

Digital Medication Prescription System with JSON

Liverson Paulo Furtado Severo^a and Jean Everson Martina^b

Department of Informatics and Statistics, Federal University of Santa Catarina, Florianópolis, Santa Catarina, Brazil

Keywords: JSON, JWS, FHIR, JAdES, Signature, Interoperability.

Abstract: The rapid evolution of digital health solutions, accelerated by the COVID-19 pandemic, highlighted the necessity for secure and efficient electronic prescription and medication dispensing systems. This paper presents a study on integrating HL7 FHIR standards and JAdES signatures to facilitate the digitalization of healthcare documentation. By addressing key challenges such as interoperability, data volatility, and security, the research proposes a framework that ensures the authenticity and integrity of electronic prescriptions—Emphasizing the importance of self-contained digital documents that eliminate reliance on external references to enhance the reliability of health information exchange in Brazil. Furthermore, it outlines the legal implications of electronic signatures in Brazil, advocating for compliance with national standards to ensure the legal validity of digital prescriptions. The findings indicate that the proposed solutions not only streamline healthcare processes but also foster a gradual transition from traditional paper-based systems to a robust digital infrastructure, ultimately improving patient care and operational efficiency in the healthcare sector.

1 INTRODUCTION

Like the rest of the world, Brazil faced a significant health crisis due to the COVID-19 pandemic. This situation accelerated the adoption of electronic medical documents and their digital processing (Conselho Federal de Medicina, 2021). Brazilian law states these documents can be electronically signed with legal validity. However, qualified electronic signatures are mandatory for special control prescriptions and medical certificates (Presidência da República do Brasil, 2020).


Currently, in Brazil, prescriptions and medication dispensing are issued through printed documents with a handwritten signature, and dispensing is done all at once. This system is inflexible to the patient and has security issues related to falsification, problems with prescription legibility, and lack of traceability.


The aim is to transform this process by using digital technologies and introducing a new concept of partial dispensing, where patients can access medications gradually based on their needs. Electronic signatures represent a crucial step in facilitating the flow of digital documents, making it easier to share information, streamline bureaucratic processes, and enhance storage solutions.

Electronic signatures are a way to authenticate and validate documents digitally using tools specifically developed for this purpose. There are three categories of electronic signatures. The simple electronic signature is similar to traditional signatures made on paper. The advanced electronic signature employs cryptographic algorithms to ensure the signature cannot be forged. Finally, the qualified electronic signature is used in more specific contexts, incorporating time-stamping and offering greater robustness. These categories serve different needs and levels of security in the digital signing process.

Electronic signatures can be categorized as embedded or detached. Embedded signatures are integrated with the document, resulting in a single signed document. In contrast, detached signatures separate the document and the signature into two files. These two components demonstrate that the signature is valid when submitted for validation.

Qualified signatures are advanced signatures created using a qualified signature creation device based on certification qualifications for electronic signatures (European Parliament and Council of the European Union, 2014). In Brazil, a qualified signature complies with the terms outlined in Law No. 14,063 regarding qualified signatures (Presidência da República do Brasil, 2020).

^a  <https://orcid.org/0009-0006-3962-8593>

^b  <https://orcid.org/0000-0003-4104-1741>

This framework has paved the way for the evolution of signatures in the health sector; however, there are still potential improvements to be addressed. One area that requires enhancement is the interoperability of signed patient documents, as there is currently no standardization to facilitate information exchange between different healthcare institutions. To address the issue of data interoperability, the National Health Data Network (RNDS) project was initiated, aimed at the digital transformation of healthcare in Brazil (Ministério da Saúde do Brasil, 2020). Interoperability can be understood as the standardization of vocabularies, data representation structures, and messaging protocols between systems. However, the development of these standards is slow, and their adoption is even slower (Roehrs et al., 2021).

The RNDS project uses the Fast Healthcare Interoperability Resources (FHIR) standard Health Level Seven International (HL7) created for data files to enhance interoperability. To enable the use of files generated in the FHIR standard, they must be transformed into digital documents, as relevant information must be self-contained for them to qualify as such. In the case of HL7 FHIR, external references for pertinent details may pertain to the healthcare provider or the patient.

Despite this, using the FHIR standard can facilitate the electronic registration and dispensing of medical prescriptions. A medical prescription document must be signed by a physician in a manner that allows for determining when the signature was made and ensures that the physician has the authorization to practice, as stipulated by the Federal Medical Council (CFM) and registered with the Regional Medical Council (CRM) of the physician (Presidência da República do Brasil, 1957).

To dispense medications, it is essential to ensure that the pharmacist is authorized to practice, as indicated by their registration with the Federal Pharmacy Council (CFF) (Presidência da República do Brasil, 1960). Therefore, during the dispensing process, a separate file is created solely for the total or partial dispensing of the prescribed medications. This file must also be signed, including information on when the signature was made.

