

Digital Signature in the XAdES Standard as a REST Service

Renato Carauta Ribeiro and Edna Dias Canedo(✉)

Department of Computer Science, University of Brasília (UnB), P.O. Box 4466, Brasília, DF, Brazil
{rcarauta,ednacanedo}@unb.br
http://www.cic.unb.br

Abstract. The Brazilian government has been discussing the topic of information security and the availability of information through digital media. Information made available in digital format must have the same protection as information in physical format. One of the solutions proposed in the educational area to make documents available in a secure digital format was introduced by the Ministry of Education (MEC), which was the creation of a model for signing papers and University Degree in digital format. The government defined the main guidelines for the creation of this digital signature solution through ordinances. According to the MEC, the deadline for implementing a system for signing University Degree and documents in digital format must be established by 2022. This work presents a digital signature solution for the University of Brasília (UnB). Besides, we demonstrate the current architecture used by UnB and how the creation of new solutions can be incorporated into this architecture. Thus, we present the internal architecture of the digital signature module and demonstrate how the developed solution will be integrated into the current architecture of UnB. As a main result, the proposed solution presents a reduction in the costs of signing digital documents and allows higher speed in signing University Degree and documents in digital format.

Keywords: RSA · Digital signature · XAdES · Information security · Cryptography

1 Introduction

Information security is a topic widely discussed by several countries that have create increasingly stringent laws for the protection and security of information. In general, security is the ability to protect against any threat or damage, whether intentional or not, for a specific purpose [1]. Information security aims to protect the reliability, integrity, and availability of information, whether in the storage, processing, and transmission of data. To have good security, a security policy, education, training, and awareness of the parties involved in the use of technology is necessary.

© Springer Nature Switzerland AG 2020
O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12249, pp. 676–691, 2020.
https://doi.org/10.1007/978-3-030-58799-4_49

Several countries have been concerned about information security and the consequences of possible data leaks. For this reason, several laws were passed to standardize the protection of information. Currently, the international law of the European Union (EU) that deals with the protection and security of personal data is the General Data Protection Regulation (GDPR) [2]. The GDPR is a regulation of the European Parliament and Council of the European Union and the European Economic Area. According to the law, based on a policy of transparency and privacy notification, the user must have control over what data will be used by companies that collect personal data.

On August 14, 2018, Brazil approved the Brazilian General Data Protection Law (LGPD) [3]. This law provides for the processing of personal data, including in digital media, intending to protect the fundamental rights of freedom, privacy, and the free development of the personality of the natural person. For these personal data, that is, digital information, to be safe, it is essential to adopt technical and administrative security measures to protect this information [3]. The LGPD determines what can and cannot be done about the collection and processing of personal data in Brazil, providing for punishments for companies that disrespect its principles [3].

One of the essential processes for protecting information is data encryption. One of the crucial uses of public-key cryptography is the use of a digital signature. It is a way for a user to sign a message or document with their private key. However, it is possible that another user can verify the veracity of the information using the public key of the user who signed the message [4]. The advantage of this approach is that, once the document or message is signed with a user's private key, the user cannot deny having signed the document or sent the message, which guarantees strong security and the principle of non-repudiation [5].

Digital certificates were used to guarantee the authenticity of public keys, that is, to ensure that a given public key does belong only to a person or organization associated with it. This guarantee requires a trusted third party, called the Certification Authority (CA), responsible for verifying the claim of each owner that generates a public key. For this, CA signs the owner's public key, thereby ensuring its authenticity [6].

In Brazil, the Ministry of Education (MEC) has established that the University Degrees of the Federal Educational Institutions (IFES) must be in digital format with the use of digital certificates in the XAdES standard. The MEC portal stipulated several deadlines for the implementation of the University Degree in digital format. The process started in 2018 and should end by 2022. From that date, University Degree will be made available only in digital format [7].

The standard for signing documents in digital format determined by the MEC must be valid throughout the national territory and must be signed by an ICP-Brazil Certification Authority. The certificate must be A3 or higher [8]. Thus, it is of paramount importance that the University of Brasilia (UnB) has a fast, scalable digital signature system, within the standards determined by the MEC and can sign several documents in batch, in addition to the possibility of verifying their validity and authenticity.

This work aims to develop a new digital signature solution focused on microservices architecture, ensuring greater scalability and fault tolerance. We developed the system in compliance with data privacy laws (LGPD and GDPR) and Federal Government ordinances.

