information

Article

A Digital Signature Model Using XAdES Standard as a Rest Service

Renato Carauta Ribeiro *,†, Murilo Góes de Almeida *,† and Edna Dias Canedo *,†

Department of Computer Science, University of Brasília (UnB), P.O. Box 4466, Brasília 70910-900, DF, Brazil
* Correspondence: rcarauta@unb.br (R.C.R.); murilo.almeida@aluno.unb.br (M.G.d.A.); ednacanedo@unb.br (E.D.C.); Tel.: +55-61-98114-0478 (E.D.C.)
† These authors contributed equally to this work.

Abstract: The digital signature of documents and degrees is a topic widely discussed in the Federal Public Administration. Several laws and ordinances were created to standardize the issuance, validation and legal validity of digitally signed documents in national territory, such as the ordinances created by the Ministry of Education (MEC) to regulate the issuance of degrees in digital format. These ordinances created guidelines and standards that must be adopted by Federal Universities for the signing of in digital format. The main objective of this work is to study these ordinances, the main technologies and digital signature standards used in the literature to create a digital signature system model for University of Brasília-UnB, which complies with the MEC and ICP-Brazil standards. Moreover, the model must be developed with the main standards and technologies in the market, cohesive to the current UnB architecture, easy to maintain and update to new standards that may emerge, and also be a fully open source project. An architectural model and a prototype in Java language were developed using XAdES4j library as a microservice intermediated by the bus used in UnB. The prototype developed was compared with the current digital signature system named C3Web. The comparative tests and results between the two solutions showed that the current system used in UnB does not perform the signature in accordance with the standard proposed by the MEC, in addition to being a private system using proprietary technologies for the execution of digital signatures. The tests performed with the proposed model demonstrated that it performs the digital signature in accordance with the XAdES-T standard, regulations of the MEC and ICP-Brazil. In addition, the solution presented a performance comparable to the current system used by UnB with a little more effective security than the current system used. The current model developed in this work can be a basis for the creation of future subscription systems for Brazilian Universities.

Keywords: digital signature; XAdES; REST; RSA; ICP-Brazil; XAdES-T

Citation: Ribeiro, R.C.; de Almeida, M.G.; Canedo, E.D. A Digital Signature Model Using XAdES Standard as a Rest Service. *Information* **2021**, *12*, 289. https://doi.org/10.3390/info12080289

Academic Editor: Nelly Leligou

Received: 16 June 2021
Accepted: 15 July 2021
Published: 22 July 2021

1. Introduction

The Brazilian Federal Government is concerned with modernizing the issuance of degrees, currently issued in physical format. This model results in several problems, such as: high cost, greater ease of forgery, limitation of validation and longer delay for issuance, because in addition to printing, they must be physically signed by the University's rector.

In this scenario, the Ministry of Education (MEC) created two ordinances, the no. 330 and no. 554, which authorize Brazilian Federal Universities to issue degrees in digital format and standardize the format of a digitally signed degree [1].

The University of Brasília (UnB) aims to modernize the issuance of digital degrees and is used to show what is regulated by the Ministry of Education ordinance. In 2018, UnB spent BRL 11,000 with the issuance of postgraduate degrees and, in the same year, it started to make available a system for the issuance of digital degrees, named C3Web (accessed on 20 February 2021) [2]. The system maintenance contract is about BRL 200,000 per year. This system has some disadvantages, such as not signing degrees that are not previously stored in the database. In addition, as it is proprietary software, UnB is charged an annual

fee for its use. Another disadvantage is not providing the source code for the evolution of the system, corrections of possible bugs and adaptation of this software to the Ministry of Education ordinance. Therefore, it is necessary for UnB to develop its own system for signing documents in digital format.

The most common problems found in the current solution used by UnB are the nonconformity to the standards proposed by the Ministry of Education and the difficulty for maintenance and evolution, caused by proprietary libraries. In addition to that, signed degrees are kept in the database outside of UnB data model, which means that the data needed to present the saved degrees is replicated. Another problem is that degrees can only be signed if they are previously stored in the database, which prevents the signing of external degrees. Last, but not least, the system is sealed and does not have services for communication between other applications. Moreover, the software used to read digital certificates does not integrate with any database, making it necessary to read the certificate each time a batch of the system is signed.

The purpose of this work is to create a model for digital signature according to the Ministery of Education and IPC-Brazil standards, cohesive to the current UnB architecture. Thus, for the development of the digital signature model focused on the current UnB architecture and the Federal Government guidelines, we analyze laws related to document signing, standards, files made available by MEC, processes defined by MEC, and current signing standards to create an architectural model of the signing process.

2. Background and Related Works

The Brazilian Federal Government published two ordinances and a normative defining and exemplifying the standards and technologies that must be used in the digital signature of degrees. The ordinances mention that the XML format must be used and the signature must be done using the minimum standard XAdES-T with the Rivest–Shamir–Adleman (RSA) algorithm [1,3].

The signature of degrees and documents in digital format must have the same validity as the signature made in physical format. To execute the signature in digital format we use the asymmetric cryptography, also called public key cryptography together with the RSA algorithm, as recommended by the Brazilian Federal Government [4]. Public-key cryptography is based on mathematical functions and uses two distinct keys, public and private [5]. By using two different encryption keys, it is possible to encrypt a file using one of the keys and decrypt it using the other key. The cipher flow of public key cryptography is demonstrated in Figure 1:

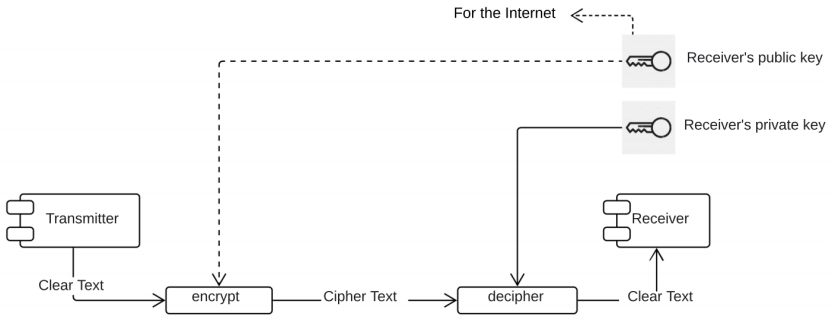

Figure 1. Asymmetric encryption [6].

When an asymmetric signature is used, it is possible to guarantee the authenticity and integrity of the information, but it is not possible to guarantee non-repudiation. To be specific, suppose that Bob and Alice exchange messages using the public key scheme, in this case, some problems can arise: (1) Alice can forge a different message and claim that it came from Bob. (2) Bob can deny the message sent to Alice. To ensure that a document was actually signed by that certificate and considered valid, the subscriber's public key

must be signed by a Certificate Authority (CA). This CA guarantees that the certificate is true, integral, and valid. In Brazil, the main CA is named ICP-Brasil.

The Ministry of Education's ordinances and the technical note regulate that documents must be signed in XML Advanced Electronic Signature (XAdES) format. This standard of signature is done in documents in XML format in order to ensure authenticity, integrity and non-repudiation, defining electronic ways that guarantee its validity for a long period of time [7]. A signature using the XAdES standard provides basic authentication, integrity protection and meets the legal requirements for advanced signatures as defined in the European Directive [EU-DIR-ESIG], but not all types of signature made in the XAdES standard ensure the non-repudiation [7]. There are several types of signatures that can be made using the XAdES [8] pattern:

- XAdES-BES: it is basic way of signing documents in XML format, where authenticity and integrity of records are guaranteed; however, it does not offer the non-repudiation.
- XAdES-T: there is the addition of timestamp to the XAdES-BES basic signature, which ensures non-repudiation.
- XAdES-C: it adds dataset references to XAdES-T that support electronic signature validation. Information such as certification path reference, certificate status and revocation. This type of signature is important when you want to archive information externally.
- XAdES-X: builds on XAdES-C by adding timestamps to protect against risk of any keys used in the certificate chain or revocation status information that may be compromised.
- XAdES-X-L: added to XAdES-X providing more validation data, such as certificate revocation values, in case the revocation information is not stored in another external location.
- XAdES-A: builds on XAdES-X-L by adding a timestamp field for archiving signed documents.