The hypothesis is that the HL7 FHIR pattern with digital signature JAdES effectively enhances the interoperability and the security of the prescription and dispensation of medicines in Brazil, promoting a process transition from paper to robust digital infrastructure. To do that, this research looks to develop a digital system to prescribe and dispense medicines, exploring technologies such as the pattern HL7 FHIR and JAdES digital signatures. The following features:

- Allow the generation of digital prescript and its registration with support to the partial dispensation of medicines;
- Validation of documents through APIs and the implementation of a database to control the dispensation of medicines;
- Implement an interoperability and signature pattern to medical prescriptions and dispensations;
- Validation of the project in a controlled environment.

2 SIGNATURE IN DOCUMENTS IN JSON FORMAT

Despite the existence of other formats, such as XML, JSON is a simple format that provides the necessary structures for information exchange and can be self-explanatory for humans (Pohls, 2015). JSON syntax has increasingly become prevalent in electronic transactions, extending beyond just support for web tokens (JWT). As a result, the JSON Web Signature (JWS) has been defined for digital signatures (Ibarz, 2020).

2.1 JWS

According to (Jones et al., 2015), JWS represents secure content using signatures or message authentication codes (MACs) with data structures based on JSON and Base64 encoding. Three fields are used in the composition of these structures: the *JSON Object Signing and Encryption (JOSE) header*, the *JWS payload*, and the *JWS signature*.

The *JOSE header* is a JSON object that contains a description of cryptographic operations and parameters used, all compressed into header parameters. It consists of a protected *JWS header* and an unprotected *JWS header*, where the protected header includes parameters whose integrity is ensured by the *JWS signature*. In contrast, the unprotected header lacks this integrity protection. The *JWS payload* is the message that must be secured in octet format, which can be in an arbitrary sequence. The *JWS signature* is the digital signature or MAC that protects both the protected *JWS header* and the *JWS payload*.

JWS can be serialized in two forms: *JWS Compact Serialization* and *JWS JSON Serialization*. In *JWS Compact Serialization*, the unprotected header is not used; thus, the *JOSE header* and the protected *JWS header* are the same. The *JOSE header*, *JWS payload*, and *JWS signature* are concatenated as Base64-encoded strings, separated by periods. In contrast, *JWS JSON Serialization* requires at least

one of the headers mentioned above, or both, with the JOSE header representing the combination of the header information (Jones et al., 2015). Figure 1 illustrates an example of a JWS signature.

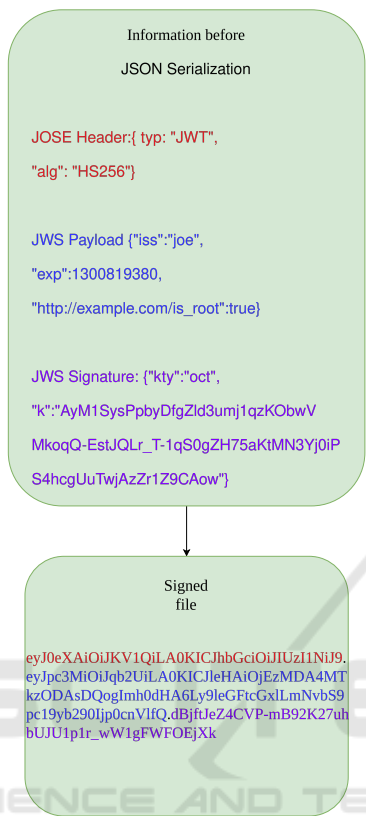


Figure 1: JWS signature example.

2.2 JAdES Signature

In 1999, the *European Telecommunications Standards Institute (ETSI)* established the *ETSI Electronic Signatures and Infrastructures Working Group*, a committee focused on developing the European standard for digital signatures and related infrastructures (Ibarz, 2020). According to (Kutyłowski and Błażkiewicz, 2023), these signatures possess the following characteristics:

- They are uniquely linked to a signer;
- They are capable of identifying the signer;
- They are created using electronic signature creation data that the signer can use exclusively and with a high level of confidentiality;
- They are connected to the signed data so that any subsequent changes will be detected.

After updates, the committee published the European standards, approved by the *National Standardization Organizations of the European Union Member*

States, which defined the family of *Advanced Electronic Signatures (AdES)* for digital signatures. The following features characterize these:

- A set of signed and unsigned attributes with a specific syntax (initially using ASN.1 dictionaries, followed by XML, PDF, and later JSON);
- Mechanisms to incorporate these attributes into the digital signature structure;
- A series of signed and unsigned attributes combinations are called levels.

