российская Федерация, https://orcid.org/0000-0003-1377-6003, valeria.kuleshova@yahoo.com

Коржук Виктория Михайловна — кандидат технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sc 56875395200, https://orcid.org/0000-0002-0240-9067, vmkorzhuk@itmo.ru

Статья поступила в редакцию 20.06.2024
Одобрена после рецензирования 21.01.2025
Принята к печати 18.03.2025