Related Works

Crampton [9] discussed the need to use cryptography and digital signature in documents in XML format to protect confidentiality and provide guarantees on the integrity of those documents transmitted through insecure means. The author focused on how some XML document access and control policies can be applied using cryptography. Techniques for assigning keys in a security network that can be adapted to minimize the number of keys distributed to users were also presented. The author proposed a new XML document access control policy.

Engelbertz et al. [10] evaluated the validation logic of the open source software library for creating and validating signed documents—provided by the Connectiong Europe Facility (CEF) named Digital Signature Service (DSS)—, related to XML-based attacks. The vulnerabilities discovered allowed reading files from the server and bypassing the protection provided by XML Advanced Electronic Signature (XAdES). The authors concluded that there is an urgent need for documents of good security practices and automated security assessment tools to support security-relevant implementations.

Lepiane et al. [11] presented an insight about the problem of physical degree forgery that occurs in Brazil and how the certificate in digital format can help to resolve this issue. Certifications must be secure and legally acceptable throughout the Brazilian territory. The authors work proposes a technical specification that can be used by higher education institutions in accordance with the policies adopted by the federal government.

The work proposed by Oliveira Fernandes et al. [12] had as an objective a technical study for the viability of using blockchain in degrees in a digital format that must be compatible with Ministry of Education and ICP-Brazil regulations. The study concluded that the characteristics of the blockchain show that it is possible to use it, therefore, digital degrees can be accessed in a secure way.

Ibarz and Cruellas [13] mentioned a new way to provide digital signatures using the Json Web Token (JWT) for digital signatures in the JAdES standard. This standard must

have the same security and validity as the other signature formats of the ETSI AdES family (CAdES, PAdES and XAdES). The JAdES standard has special emphasis on signing with the JWT and the timestamp. This signature must be valid over time along the same lines as the other standards. At the end, the authors summarize the results obtained by a program designed to verify the accuracy of the technical approaches adopted and which serve as proof of concept. This work was a starting point for the construction of a formal proposal for the production of an ETSI (European Telecommunications Standards Institute) using JWT [13].

Henny Indriyawati et al. [14] created a certification system for issuing digital degrees for Semarang University in Indonesia. The process adopted for signing the degree through physical means was quite bureaucratic, long, ineffective and inefficient. Therefore, there was a need to develop a digital signature model adhering to the standards of Semarang University in a web system developed in PHP. The authors created a secure system using the AES algorithm with a 256-bit key.

Some specific countries, such as Indonesia, recognize the importance of digitally signing degrees and documents. Many of them developed solutions through the web, using object-oriented programming languages and the Unified Modeling Language (UML) to model the proposed architecture [3,14,15]. Some of the solutions studied used QRCode to guarantee the validity of a digitally signed degree. Other legislations, such as the Brazilian and European ones, mentioned that the main format that guarantees the legal validity of a degree must be the XML format with the XAdES signature pattern with, at least, the timestamp. In addition to the degree in XML format, the same degree must also be made available in a visual format in PDF using a QRCode for validation [1,14].

Like the solution presented by Semarang University, many solutions identified in the literature developed closed systems, some with desktop subscription, others using web solutions, but none of the studies surveyed developed a microservices model focused on REST communication and saving certificates for signature made exclusively through the web [16]. Unlike other related works, in this research a model was developed with validation by a functional prototype whose main objective is to achieve national legal validity and be validated by any validator of ICP-Brasil.

3. The Electronic Signature Law in Brazil

In 2018, the Ministry of Education (MEC) published several ordinances for Brazilian federal universities, both public and private, that allow them to issue documents in digital format. According to the Ordinance No. 330 of 5 April 2018, the digital degree was instituted within public and private universities belonging to the Federal Education System. According to this ordinance, the digital degree must cover the student and academic record. Only educational institutions that have the prerogative to issue and register degrees can do it in digital format. It is emphasized in this ordinance that digitally signed degrees must meet the certification guidelines of ICP-Brazil, which guarantees their validity throughout the national territory. Finally, the aforementioned ordinance stipulates a time of 24 months for the implementation of the digital signature solution by federal higher education institutions [17].

The ordinance No. 554 of 11 March 2019, has the objective to regulate the mandatory issuance of graduation degrees in digital format by federal institutions of higher education. This ordinance says that the degree issued in digital format must be preserved in a computer environment that insures [1]: (1) validity at any time; (2) interoperability between systems; (3) a security technology update; and (4) the possibility of multiple signatures on the same document.

The signatories of the digital degree must be the same signatories of the degree in physical format, requiring the signature with the ICP-Brazil digital certificate type A3 or higher. The certificate must be an official certificate from the higher education institution that signs the degree in digital format. The degree must be signed in XML format with the signature in XML format Advanced Electronic Signature—XAdES [1].

The ordinances No. 330 and 554 regulate how to provide a degree in digital format that is accepted throughout the national territory and in accordance with current Ministry of Education guidelines and ICP-Brazil. In addition to these two ordinances, the Ministry of Education makes available the layouts, patterns and the technical note named Normative Instruction No. 1, of 15 December 2020, which aims to provide a better technical specification for each criterion involved in the issuance and registration of the digital degree [3].

According to Normative Instruction No. 1, of 15 December 2020, it is necessary a storage in digital media, and whose legal validity is presumed upon signature with digital certification and timestamp in the Brazilian Public Key Infrastructure—ICP-Brazil, according to the parameters of the Brazilian Standard for Digital Signatures—PBAD. Only signatures that follow the standards recommended by the ordinances, technical norms and the XML Schema Definition—(XSD) defined by the Ministry of Education [3] will be considered valid.

The digital degree is digital native, that is, it is issued and stored entirely in digital media. The digital degree must be stored according to the procedures and technologies that allow validation over time. Technological evolutions must be observed, and the format of the stored document may be changed to ensure its authenticity, integrity, reliability, availability, traceability, non-repudiation, timeliness, privacy, legality, interoperability and national legal validity. The degree issued in digital format must have the same validity and follow the same current federal legislation that regulates the issuance and registration of the physical degree. It is the responsibility of higher education institutions to follow the legislation, regulations and the internal flow for issuing a degree in digital format [3].

The Normative Instruction No. 1, of 15 December 2020 says that it is necessary to ensure the integrity and correct formatting of the degree in XML format, it is necessary to generate the XML based on a schema definition (XSD) defined by the Ministry of Education. XSD is a document based on the XML standard that guides the definition of a XML document and is also used to check its validity. The XSD documents will always be maintained and updated to meet the standards required for signing a degree in a digital format [3].

The XSD files must be constantly updated to follow the current federal legislation with current technology standards. The XSD made available by the MEC for the creation of a degree in digital format is present in the so-called "degree portal", made available by the same ministry [3,18]. The XSD contains the definitions of type, size, occurrence and filling rules for the elements that must compose the XML document. The MEC presents some XSD files for specifying the digital degree and how the signature should be done:

- Digital Degree_v1.00.xsd : defines the syntactic structure of the graduate's XML.
- Academic Documentation Digital Degree Registration_v1.090.xsd: defines the syntactic structure of academic documentation for issuance and registration.
- Basic Types_v1.00.xsd: responsible for syntactic control of all types used in other files of this technical specification of the digital degree. It serves to guarantee the syntactic integrity of the fields used in the digital degree.
- Digital Degree Layout_v1.00.xsd: Responsible for syntactic control of the XML structure of the graduate.
- Academic Documentation Layout of Digital Degree Registration_v1.00: Responsible for syntactic control of the XML structure of academic documentation for issuance and registration.
- Xmldsig-core-schema_v1.1.xsd: responsible for syntactic control of the digital signature XML structure.

4. Digital Signature Requirements

According to MEC and ICP-Brazil, the degree in XML format must have UTF-8 format to be signed in the XAdES standard. The use of XAdES-T is the minimum standard recommended by the MEC for a document to have national validity, be complete and

guarantee non-repudiation. For digital signature, the degree must already come with all data of the graduate, the issuing IES, the course data, the data of the registering IES, the information in registration book, the e-MEC code composed by the code of the issuing IES , the code of the registering IES in addition to the code of digital degree location. If some of these elements are missing from the degree, an error message must be sent and the degree will not be signed. In the model, it is also necessary to validate the degree to verify that all necessary elements to carry out the digital signature are present [3].