In the case of basic electronic signatures, if the signing certificate expires, the signature automatically becomes invalid. To address this issue, formats allow incorporating additional information in the signature to ensure long-term validity. This information includes evidence from a third party (such as certification authorities) and time stamps in the signature to verify the status of the signature at the moment it was created (Ibarz, 2021).

In 2021, a new advanced electronic signature was created using JWS, known as JAdES. The general requirements for a JAdES signature are the components defined in the JOSE header (Ibarz, 2020). For a JAdES signature to be valid, it must not only contain the header parameters of a JWS but also include new parameters for signature qualification based on the specified level. JAdES features four classification levels that function incrementally, each designed to be used according to the application’s needs. The available levels are:

- Level B-B incorporates signed header parameters and some unsigned components within the unsigned header parameter etsiU when the signature is generated.
- Level B-T requires the generation and inclusion of a trust token that proves the signature existed at a specific date and time in an existing signature.
- Level B-LT mandates incorporating all signature validation materials into the signature document, allowing for the long-term availability of validation materials.
- Level B-LTA necessitates the inclusion of time stamps that enable the validation of the signature for extended periods after its creation, ensuring the long-term validation and integrity of the document.

The first level is the simplest to implement, requiring fewer parameters to create. Generally, this advanced signature utilizes the header parameters already defined as mandatory by the JWS signature, adds the requirement for optional JWS parameters, and introduces new parameters.

The header parameter *JWS* defines as mandatory for a signature is the Algorithm (*alg*). This parameter is protected and serves to identify the cryptographic algorithm used for the security of the *JWS*. Therefore, a *JWS* signature will be invalid if the *alg* does not contain a supported algorithm or if no associated cryptographic algorithm exists for the MAC content (Jones et al., 2015). The mandatory header parameter defined for a *JAdES* signature is the Claiming Signing Time (*sigT*). This is a protected parameter whose function is to specify the moment the signer intends to perform the signing process. Thus, the record must include a string in Coordinated Universal Time (UTC) format indicating the time of the signature.

The protected header parameter *Critical* indicates which extension parameters are used in the signature and must be processed and understood. Thus, a list that should never be empty is generated when it includes parameters that need to be processed (Jones et al., 2015). In the case of *JAdES*, the attributes eligible to be included in the *Critical* list are: *sigT*, *x5t#o*, *sigX5ts*, *srCms*, *sigPl*, *srAts*, *adoTst* and *sigPIId* (Institute, 2021). The *content type* (*cty*) header parameter is used to indicate the media type contained in the *JWS payload* of the document. This parameter is included when more than one type of object may be present in the *JWS payload*, allowing the application to use the value of this parameter to eliminate ambiguity regarding the data that may be present in the document.

The header parameters *X.509 Certificate SHA-256 Thumbprint* (*x5t#S256*), *X.509 Certificate Digest* (*x5t#o*), and *X.509 Certificates Digests* (*sigX5ts*) are protected parameters intended to indicate the *message digest* responsible for hashing the document. The *x5t#S256* was defined in *JWS* as an optional attribute and is specific for use with SHA-256. The parameters *x5t#o* and *sigX5ts* are defined by *JAdES*, where *x5t#o* is used for any hashing algorithm other than SHA-256, while *sigX5ts* is utilized when multiple certificates are used in the signature. In addition to defining the requirements for the parameters as mentioned above, the deprecation of the *X.509 Certificate SHA-1* (*x5t*) defined for *JWS* signatures is noted due to its vulnerability, making it easier to break encryption and retrieve information from the signature (Institute, 2021).

The header parameter *X.509 Certificate Chain* (*x5c*) contains the *X.509* public key certificate or the chain of certificates corresponding to the key used to sign the *JWS* digitally. Thus, *x5c* is a list of certificates represented as a *string* value in Base64 format. This parameter must be present if the parameters *x5t#S256*, *x5t#o* or *sigX5ts* are not included; other-

wise, its inclusion is optional. In addition to including protected parameters, it is possible to add unprotected parameters, which are inserted into a list of parameters called *etsi Unsigned* (*etsiU*), with all entries formatted in Base64. Table 1 shows the minimum parameters required for creating a *JAdES* document at level B-B.

Table 1: Minimum parameters needed to create a *JAdES* signature.

Parameter	Mandatory level
Alg	Mandatory
SigT	Mandatory
Crit	Mandatory (sigT)
Cty	Mandatory (multiple media)
X5t#S256	Conditioned (without x5c, x5t#o, sigX5ts)
X5t#o	Conditioned (without x5c, x5t#S256, sigX5ts)
SigX5ts	Conditioned (without x5c, x5t#o, x5t#S256)
X5c	Conditioned (without x5t#S256, x5t#o, sigX5ts)

3 HL7 FHIR

HL7 is a nonprofit organization providing frameworks and standards that facilitate the exchange, integration, sharing, and retrieval of electronic health information to support clinical practices and the handling, delivery, and verification of healthcare services (Health Level Seven International, 2023). HL7 FHIR is a platform specification that defines a set of capabilities for interoperability processes within the healthcare sector (Health Level Seven International, 2023). According to (Monsen et al., 2023), it is a solution for sharing health data information using modular components, with numerous developers working tirelessly to contribute to various specification components that can be utilized in different contexts, such as best practice guidelines, clinical document architecture translation, and clinical care of injuries.

Before the HL7 FHIR standard, other standards were developed with the same purpose. Still, they had a lower level of human-readable abstraction, which resulted in greater effort required for data interpretation. One example is HL7 V2, created in 1989 to integrate various hospital systems, including administrative processes and clinical systems (Bender and Sartipi, 2013). Despite its application, the HL7 V2 standard lacked good scalability. It could not adapt to other use cases, such as the judicial system, and was difficult to comprehend, as illustrated in Algorithm 1.

The next standard developed was HL7 V3, created in 1995 to address the deficiencies of its predecessor. Semantic and lexical element structures were defined for this standard to generate message artifacts automatically. However, the standards are not directly implementable and require tools to create software systems. It offers available XML schemas but not norma-

```

1 MSH|^~\&|Regional MPI||Master MPI|Alpha
  Hospital|20060501
2 140010||ADT^A28|3948375|P^T|2.4|||ER<cr
  >
3 EVN|A28|20060501140008|||000338475^
  Author^Arthur^^^^^
4 ^Regional MPI
  &2.16.840.1.113883.19.201&ISO^L
  |20060501140008<cr>
5 PID|||000197245^^^NationalPN
  &2.16.840.1.113883.19.3&ISO^PN
  ^4532^^
6 ^CarefulCareClinic
  &2.16.840.1.113883.19.2.400566&ISO^
  PI^3242346^^
7 ^GoodmanGP
  &2.16.840.1.113883.19.2.450998&ISO^
  PI||
8 Patient^Particia^^^^^L||19750103|F||
9 |Randomroad 23a&Randomroad&23a^^
  Anytown^^1200^^H||
10 555 3542557^ORN^PH^555 3542558^ORN^FX
  |555 5557865^WPN^PH<cr>
11 PV1||N|<cr>

```

Algorithm 1: Example of a HL7 V2 message.

tive ones, primarily for verification purposes. Despite the evolution of the model, the use of HL7 V3 involves complex transformations of models, operating at a level similar to that of a compiler.

HL7 FHIR was created in 2011, building on the standards that preceded it and combining their advantages with modern data transfer technologies. The standard specification provides basic resources, frameworks, APIs, and a platform for implementing different solutions. To address information not included in the basic resources, HL7 FHIR offers an embedded extension mechanism that can be adapted for specific use cases to ensure interoperability. Therefore, this standard can cover different healthcare domains and manage resources, making it suitable for various purposes, contexts, and workflows (Vorisek et al., 2022).

There are two main types of FHIR solutions: resources and profiles (Monsen et al., 2023). Resources are data organized in packages that can be formatted in JSON or *Extensible Markup Language* (XML) and transported using HTTPS. Profiles are the rules for data exchange, including constraints and additional data elements (Duda et al., 2022). Implementation guides serve as procedural standards for the consistent use of FHIR resources and support *Application Programming Interfaces* (APIs) to facilitate workflows in specific domains (Duda et al., 2022). FHIR resources have the following characteristics (Bender and Sartipi, 2013):

- They must have a clear boundary that corresponds to one or more logical transaction scopes;
- They must be different in meaning, not just in usage;
- They need to have a natural identity;
- They should be very common and widely used in commercial transactions;
- They must not be too specific or detailed to hinder support for a wide range of commercial transactions;
- They must be mutually exclusive;
- They can use other resources but must not be merely a composition of resources;
- They need to provide new content;
- They should be recognized within a logical *framework* based on the similarity of the resource and what it is connected to;
- They must be large enough to have a meaningful context.

4 CORRELATED WORKS

The exploration of FHIR resources for interoperability is not a new concept. In the research by (Monsen et al., 2023), the technology is employed to standardize nursing practices to improve the quality of data outputs. This information can be utilized within the standard for assessments, care planning, and outcome measurement, demonstrating its potential to enhance data transmission, information storage, and knowledge discovery in nursing and public health. Their research shows the utility of FHIR in creating standardized healthcare data focused on the nursing sector and does not address the digital signature requirements critical for secure prescription and medication dispensing processes. While this study focuses on using the standard for nursing data interoperability, it does not explore the use of digital signatures to ensure the authenticity of documents, a crucial factor for the functionality of prescription and medication dispensing addressed in this article's study.