If the degree is valid, it is necessary to sign the degree in XAdES format in accordance with the ICP-Brasil standard and the Brazilian Standard for Digital Signature—PBAD. The PBAD standard aims to impose validation rules and the creation of digital signatures so that documents have the necessary security and can be validated by national and international institutions [3]. According to the ICP-Brasil document for digital signature, the XAdES signature must be based on the XMLDsig signature. In addition to the mandatory elements of the XAdES signature, the following elements must be included: DataObjectFormat (for detached signatures), SigningCertificate and SignaturePolicyIdentifier [19]. A certificate, according to ICP-Brasil, must have at least the following attributes for its validity, as shown in Figure 2 [19].

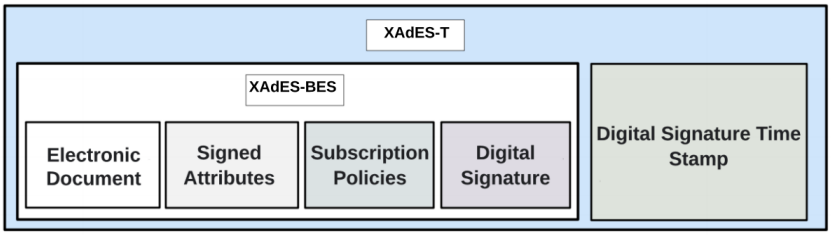

Figure 2. Digital signature with time reference [19].

After adding the ID attribute in the Signature element, the initial degree hash function in XML format must be added. The hash format defined by the MEC technical note is the SHA256 format, and the the degree element must be used to generate the hash [3]. After generating the hash for the degree element, the signature is created following the XMLDsig pattern. Next, the elements necessary for the signature to be valid, according to the ICP-Brasil standards, are included in the Object element. In addition, it is necessary to add the elements referring to the type of signature used. Inside the Signature element, the attribute xmlns:ds is added, which represents the signature pattern used, which must be XMLDsig. In the SignatureValue element, the value of the signature transformed to base64 is added [20].

It is also necessary to add the real value of the digital signature that is inserted into the XML inside the SignatureValue element. In addition to this element, the X509Certificate element must also be present in the digital signature, which includes a public key, digital signature and information about the identity associated with the certificate and its issuing CA. With these two elements and the use of cryptographic HASH, the integrity and authenticity of the signed degree [20] is guaranteed. The digital signature must be done with the minimum standard XAdES-T and in accordance with XMLDSIG (accessed on 20 February 2021). Using this standard, authenticity is guaranteed for a long period of time with a signature considered valid, even after the invalidation of the certificate that signed the given degree [3,20].

5. Digital Signature Model

The proposed signature model aims to demonstrate how a digital signature system should be developed that uses the XAdES standard and is signed with the certificate A1, A3 or higher, which must be read by a desktop system and saved in a database. Afterwards, all degrees must be signed using a REST service, where all degrees in XML format are sent in a zip compressed format. After reading, the elements of the degree that will be signed are checked, observing if there is the main element <Degree>. Thereafter, a signature is made,

and each of the signed degrees is saved in the database. This model aims to demonstrate how a microservices architecture can be developed with the XAdES-T signature, which is the type of signature that will be developed in this work. Figure 3 shows the complete flow of the digital signature, from signature until the degree is saved and made available signed in the database.

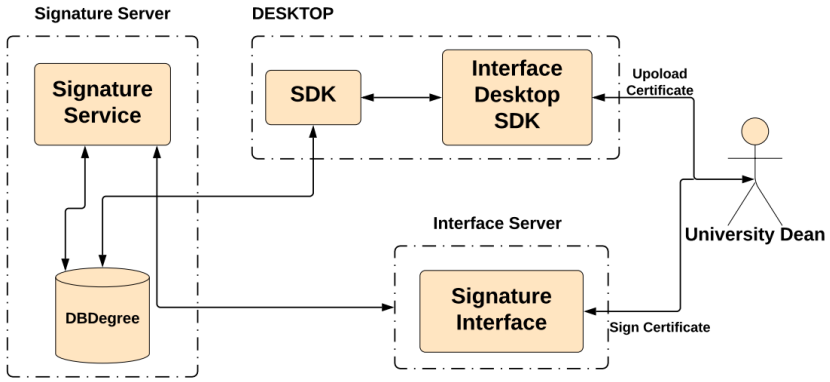

Figure 3. Digital signature components.

As can be seen in Figure 3, the process of signing degrees in digital format is divided into two steps. In the first step, the degree is read, both A1 and A3. In the second step, a batch of degrees is signed in XML format, compressed in zip format, and all degrees in the XAdES-T standard are signed, in addition to saving the signed degrees in the database.

To read the A3 certificate, some specific dlls must be used which have to be installed on the Desktop. For this reason, a Desktop system is necessary, called SDK, and in this model, the degree read is saved in a database. Once the degree is saved in the database, it is possible, later, to execute the signature of degrees through the digital signature service, as shown in Figure 3, it is stored and provided by the server, without the need for have any system installed on the Desktop. The subscription service is a REST service using the POST method that needs two parameters to be passed in the request body. The degree batch in zip format and the certificate password must be sent, then the degree can be signed. Degrees are signed by the service, saved in the database, and a success message is returned to the user who signed the degree.

After that, the degrees can be made available by other systems for their visualization and validation. Figure 3 shows the process performed, from the reading of the degree to the use of a REST service for the digital signature of degrees. At no point in this process is there any access to the internet, only the university's intranet.

The digital signature module is just another service that is provided through the STI/UnB service bus. The bus communicates with the access method to initiate the subscription flow within the subscription module. The digital signature system must be self-contained and have the ability to easily integrate through the main signature model. A public communication interface is made available for easy integration of this solution with any other system that will consume this service. Figure 4 presents the summary of the current architecture of the authentication services proposed by this work and how the communication and integration between the backend module and the bus is done.

Figure 4 presents the applications that communicate via REST to authenticate using the LDAP and Oauth2 protocols. The subscription service must be a Java module that is hosted in a server without internet access. This module is used by the STI/UnB bus as an intermediary for accessing the subscription service. The digital signature service has three basic modules. Figure 4 shows the communication flow from a frontend application to the signature module and the database for storing degrees and certificates. To show the internal architecture of the digital signature service, is presented the class diagram—using the UML notation—with the main classes of the digital signature system in the model shown in Figure 5.

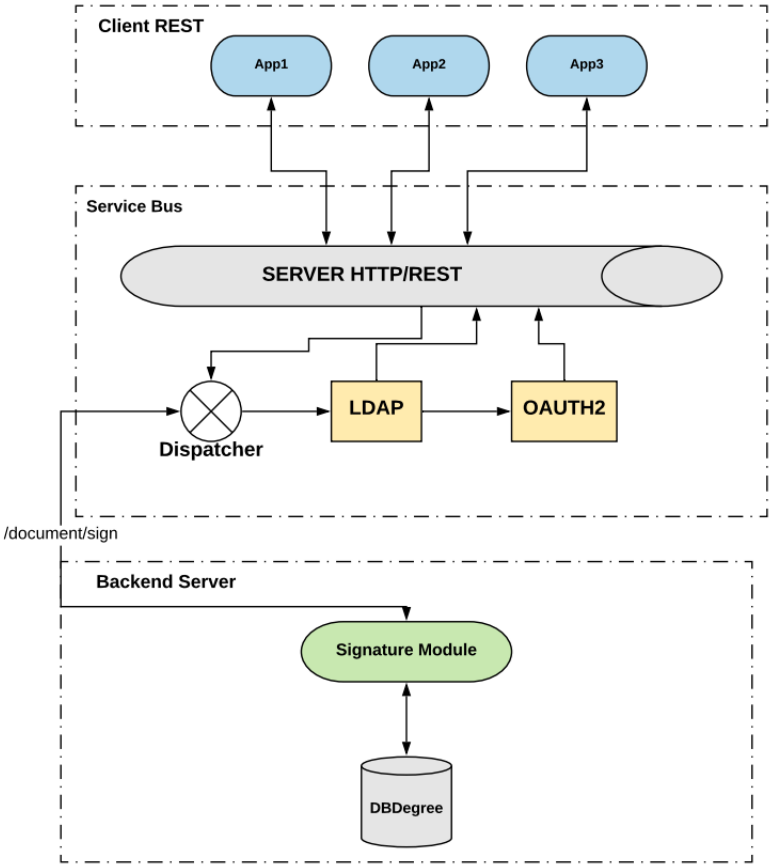

Figure 4. Service bus diagram.

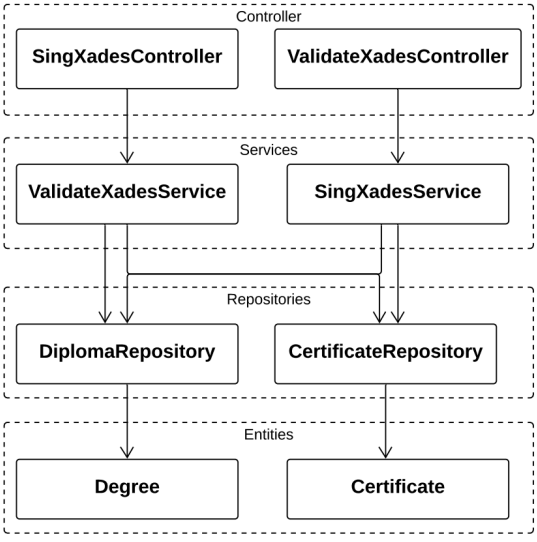

Figure 5. Subscription model class diagram.

In this Figure 5, the structure of packages can be seen in classes and their interactions. It is necessary to demonstrate what each class does and its importance in this model:

- XadesController Signature: It is the initial class that has the communication interface with the service bus. The signXades method is the main method for signing in the XAdES standard. As a parameter, the degrees are compressed in zip format, the certificate password and the idPerson are sent to search the certificate.

- ValidateXadesController: It is the initial class that makes the communication interface for the validity of a signed degree. The main method is the validate method, which checks if the signed degree complies with the MEC standard, as the xsd format for degree validation.
- SignatureXadesService: It is the service class that actually has the function of signing each document that is inside the digital degree signature zip file. The main method of this class is the sign method, which makes the signature of a degree using the XAdES standard. There are two auxiliary methods, one to save the signed degree into the database and another to fetch the certificate saved by the sdk in the database to perform the signature.
- ValityXadesService: It is the service class that uses xsds files to validate the degree signed in the MEC standard. The method validateDegree is the main method that informs whether the degree is valid or not according to the standard specified in xsd.
- DegreeRepository: It is the class that saves the signed degree in the database and joins the saved degree to the signed idPerson and the idPerson of the degree student.
- CertificateRepository: Retrieves the certificate from idPerson to sign a batch of degrees.
- Certificate: It is an entity that has all database parameters. It is all the data that will be retrieved in the certificate table.
- Degree: It is the entity that sets all the parameters to save a degree. All data will be saved in the degree table.

This work focused on how the tags of the digital signature system are, how this signature execution module is inserted within the current UnB architecture and, during the development of the model, demonstrated why the use of a desktop model for creation of the SDK and another for the execution of the digital signature in the XAdES standard in accordance with the guidelines of the MEC and ICP-Brazil. The digital certificate for signing degrees in digital format is carried out in a web environment. In the case of A1 certificate, which is used in this prototype, the digital signature is made through a frontend web application that sends the certificate to be stored in the server, therefore it improves the performance of the digital signature at execution time. The standard format that must be accepted for certificate storage has the .pfx format.

The A3 certificates are stored via USB sticks or memory cards, which are inserted into computers and can only be read locally, it is not possible to be read directly by the browser, unlike the A1 certificate. Thus, a desktop solution would be needed for accessing, validating and storing the A3 certificate in the server for future signatures [21]. To add an A3 level certificate in the server for future signatures, it must be done locally by an SDK that will read the token, validate and save it in a specific server for signing degrees in digital format. This module must have a desktop component in order to validate and integrate the certificate into the server, then, batches of certificates can be signed in the future through a frontend application.

For the SDK it is necessary to add specific dlls for each of the certifiers, then the SDK module can read the certificate correctly and store it in the server, consequently, the document batches are signed. All certificates are added using database and only some specific IPS are allowed to save the certificates in the server. A very good security is needed to ensure that only specific people have access to this server and everything running on it, which must be done by the logged-in user. The general model of the architecture, from reading the certificate to signing the batches of degrees in digital format, is presented in Figure 6:

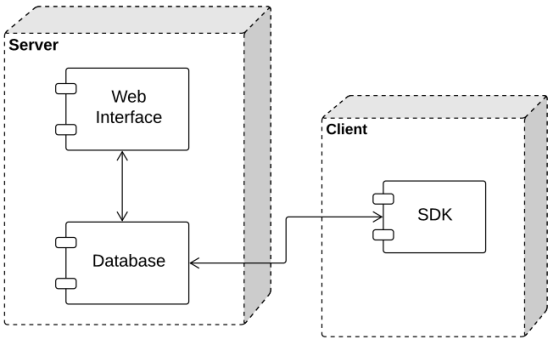

Figure 6. Subscription solution components diagram.

The model presented is minimalist and based on microservices. The focus of this work is the creation of a digital signature model, which should be of easy integration, evolution and composition between the services to be created. The model presented was developed by composition of services, which shows the integration between services for the complete development of the digital signature system according to MEC and IPC-Brasil. Figure 7 presents the composition of all the requirements needed by MEC and shows that it is possible to create a system in several small parts, which guarantees good modularity, maintainability and that future evolutions take place in a controlled manner.

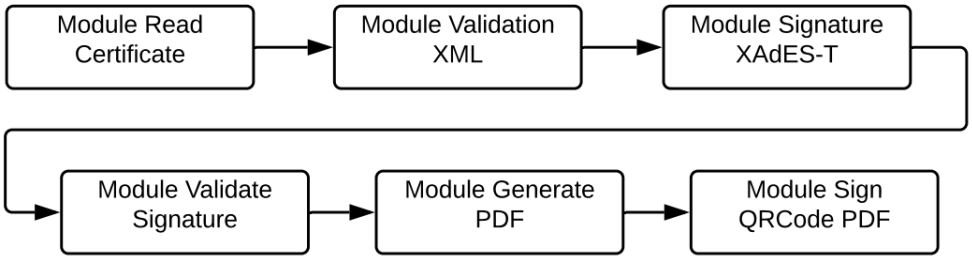

Figure 7. Separation of digital signature process modules.

Figure 7 presents the complete signature process proposed by the MEC with the separation of components:

- The digital signature of the degrees must be made with the A1 or A3 format.
- After reading the certificate, it is necessary to generate the XML according to the XSDs provided by the MEC website digital degree (accessed on 20 February 2021).
- After reading and validating with the XSDs provided by MEC, the signature is made with the XAdES-T standard.
- It is necessary to provide a module for the external digital signature.
- After signing the degree in XML format, it is necessary to generate the degree in visual format in PDF format.
- A QRCode is generated to ensure the integrity of the degree in visual format.
- Both the degree signed in XML format and the other in visual format, in PDF format must be made available to the student by digital means, being accessible at any time.

6. Tests and Discussion

The methodologies used are both black box, with performance tests and security tests done at runtime, as well as white box tests, using static code analysis. The model used by the performance test was based on the 25010 standard, in which five basic software quality requirements are evaluated. To define the best expected performance in each of the requirements of the tests studied, the Key Performance Indicator (KPI) metric was used

in order to indicate the expected results for the tests performed and what were, in fact, the values achieved by each one of the tests applied.

In the first part, it was defined, according to what is expected by UnB, what is important for an acceptable performance, security and quality for a future system for signing degrees in digital format. The parameters necessary for the model to be validated as acceptable were defined, as shown in the Tables 1 and 2.

Table 1. List of C3Web KPI Indicators.