The study by (Bender and Sartipi, 2013) compares the evolutions of the standards set by HL7, highlighting the properties of each standard that allow for a comparison of their strengths and weaknesses. It emphasizes that the FHIR standard has garnered significant attention from the relevant community due to its simplicity and the potential for FHIR to leverage the experiences gained from the implementations of

preceding standards to enhance the state of communication in healthcare systems. Therefore, their study highlights FHIR's potential for improving healthcare communication but lacks the possibility of using a file with an FHIR pattern as an authenticated digital document and digital signatures to use these documents to prescribe medications and create a rastreability on it.

(Vorisek et al., 2022) analyzes the benefits of HL7 FHIR in improving the interoperability of health information. This article compiles a review of existing literature to enhance understanding of the standard, with less emphasis on its application. Thus, the article aims to identify potential use cases for HL7 FHIR in health research while highlighting the associated limitations and providing a realistic perspective on its implementation in medical research. While the article identifies potential use cases for HL7 FHIR in health research, it does not address practical applications involving digital signatures to ensure the authenticity and security of medical documents, a gap this study aims to fill.

(Gruendner et al., 2021) developed a preprocessing service to enable the direct loading of FHIR data. The data is transformed into ready-to-analyze *subsets*, converting JSON information into PostgreSQL data format. This facilitates the transition from data acquisition to relevant clinical research, allowing for more efficient handling of large-scale clinical data without reliance on cloud servers. While the study focuses on storing data without needing cloud servers, it does not address the resolution of data exchange between healthcare centers and pharmacies. Consequently, it does not bring the need for data validation within the database, as demonstrated in the project presented in this article.

(Cheng et al., 2021) introduces a module for clinical data interoperability services to the REDCap software, designed to create databases for clinical trial research and any electronic health record systems that utilize the HL7 FHIR standard. This module facilitates the independent collection and mapping of data to REDCap fields while enabling real-time data extraction to support data collection for clinical studies through intuitive interfaces requiring minimal IT involvement. Although the survey implements FHIR interoperability to facilitate the collection and mapping of clinical data, it does not address the use of digital signatures to authenticate documents, a key feature explored in the present work to ensure security and compliance in medical prescriptions.

(Georgioska, 2020) aimed to analyze the practical feasibility of using digital signatures in the public procurement system of North Macedonia. The objective

was to enhance the security and authenticity of documents, primarily focusing on providing a method for verifying the signer's identity to ensure the authenticity of signed data. The research demonstrates significant effectiveness in security and improves procurement processes' efficiency by reducing bureaucratic paperwork and fostering better communication among the parties involved. Although the study explores the use of digital signatures to ensure security and authenticity in public procurement systems, it does not address the application of these technologies in the healthcare sector, particularly in the context of digital prescriptions and medication dispensing, which is the focus of this study.

5 METHODOLOGY

To digitalize prescription and medication dispensing documents, it was essential first to understand the standards used for information exchange in healthcare. In the medical field, HL7 is renowned for its data standardization, having established HL7 V2 and HL7 V3 as initial solutions for health information standardization. However, despite well-established standards, interpreting data within these frameworks requires significant effort, and developing an application capable of performing this interpretation poses an even greater challenge.

Thus, the search shifted toward the evolving HL7 FHIR standard, which has shown great potential. This standard employs more user-friendly formats that facilitate easier association and transport, reducing effort for humans and applications in data interpretation. Among the possible formats for generating a file in HL7 FHIR are JSON and XML, which are more manageable for applications and can effectively support electronic document signatures.

With its high capacity for information transfer and low storage and memory requirements, along with the ease of understanding the contained information due to the hierarchical organization within the file, the JSON format has proven to be the ideal choice for advancing the next steps of the research. In contrast, while XML also has a well-defined hierarchical structure, it requires more effort for data transition and interpretation, as illustrated in Table 2.

There were issues to be resolved regarding using HL7 FHIR, particularly due to the reliance on hyperlinks as references. While bundles and contained resources are used, references with links associated with those bundles remain possible. This approach hindered the creation of a signed document, as a digitally signed document must contain its entire scope.

Table 2: Comparison between JSON and XML adapted from (Nurseitov et al., 2009).

	JSON	XML
Number Of Objects	100000	100000
Total Time(ms)	7497.36	310017.47
Average Time(ms)	0.07	3.10
Average System % CPU Utilization	11.30	36
Average memory % utilization	68.06	68.79

Furthermore, these references are volatile and would invalidate the generated prescription because of the information change after the signature. To address this, these references were incorporated into the document, ensuring that all necessary information is self-contained, regardless of the possibility of external links. These issues were resolved by embedding this information within the document to guarantee completeness and preserve the integrity of the signed document.