Requirements	Expected Value	Value Obtained
Code Quality	0.0%	0.0%
High Alerts	0	0
Medium Alerts	1	3
Low Alerts	7	4
Error Instances	50	390
Performance	12 min	6 min and 25 s

Table 2. List of Java Prototype KPI Indicators.

Requirements	Expected Value	Value Obtained
Code Quality	0.0%	0.0%
High Alerts	0	0
Medium Alerts	1	3
Low Alerts	3	4
Error Instances	50	8
Performance 12 min	9 min and 25 s	

Comparing the expected results with what was achieved with the tests, it was possible to determine that both systems have a performance within the expected standard, both have good code quality, without any duplicated code, but the current UnB system has less quantity of security flaws considering the parameters raised and expected by UnB. The prototype developed, on the other hand, as it has a smaller scope and is highly modularized, the security parameters are in accordance with what is expected for a secure system, according to the needs of UnB.

In this section, we present a comparison between the current system used by UnB named C3Web, and the current model proposed in this paper, to verify which one is more secure and whether both have a suitable performance for signing UnB degrees. Tests were carried out to verify security and performance. The tests performed were based on problems present in systems documented by the Open Web Application Security Project (OWASP). Test analysis should focus on the following principles: reliability, integrity, availability, authentication, and authorization. We verified which of the systems has greater compatibility with MEC and ICP-Brazil regulations and which of the solutions has greater possibility of future evolution.

We performed static tests using SonarQube [22] to check for possible flaws in the solutions and verify test coverage in the models. As a consequence, it was possible to analyze which of the systems is more likely to have a critical flaw in the code. For dynamic tests, the OWASP ZAP software was used. The purpose of this system is to identify the main security flaws reported by OWASP [23], as well as verifying if any of these defects exist in the compared solutions, in addition to analyzing the severity of them.

The code of the C3Web project currently used by UnB was analyzed using SonarQube. The tests revealed that this system has five bugs, with no vulnerabilities and no code smell, as can be seen in Figure 8. Thereby, we can conclude that this system has no security issues, according to static code analysis.

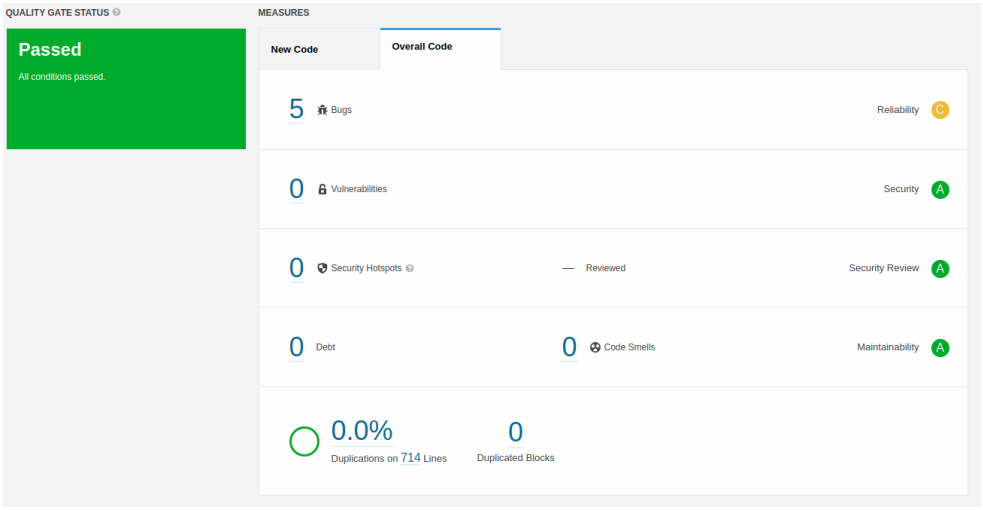

Figure 8. Results of static tests in C3Web System.

Despite C3Web system test results showing five potential bugs according to the SonarQube tool, these bugs do not have a high vulnerability in the application. Despite C3Web being a system that uses a proprietary library to execute the signature, it is secure and reliable for signatures in the XAdES-BES standard. To date, this system does not use XAdES-T, which is the standard recommended by the MEC.

To perform the static test of the solution proposed in this work, we also used the SonarQube. The solution was developed using Java language and XAdES4j library to implement the system for signing degree batches, according to the MEC and ICP-Brazil format. The test results are shown in Figure 9.

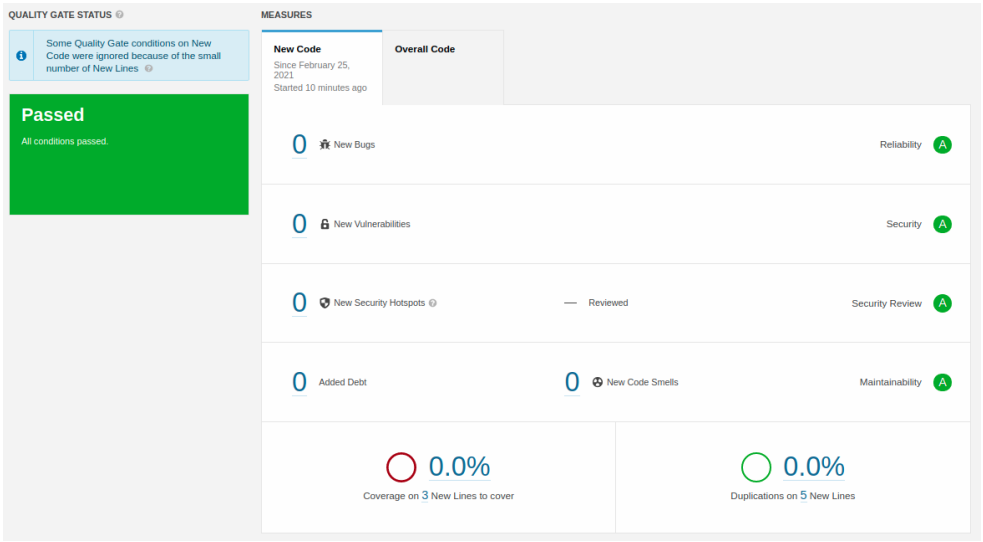

Figure 9. Results of static tests in the proposed solution.

The results demonstrated that the proposed model and the prototype developed using the XAdES4j library have a simple and minimalist solution, having no bugs, vulnerabilities or duplication of code. This result ensures that, statically, the model proposed in this work has the same results as C3Web, with a smaller amount of bugs and does not have any duplicated code.

In order to validate the system's security, it was necessary, in addition to static tests, to perform dynamic security tests. One of the most used standards to validate the security of services came from OWASP. OWASP is a non-profit organization with the goal of improving software security. The main tool that checks the main security vulnerabilities

documented by OWASP is named OWASP ZAP. This tool is considered a great solution for problem analysis in web applications and [24] services. This software performs a runtime scan to check whether the software is secure or not.

After the comparison performed with the static code using SonarQube, the dynamic security test of the two solutions was done using the OWASP ZAP [24] tool. For this reason, it was possible to verify at runtime if the applications had acceptable security standards for signing degrees in digital format [25].

The current system used by UnB, C3Web, use a desktop version to make the signature of degrees and has a portal for storing certificates, degrees and standards for signing and maintaining the systems. Security tests were carried out on this administration portal to verify the security of the storage of degrees, certificates and signatures. The results are shown in Figure 10.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	4
Informational	2

Alerts

Name	Risk Level	Number of Instances
Directory Browsing	Medium	1
Vulnerable JS Library	Medium	3
X-Frame-Options Header Not Set	Medium	2
Absence of Anti-CSRF Tokens	Low	36
Incomplete or No Cache-control and Pragma HTTP Header Set	Low	11
Private IP Disclosure	Low	1
X-Content-Type-Options Header Missing	Low	175
Information Disclosure - Suspicious Comments	Informational	134
Timestamp Disclosure - Unix	Informational	27

Figure 10. Security test with the C3Web system.

A test into the security model proposed in this study was performed. The result of the tests, using the OWASP ZAP tool, concluded that no high risk was found, there was only an intermediate level risk that has no relevant impact on the security of the proposed model, as shown in Figure 11.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	3
Informational	0

Alerts

Name	Risk Level	Number of Instances
Buffer Overflow	Medium	3
Application Error Disclosure	Low	2
Information Disclosure - Debug Error Messages	Low	2
X-Content-Type-Options Header Missing	Low	1

Figure 11. Security test performed on the prototype of the proposed solution XAdES4j.