Thus, what were previously external references and hyperlinks are transformed into self-references at other points within the JSON object. All necessary information in the file ensures that the document is self-contained and capable of providing all the required data to generate a digital prescription. This step is crucial, as there are instances where, in HL7 FHIR, the information retrieved online tends to be volatile, especially considering the high rate of updates based on changes in the circumstances of the doctor and the patient.

The next step to be defined is the signature standard to ensure the document's validation in JSON. The first consideration was JWS; however, its implementation has two issues. The first is the requirement for header parameters that qualify the electronic signature, as qualified signatures are mandatory for medication prescriptions. This necessitated a deeper exploration of JSON signatures. The JAdES standard, created by ETSI, emerges as the most suitable format. The parameters for *Claiming Signing Time* and those providing information about the certificate used for signing are essential for qualifying the signatures made by doctors when prescribing medications and pharmacists when dispensing them.

The highlighted signature was chosen because it allows verification of its validity without sharing document information. HL7 FHIR proposes implementing the DaVinci signature in its framework. While this signature is also based on JWS, it was not selected for use due to the greater robustness of the security offered by JAdES. JAdES allows for the definition of different levels, enabling more efficient validation of signed documents over the long term.

With the assurance that the document to be signed contains updated information from the moment it was

generated, the focus shifts to executing the qualified signature. Here, the most critical parameter to consider is the one that indicates when the document was signed; thus, the sigT parameter is essential for contextualizing the timing of the signature. This enables an application to generate and sign an electronic document related to a prescription for a patient. In the API, the credentials of the doctor or pharmacist are validated before recording a prescription or dispensing. The architecture diagram of the project in Figure 2 illustrates how the applications are interconnected.

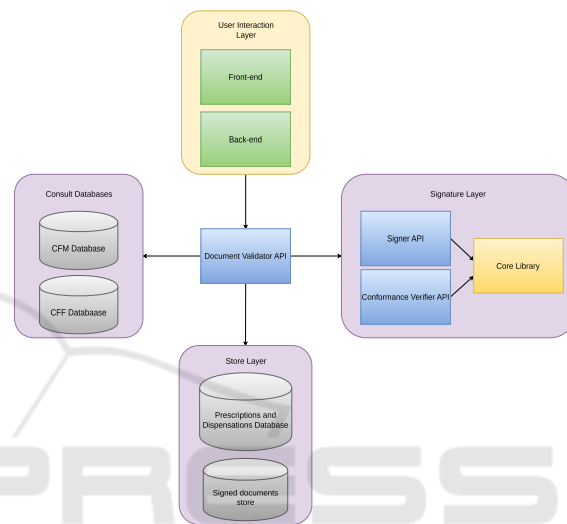


Figure 2: Architecture diagram of the project.

The Signature Validator API was developed to create the adapted FHIR document and perform semantic validation of the information in the signature. In the prescription, this API is responsible for matching the doctor's social security number (CPF) with the number of CPF registered with a consult on the CFM database of this doctor's CRM number. All this process is done when the doctor requests the API to sign the document. This process is crucial to prevent people who are not qualified doctors from prescribing any medication to a third person.

The signed prescription must be valid according to the Brazilian Pattern of Digital Signatures (PBAD) to be accepted. A Signer API was developed to ensure the signature is valid with PBAD and confirm that it will be trusted and valid in Brazilian territory. This API will create a signature with valid parameters using the certificate uploaded by the doctor in the user interface to sign the document. It will also confirm whether the certificate and its trust anchor are valid, according to PBAD.

After creating and validating the prescription, the Signature Validator API is also responsible for creating the prescription register in a database. To insert

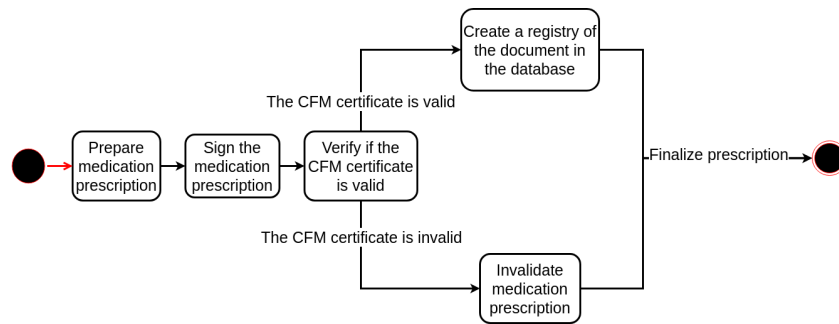


Figure 3: State machine diagram of a registry of medication prescription.

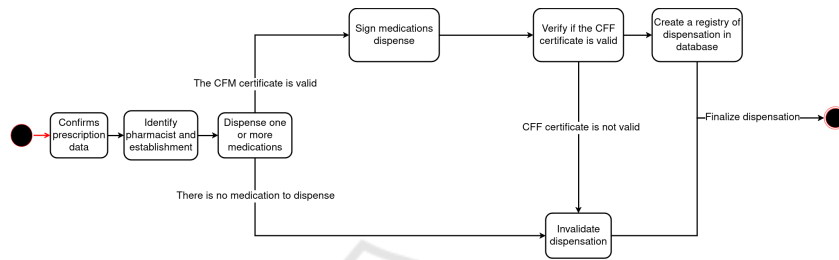


Figure 4: State machine diagram of a registry of medication dispensation.

the prescription information into the database, a hash value for each prescription is made with the date it was created. It also creates a table with the prescription ID and available medications to be consulted in the dispensation. In this way, the API stores the data and the document as shown in Figure 3.

It is important to highlight that data storage was carried out on a local test server when the research was conducted. However, a server with shared access across different hospitals, clinics, doctor’s offices, medical centers, and pharmacies would be essential to ensure the solution’s applicability in a real-world setting. A third-party organization interested in implementing this solution must provide the necessary infrastructure to achieve this.

To dispense the prescription medications, the pharmacist needs the prescription’s hash value and uses it to access its information. The Signature Validator API will bring the document, check if it’s correct semantically, and send it to the Conformance Verifier API. The Conformance Verifier API will check the validity of the signature and its trust anchors and validate the signature parameters according to PBAD to return to the Signature Validator API, which will perform a query at the database and return the medications prescribed and their amounts. Signer and Conformance Verifier APIs have some common implementations; therefore, these implementations were detached and called core libraries to enhance comprehension and make the development easier.

After this process, the Validation API is responsible for consulting possible previous dispensations

linked to that prescription by ID key and performing the same verification made in the prescription if necessary. The pharmacist has two options for dispensation: partial dispensation, which will dispense some prescribed medications, and total dispensation, which will dispense all prescribed medications.

To perform the dispensation, the pharmacist will select the amount of each prescribed medication and fill out a form with his information and CFF number. This will allow the Signature Validator API to consult the CFF database. After this confirmation, the pharmacist will select the amount to dispense. If dispensing medication is not allowed anymore, previous dispensations will show a stack trace of dispensations. Otherwise, the document of dispensation is created, and the pharmacist will sign it to pass through the validation process of the Signature Validator API and Signer API, which will be stored with its respective prescription as seen in Figure 4.

Unit tests were developed to guarantee the correct functionality of APIs. Tests on Signer API verify if all needed parameters were inserted in the signature, it also verify if the signature was made and use artefacts to verify the insertion of the digest algorithm parameter. The Conformance Verifier API has tests to see the validity of the signature, non-repudiation of the signature, its certificate chain, and the validity of the signature parameters.

Document Validation tests verify the correctness of the professional’s credentials and the consistency of the signatory’s information with the data retrieved from the CFM and CFF databases. They also ensure

that the credentials are included in both the prescription and the dispensing of medications. Additionally, tests were developed to verify the validity of the prescription and dispensing and the functionality of the database.

After implementing all unit tests, a pilot test was conducted with one doctor to test the API's behavior during the prescribing process and a pharmacist to test its behavior with the partial and full dispensing of medicines. In this pilot, the system behavior was tested with valid and already dispensed receipts, valid and invalid CRM and CFF, and valid and invalid signatures.

6 RESULTS AND CONCLUSION

The project holds great potential to improve the prescription and dispensing process, and the pilot test showed its technical viability. It can also revolutionize dispensing practices with a new concept of partial dispensing, increasing patients' flexibility in purchasing their medications. The combination of FHIR standardization and digital signatures, where the JSON format and JAdES served as crucial communication bridges between these concepts, demonstrated a viable path toward digitalizing the medication prescription process.

In addition to the problems already faced, this approach still needs to be facilitated for common patients. For this, the solution under analysis is to use a PDF representation for the patient that will be issued digitally, containing a QRcode referencing the hash of the official medication prescription and dispensing document. The generated PDF will be signed by the doctor upon prescription and signed by a pharmacist upon dispensation, and the objective is to use it as a human-readable document.

Although adaptations are necessary, the transformations implemented have been feasible and leave room for further evolution. The technologies employed are still considered new and can be explored in various ways. A Brazilian definition based on FHIR can be established, allowing for a gradual transition from current paper prescriptions to a digital format.