In addition to the security tests, performance tests were also carried out, because digital signature solutions must sign a batch of 200 to 500 documents in an acceptable time. To accomplish the tests, a batch of 200 degrees in zip format was used. The result is shown in Figure 12:

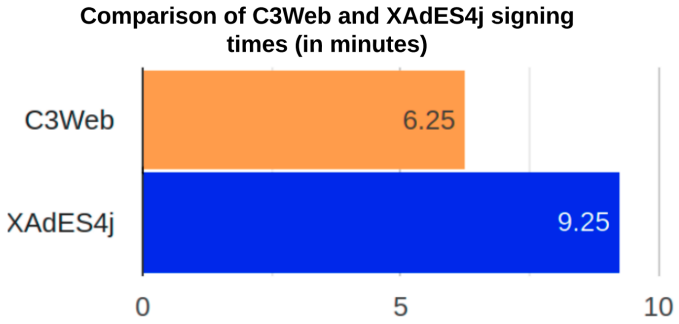

Figure 12. Signing time.

It is possible to see in Figure 12 that the performance in minutes for signing 200 degrees using C3Web, was 6 min and 46 s. Using the prototype proposed by this work developed in Java and with the XAdES4j library, it has a total performance of 9 min and 25 s for signing the same quantity of degrees.

It can be realized that the current UnB system has a better performance; nevertheless, it is not configured in a real comparison with the proposed system in this work, because this C3Web makes the XAdES-BES signature without the timestamp. The signature system developed in this work, on the other hand, makes the signature of degrees in the XAdES-T standard with timestamp and in the current standard of the MEC and ICP-Brazil, which shows that they have different protocols, with different characteristics, and consequently different signing times.

6.1. Guarantee of Better Security in the Signed Degree

According to the work being developed at federal universities, to obtain better security for degrees signed for a long period of time, blockchain [26–28] is being used [29,30]. The Federal University of Paraíba (UFPB) performed a study with the objective of creating a private blockchain among Brazilian Federal Universities; consequently, the degrees signed with the XAdES-T standard have ensured its security and reliability, with the validity of the blocks already inserted and of the transactions that will insert new blocks [31].

How it is a private network between the Federal Universities and the MEC as a central entity, the integrity of the blockchain network depends on the credibility of the nodes added to this network. Node trust is required to ensure total network integrity. This private blockchain model serves as a dissemination and data control with certain security and privacy of the degrees inserted in this network, which is an additional way for the degree to not be stored only in a single location [3,31,32].

Another work developed in Getúlio Vargas Foundation (FGV) has a proposal to create a private blockchain network for federal universities to share their degrees signed in the XAdES standard, ensuring the internal and external security of these documents. This private network would have the MEC as the central body and the federal universities as sharers of the degrees inside of the blockchain network, where they would be signed and their security would be reinforced [33].

Considering the proposal of developing a new network for blockchain following the regulations of the MEC and IPC-Brazil to sign degrees, it is necessary that the degrees are first signed in the XAdES standard with a timestamp, and can later be inserted into the blockchain network and signed, therefore, it is possible to have greater security in the information present in the degree and, since it is a private blockchain network, it is possible to guarantee reliability in the data added to this network. In addition to this blockchain network for degrees in digital format, the Brazilian federal government has a National Archive where all documents, whether in physical or digital format, are kept stored for the period of validity of this document.

According to the National Archive's digital document preservation policy, an entity must be able to maintain the authenticity of the documents stored digitally by the institution. Thus, policies and methods must be used to ensure that the document is not manipulated,

altered or falsified [34]. All copies made in the stored digital document must be authentic, all changes must be mapped, and all digital documents must be identified and cataloged in order to have a record of the digital documents that are stored [34].

All data present in digital format documents must be kept with integrity and without changes from the moment that this document is considered valid [34]. Within the scope of UnB, a degree is considered valid when it is signed in accordance with the XAdES standard. As a consequence, the data present in the digital degree must be fully preserved.

According to the National Archives, the repository for storing digital documents must have the capacity to expand to a minimum of three years [34]. The technical note of the MEC does not have a minimum period for validity and storage digitally signed degrees; however, it is mentioned that a digitally signed degree must be updated, be valid at any time and be stored for a long period of time [3].

To ensure the availability, integrity, authenticity and validity of the digital degree at any time, without fraud, in addition to all the measures presented above, it is necessary that the degree can be signed only once. If it is necessary to change any information in the degree, the MEC regulations say that the old degree must be invalidated and a new degree has to be signed [3]. Every time that a degree is invalidated, the employee name who invalidated the degree must be saved in a permanent log. This is one of the guarantees, in addition to the blockchain, which helps to prevent internal and external fraud.

The technical note of MEC says that the digital degree must be stored in a digital environment that ensures validation at any time, interoperability between systems, technological security update and the possibility of multiple signatures in the same degree [3]. For this reason, UnB must store digitally signed degrees in local servers, in the blockchain private network and also in the National Archive, which guarantees that the same degree is stored in three different places, and the integrity of that degree can be validated by analyzing the three places to verify that they are all the same, as shown in Figure 13.

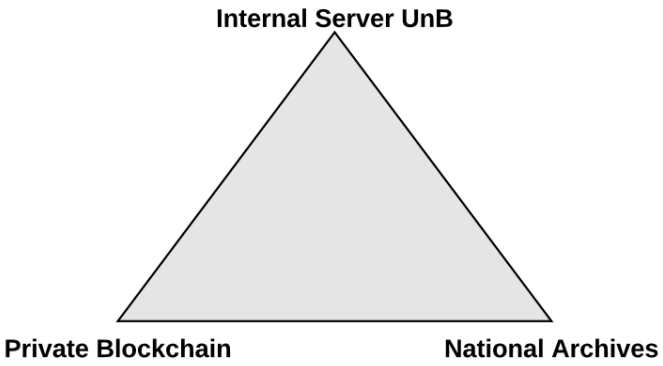

Figure 13. Verification servers for validating the signed degree integrity.

As can be seen in Figure 13, there must be three replicas of the same degree. One must be kept on UnB's local server, another copy in the National Archives and a third in the blockchain private network. This ensures a better security in the integrity of the stored data. An improper alteration in one of the degree's replicas will make it different from the others, which will invalidate the change.

Using the blockchain and signature techniques with the XAdES standard, it is possible to keep the security of degrees in digital format. By sharing degrees in this future network, it will be possible to have a high availability to verify the validity of the degree at any time. Another important point, addressed both by the MEC's technical note and the National Archive, is the fact that the degrees will remain valid for a long time. For a degree to remain valid and complete, there was proposed an addition of degrees signed in the blockchain network. In addition, documents can be stored in a trusted archival service (TAS). This is a secure storage location where documents are securely available. If there is a technological

evolution, only the central file server should be updated to keep the documents stored and already signed in a secure and valid way [35].

With the addition of the degree signed in the blockchain network that will be created by the MEC and with the internal storage in a TAS, the degrees will have a guarantee of long-term security, regardless of technological changes and document signing that may occur in the future.

To date, there are studies both for the creation of a private blockchain network between the Federal Universities and the MEC as a central entity, and for using the blockchain together with the digital degree signature standard proposed by the MEC [30,33]. In addition to these two current studies that demonstrate how to insert a blockchain network and display its advantages, there are some initiatives to create a degree validation network; that is, at the time of validation, the degree must be validated in the three places mentioned in Figure 13.

6.2. European Standard for Signing Digital (Europass)

The European standard for signing digital degrees assumes that every student has a Europass. Europass is a set of online tools to help create a Curriculum Vitae (CV) for each student. Thus, Europass works as a digital resume validated with digital certification. Certificates and degrees are signed by the institution and also by the student [15]. In Brazil, only university degrees are validated with a digital certificate and the student does not have a digital card as in Europe.

Because of Europass, documents can be validated without the need of a third party to validate the student's data or identity. In addition, the European Union is concerned about issuing certificates in physical format. The digitally signed degree must have greater security than a degree issued in physical format [15]. Degrees and certificates signed on European territory must be valid within and outside Europe [15]. In Brazil, the Ministry of Education, using the ICP-Brazil, ensures that signed degrees are valid only in the national territory [3].

For digital signatures, the MEC guidelines recommend that the signature be done using the XAdES standard with the timestamp. The degree must be signed with at least a A3 digital certificate. In addition to the XML that must be signed, it is also necessary that a degree be available in a visual format. The main current works on digital signature are using the blockchain both to sign a document and to keep the document valid for a long time. The blockchain is a kind of digital signature. There are several formats of digital signature that can be made in documents:

- Aggregate Subscription: It is a kind of subscription that receives n different subscriptions from n different users, and it is possible to summarize all these subscriptions in a single short subscription. This summary ensures that the n users signed the document. The advantage of this technique is that the computing power for signature storage and verification is greatly reduced. This technique is recommended in locations with low bandwidth and limited storage space [36].
- Ring Signing: This scheme assumes a public key for all users and a private key for each user. This kind of signature is used on documents that need traceability and that need long-term protection. This approach eliminates the needing of a third party to validate the signature on the signed document was made [36].

The blockchain is a way of peer-to-peer signing where there is no central control. To ensure security, a blockchain signature is written so that this document cannot be changed. Nevertheless, it must accept new transactions. To add new elements in the blockchain, it is necessary to place a hash reference from the previous block in the current, sealed block. Because of it, the break attempt in a single document impacts all of previous documents. Therefore, it is possible to add new transactions, but it is almost impossible to change the data that was triggered in the past. Any attempt to change it breaks the hash [37].

The European Union has a document with guidelines for implementing a school record using digital certification. The Europass framework for digitally-signed credentials demonstrates the advantages of using blockchain in conjunction with the PKI public key signature framework. This technology enables the verification authority to be decentralized, in addition to controlling the transactions executed on this signed document. It also prevents anyone from trying to cheat by generating the document with a fake [15] signature. As was discussed above, this would invalidate the complete chain of certificates, which facilitates the identification of the fraudulent document.

7. Conclusions

This paper proposed a viable solution for signing degrees in digital format using microservices architecture, in accordance with the Ministry of Education's ordinances and technical note, in addition to being in compliance with the current specifications currently used by the University of Brasília. Therefore, as it proves to be viable both in technological and legal aspects, it can be used in any Brazilian educational institution. We also identified how the storage in the Brazilian National Archive and in a future Blockchain network should be done, in order to guarantee greater security and a high availability of signed degrees.

The system with the aforementioned aspects, that is, adherent to the UnB architecture, easy to maintain and integrate, was developed with the Java programming language, the SpringBoot framework and the open source library XAdES4j. It is important to mention that the solution presented only addresses a small part of the signature system, requiring a more complete system covering the entire process involving the reading, issuance and digital signature of degrees.

During the work, we conducted comparative tests between the current signature system used by UnB, the C3Web (which does not make the signature with the XAdES-T standard), with the prototype developed in this research. The results demonstrate that both tested solutions are, for the most part, adherent to all standards considered adequate by UnB for a digital signature system. However, the system currently used by UnB showed a large number of errors during the tests performed by the OWASP ZAP tool. It is also important to mention that C3Web is a proprietary system, which makes it difficult to integrate and customize its resources. Last, but not least, the tests also demonstrated the importance of not keeping degrees stored in one place, requiring them to be kept in different locations.

According to what was presented, we conclude that it is currently necessary to create a new system for signing and validating degrees at UnB, which can be done with open source technologies and modern architectures, such as microservices. In this way, the university will not be dependent on proprietary systems that are outdated as new technological approaches and government regulations appear. In addition, the model studied and proposed in this article can be implemented by any university in the country, not limited to the scope of UnB, being a reference guide for those who wish to evolve their system.

The main contribution of this research to the Brazilian Federal Government is that we propose how the digital signature of degrees from Brazilian Universities should be developed. Thus, the proposed solution will allow the Brazilian government to minimize the cost of physically signed digital degrees and the use of proprietary systems by Brazilian universities. In addition, we demonstrated how to create a solution for storing digital documents in several places (different servers) to have better security and credibility of the stored degrees. By storing signed degrees in three different places, as proposed in this solution, it is possible to validate a degree by comparing it with the one stored in all places with the degree being validated, therefore ensuring more robust security.

Author Contributions: Writing—original draft preparation, R.C.R., E.D.C. and M.G.d.A.; writing—review and editing, R.C.R, E.D.C. and M.G.d.A.; visualization, R.C.R, E.D.C. and M.G.d.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Educação, Ministério da Educação: Portaria no 554, de 11 de Março de 2019. 2019. Available online: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/66544171/do1-2019-03-12-portaria-n-554-de-11-de-marco-de-2019-66543842 (accessed on 2 May 2021).
2. UnB Diploma, UnB Diploma. Sistema de Emissão de Diplomas Digitais. 2018. Available online: http://servicos.unb.br/diploma (accessed on 2 April 2021).
3. Normativa, I. Instrução Normativa no 1, de 15 de Dezembro de 2020. 2020. Available online: http://portal.mec.gov.br/diplomadigital/arquivos/in_01_15122020.pdf (accessed on 2 May 2021).
4. ICP-BRASIL, D. A. PadrõEs E Algoritmos CriptográFicos. 2019. Available online: https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-01-01-v-4-2-padroes-e-algoritmos-criptograficos-da-icp-brasil-copy-pdf (accessed on 13 July 2021).
5. Klavos, N.; Stallings, W. Book Review. In *Cryptography and Network Security: Principles and Practice*, 6th ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2013; 752p, Volume 23, pp. 49–50. ISBN 13: 978-0133354690.
6. Forouzan, B.; Catherine, C.; Sophia, C.F. *Introduction to Data Communications and Networking*; McGraw-Hill, Inc.: New York, NY, USA, 2012.
7. ETSI. 101 903 Xml Advanced Electronic Signatures (xades), v1. 3.2. European Telecommunications Standards Institute. 2010. Available online: https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf (accessed on 1 June 2021).
8. Brzica, H.; Boris, H.; Hrvoje, S. Long-Term Preservation of Validity of Electronically Signed Records. In Future 2013. November 2013 Available online: http://darhiv.ffzg.unizg.hr/id/eprint/8291/ (accessed on 6 January 2021).
9. Crampton, Jason: Applying Hierarchical and Role-Based Access Control to Xml Documents. In Proceedings of the 2004 Workshop on Secure Web Service, SWS '04, Fairfax, VA, USA, 29 October 2004. Association for Computing Machinery: New York, NY, USA, 2004; pp. 37–46. [CrossRef]
10. Engelbertz, N.; Vladislav, M.; Juraj, S.; David, H.; Nurul-lah, E.; Jörg, S. Security analysis of xades validation in the CEF digital signature services (DSS). In Proceedings of the Open Identity Summit 2019, OID 2019, Garmisch-Partenkirchen, Germany, 28–29 March 2019; Roßnagel, H., Sven, W., Detlef, H., Eds.; GI. Bonn: Bonn, Germany, 2019; Volume P-293 de LNI, pp. 95–106. Available online: https://dl.gi.de/handle/20.500.12116/20997 (accessed on 6 March 2020).
11. Lepiane, C.D.; Pereira, F.L.; Pieri, G.; Martins, D.; Martina, J.E.; Rabelo, M.L. Digital degree certificates for higher education in brazil: A technical policy specification. In Proceedings of the ACM Symposium on Document Engineering 2019, Berlin, Germany, 23–26 September 2019; Schimmler, S., Uwe, M.B., Eds.; Association for Computing Machinery: New York, NY, USA, 2019; pp. 7:1–7:10. Available online: https://dl.acm.org/doi/abs/10.1145/3342558.3345398 (accessed on 14 March 2021).
12. de Oliveira, Fernes, E.; Lima, J.L. Estudo da Tecnologia Blockchain para Aplicação na EmissãO, Arquivamento e Validação de Diplomas de Graduação em Formato Digital. Anais do Simpósio de Tecnologia da Informação e da Semana de Iniciação Científica do Curso de Sistemas de Informação (ISSN em Fase de Registro). 2019. pp. 36–40 Available online: https://www.anais.ueg.br/index.php/sti_sic/article/view/13988 (accessed on 14 April 2020).
13. Ibarz, J.C. Bringing json signatures to etsi ades framework: Meet jades signatures. *Comput. Stand. Interfaces* **2020**, *71*, 103434. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0920548919300960 (accessed on 21 February 2021). [CrossRef]
14. Indriyawati, H.; Winarti, T.; Vydia, V. Web-based document certification system with advanced encryption standard digital signature. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, 516–521. [CrossRef]
15. Europass Framework for Digitally Signed Credentials. 2018. Available online: https://ec.europa.eu/futurium/en/system/files/ged/europass_background-info_framework-digitally-signed-credentials.pdf (accessed on 10 April 2021).
16. Yarygina, T.; Bagge, A.H. Overcoming security challenges in microservice architectures. In Proceedings of the 2018 IEEE Symposium on Service-Oriented System Engineering (SOSE), Bamberg, Germany, 26–29 March 2018; pp. 11–20. Available online: https://ieeexplore.ieee.org/abstract/document/8359144 (accessed on 8 February 2021).
17. Educação, Ministério da Educação: Portaria no 330, de 05 de abril de 2018. 2018. Available online: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/9365055/do1-2018-04-06-portaria-n-330-de-5-de-abril-de-2018-9365051 (accessed on 17 April 2021).
18. Diploma Digital. 2020. Available online: http://portal.mec.gov.br/diplomadigital/ (accessed on 10 May 2021).
19. DE, Geração e Verificação: Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na icp-Brasil doc-icp-15.01 versão 2.0. ICP-Brasil, 2010. xii. Available online: https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-15-01-v-2-0-pdf (accessed on 2 May 2021).