For future work, a real case of use with a hospital and pharmacy needs to be done, and in case of success, blockchain implementation for medication dispensing is proposed. This technology aligns well with the theme by leveraging the key properties of consistency and information tracking. It can potentially enhance security and fraud prevention, which could significantly improve the safety of prescriptions and the dispensing of controlled medications. This technol-

ogy can also improve the performance and the scalability of this solution.

REFERENCES

- Bender, D. and Sartipi, K. (2013). HL7 FHIR: An agile and RESTful approach to healthcare information exchange. In *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems*, pages 326–331. IEEE.
- Cheng, A., Duda, S., Taylor, R., Delacqua, F., Lewis, A., Bosler, T., Johnson, K., and Harris, P. (2021). RED-Cap on FHIR: Clinical data interoperability services. 121:103871.
- Conselho Federal de Medicina (2021). Resolução cfm nº 2.299/2021. <https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2021/2299>. Acessado em: 09 jun. 2024.
- Duda, S. N., Kennedy, N., Conway, D., Cheng, A. C., Nguyen, V., Zayas-Cabán, T., and Harris, P. A. (2022). HL7 FHIR-based tools and initiatives to support clinical research: a scoping review. 29(9):1642–1653.
- European Parliament and Council of the European Union (2014). Regulation (EU) no 910/2014 of the european parliament and of the council of 23 july 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC. <http://data.europa.eu/eli/reg/2014/910/oj/eng>. Acessado em: 09 jun. 2024.
- Georgioska, M. (2020). Application of digital signatures in the electronic system for public procurement in republic of north macedonia.
- Gruendner, J., Gulden, C., Kampf, M., Mate, S., Prokosch, H.-U., and Zierk, J. (2021). A framework for criteria-based selection and processing of fast healthcare interoperability resources (FHIR) data for statistical analysis: Design and implementation study. 9(4):e25645.
- Health Level Seven International (2023). Fhir modules. <https://hl7.org/fhir/modules.html>. Acessado em: 09 jun. 2024.
- Ibarz, J.-C. C. (2020). Bringing JSON signatures to ETSI AdES framework: Meet JAdES signatures. 71:103434.
- Ibarz, N. (2021). Development of a tool for validating etsi ades digital signatures as defined by the european standard etsi en 319 102-1.
- Institute, E. T. S. (2021). Electronic signatures and infrastructures (esi); jades digital signatures; part 1: Building blocks and jades baseline signatures.
- Jones, M. B., Bradley, J., and Sakimura, N. (2015). JSON web signature (JWS). Num Pages: 59.
- Kutyłowski, M. and Błażkiewicz, P. (2023). Advanced electronic signatures and eIDAS – analysis of the concept. 83:103644.
- Ministério da Saúde do Brasil (2020). Rede nacional de dados em saúde (rnds). <https://www.gov.br/saude/pt-br/composicao/seidigi/rnds/rnds>. Acessado em: 09 jun. 2024.

- Monsen, K. A., Heermann, L., and Dunn-Lopez, K. (2023). FHIR-up! advancing knowledge from clinical data through application of standardized nursing terminologies within HL7® FHIR®. 30(11):1858–1864.
- Nurseitov, N., Paulson, M., Reynolds, R., and Izurieta, C. (2009). Comparison of JSON and XML data interchange formats: A case study.
- Pohls, H. C. (2015). JSON sensor signatures (JSS): End-to-end integrity protection from constrained device to IoT application. In *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 306–312. IEEE.
- Presidência da República do Brasil (1957). Lei nº 3.268, de 30 de setembro de 1957. http://www.planalto.gov.br/ccivil_03/leis/l3268.htm. Acessado em: 09 jun. 2024.
- Presidência da República do Brasil (1960). Lei nº 3.820, de 11 de novembro de 1960. http://www.planalto.gov.br/ccivil_03/leis/l3820.htm. Acessado em: 09 jun. 2024.
- Presidência da República do Brasil (2020). Lei nº 14.063, de 23 de setembro de 2020. <https://www.in.gov.br/en/web/dou/-/lei-n-14-063-de-23-de-setembro-de-2020-278574432>. Acessado em: 09 jun. 2024.
- Roehrs, A., Da Costa, C. A., Righi, R. R., Mayer, A. H., Da Silva, V. F., Goldim, J. R., and Schmidt, D. C. (2021). Integrating multiple blockchains to support distributed personal health records. 27(2):146045822110075.
- Vorisek, C. N., Lehne, M., Klopfenstein, S. A. I., Mayer, P. J., Bartschke, A., Haese, T., and Thun, S. (2022). Fast healthcare interoperability resources (FHIR) for interoperability in health research: Systematic review. 10(7):e35724.