20. Bartel, M.; Boyer, J.; Fox, B.; LaMacchia, B.; Simon, E. Xml Signature Syntax and Processing Version 1.1. *Signature* **2013** *6*, 1. Available online: https://www.w3.org/TR/xmldsig-core1/ (accessed on 10 February 2021).
21. Cooper, D.; Santesson, S.; Farrell, S.; Boeyen, S.; Housley, R.; Polk, W.T. Internet x. 509 Public Key Infrastructure Certificate and Certificate Revocation List (crl) Profile. IETF. *RFC* **2008**, *5280*, 1–151. Available online: https://datatracker.ietf.org/doc/html/rfc5280 (accessed on 13 March 2021)
22. Marcilio, D.; Bonifácio, R.; Monteiro, E.; Canedo, E.; Luz, W.; Pinto, G. Are static analysis violations really fixed? A closer look at realistic usage of sonarqube. In Proceedings of the 2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC), Montreal, QC, Canada, 25–26 May 2019; pp. 209–219. Available online: https://ieeexplore.ieee.org/abstract/document/8813272 (accessed on 9 April 2021).
23. Marchand-Melsom, A.; Nguyen, Mai, D.B. Automatic repair of OWASP top 10 security vulnerabilities: A survey. In Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops, Seoul, Korea, 27 June–19 July 2020; pp. 23–30. Available online: https://dl.acm.org/doi/abs/10.1145/3387940.3392200 (accessed on 27 January 2021).
24. Riadi, I.; Pradana, A.R.Vulnerability Analysis of E-Voting Application Using Open Web Application Security Project (Owpasp) Framework. 2019. Available online: https://pdfs.semanticscholar.org/2be6/83e9e959ca6746a9134a236deb4b603c04cd.pdf (accessed on 15 July 2021).
25. Mishra, S.; Majed, A.A.; Sunil, K.S. Impact of Security Standards and Policies on the Credibility of E-Government. *J. Ambient. Intel. Humaniz. Comput.* **2021**, *12*, 1–12. Available online: https://link.springer.com/article/10.1007/s12652-020-02767-5 (accessed on 12 January 2021).
26. Sudaryono, S.; Aini, Q.; Lutfiani, N.; Hanafi, F.; Rahardja, U. Application of blockchain technology for ilearning student assessment. *IJCCS Indones. J. Comput. Cybern. Syst.* **2020**, *14*, 209–218. Available online: https://journal.ugm.ac.id/ijccs/article/view/53109 (accessed on 18 January 2021). [CrossRef]
27. Panachev, A.; Shcherbitsky, V.; Medvedev, M.A. Application of blockchain technologies and game approach in the educational process of universities. *AIP Conf. Proc.* **2021**, *2333*, 100004. Available online: https://aip.scitation.org/doi/abs/10.1063/5.0042076 (accessed on 18 March 2021).
28. Liang, X.; Xu, S. Student performance protection based on blockchain technology. *J. Phys. Conf. Ser.* **2021**, *1748*, 022006. Available online: https://iopscience.iop.org/article/10.1088/1742-6596/1748/2/022006/meta (accessed on 20 March 2021). [CrossRef]
29. Meng, N.; Shunxiang, Z. University Education Resource Sharing Based on Blockchain and Ipfs. In *Big Data Analytics for Cyber-Physical System in Smart City*; Atiquzzaman, M., Neil, Y., Zheng, X., Eds.; Springer: Singapore, 2021; pp. 1808–1813. ISBN 978-981-33-4572-0. Available online: https://link.springer.com/chapter/10.1007/978-981-33-4572-0_270 (accessed on 15 November 2020).
30. Palma, L.M.; Vigil, M.A.; Pereira, F.L.; Martina, J.E. Blockchain and smart contracts for higher education registry in brazil. *Int. J. Netw. Manag.* **2019**, *29*, e2061. Available online: https://onlinelibrary.wiley.com/doi/full/10.1002/nem.2061 (accessed on 8 November 2020). [CrossRef]
31. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *Acm Comput. Surv.* **2019**, *52*, 1–34. Available online: https://dl.acm.org/doi/abs/10.1145/3316481 (accessed on 22 January 2021). [CrossRef]
32. Costa, R.; Faustino, D.; Lemos, G.; Queiroga, A.; Djohnnatha, C.; Alves, F.; Lira, J.; Pires, M. Uso não financeiro de blockchain: Um estudo de caso sobre o registro, autenticação e preservação de documentos digitais acadêmicos. In *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações*; Sociedade Brasileira de Computação: Porto Alegre, Brasil, 2018. Available online: https://sol.sbc.org.br/index.php/wblockchain/article/view/2356 (accessed on 23 March 2021).
33. Dubrowsky, A. Transformação Digital nas InstituiçõEs Privadas de Ensinosuperior Brasileiras: Proposta para Autenticação de Diplomas Digitais de Graduação por Meio de Blockchain. Fundação Getúlio Vargas. 2019. Available online: http://bibliotecadigital.fgv.br/dspace;/bitstream/handle/10438/27717/DISSERTACAO_ALEXANDER_DUBROWSKY_VF.pdf (accessed on 17 March 2021).
34. AN Digital Política de PreservaçãO Digital. 2016. Available online: http://www.siga.arquivonacional.gov.br/images/an_digital/and_politica_preservacao_digital_v2.pdf (accessed on 25 March 2021).
35. Stančić, H. Long-Term Preservation of Digital Signatures. Em Tehnični in Vsebinski Problemi Klasičnega in Elektronskega Arhiviranja. 2016. Available online: https://www.researchgate.net/profile/Hrvoje-Stancic/publication/301364818_Long-term_Preservation_of_Digital_Signatures/links/5e05edd44585159aa49d8b2d/Long-term-Preservation-of-Digital-Signatures.pdf (accessed on 23 March 2021).
36. Fang, W.; Chen, W.; Zhang, W.; Pei, J.; Gao, W.; Wang, G. Digital signature scheme for information non-repudiation in blockchain: A state of the art review. *EURASIP J. Wirel. Commun. Netw.* **2020**, *2020*, 56. Available online: https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-020-01665-w (accessed on 12 April 2021). [CrossRef]
37. Drescher, D. *Protecting the Data Store*; Apress: Berkeley, CA, USA, 2017; pp. 135–143. Available online: https://link.springer.com/chapter/10.1007/978-1-4842-2604-9_16 (accessed on 12 January 2021).