This article is organized into sections as follows. Section 2 presents the theoretical background necessary to understand this work, as well as related works. Section 3 presents the legislation, the methodology used for the development of this research, the architecture proposed for the development of this work, and an example of an initial prototype of the digital signature system. Section 5 concludes the article and presents future work.

2 Background

2.1 Cryptography

The encryption algorithms are divided into two groups: symmetric encryption algorithms (also called secret key) and asymmetric encryption algorithms (also called public key) [9,10]. The encryption algorithms are based on two principles: substitution, in which each element of the clear text (bit, letter, group of bits, or letters) is mapped to another element and transposition, in which the elements of the clear text are rearranged. When performing these two operations, no information can be lost [4,11,12]. For an encryption algorithm to be considered computationally secure, it must follow two criteria: the cost to break the encryption exceeds the value of the information, and the time required to break the encryption must exceed the validity time of the information [4].

Until the 1970s, the only type of cryptography that existed was symmetric cryptography, and to this day, it is the most widely used type of cryptography [4]. Currently, in symmetric cryptography the two most used algorithms are Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [4], [13], [10], [11], [12]. In asymmetric cryptography the most used algorithms are RSA and DSA [4], [12]. A new type of asymmetric cryptography has been developed, and is currently beginning to be used, called Elliptic Curve Cryptography (ECC) [14].

Symmetric Encryption. Symmetric encryption is the oldest encryption model and the first to be used. It is still the most widely used type of encryption today. The basic symmetric encryption model has five basic items [4]: 1. **Cleartext:** It is the original message or data, in readable format, that serves as input to the encryption algorithm; 2. **Encryption algorithm:** Performs several substitutions and transformations in the clear text; 3. **Secret key:** The key is the code used for the algorithm to perform the substitutions and transformations in the clear text resulting in a ciphertext; 4. **Ciphertext:** is the scrambled message, produced by the encryption algorithm. The ciphertext is the set of clear text plus the secret key; 5. **Decryption algorithm:** is the encryption algorithm

performed in reverse. Ciphertext and secret key are required. The output of the algorithm is the original clear text [4], [15].

For an encryption algorithm to be considered strong, it must be unfeasible to decrypt a message with only the ciphertext and knowledge of the algorithm, that is, the algorithm is as strong the greater the strength of the key used to encrypt the cleartext. The key must be shared through a secure channel [4]. Figure 1 presents, in a simplified way, the flow to encrypt a text with symmetric algorithm [9].

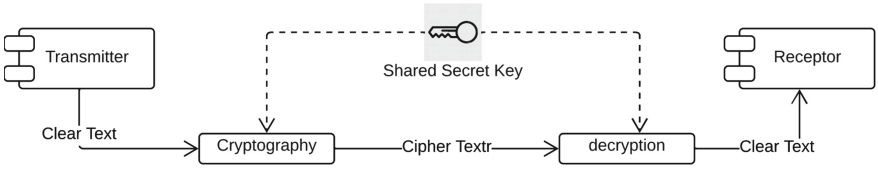

Fig. 1. Symmetric key encryption [9]

The algorithms can be encrypted bit by bit or byte by byte at a time, which is called flow encryption, or blocks of bits can be encrypted at once, usually using 64 or 128 bits at a time to be encrypted. The main symmetric encryption applications are based on the use of the block cipher [4], [16], [17].

Asymmetric Cryptography. Asymmetric cryptography, also called public-key cryptography, is based on mathematical functions, rather than substitution and permutation. Unlike symmetric encryption, asymmetric encryption uses two independent keys [4]. One of the problems that asymmetric cryptography solves is that of sharing the key between the sender and the receiver that occurs in symmetric cryptography. In asymmetric cryptography, there are two keys, one public and one private. One of the keys is for encryption and the other for decryption. The essential features of a secure asymmetric encryption system are [4]:

- It is computationally unable to determine the decryption key, given only the knowledge of the encryption algorithm and the encryption key.
- Either of the two related keys can be used for encryption and the other for decryption.

In asymmetric cryptography, both the public and private keys are generated by the issuer. The private key must be kept securely and must never be shared. The public key can be shared without compromising the security of communication [4], [9].

Figure 2 shows the process used in asymmetric cryptography. If the public key is used to encrypt a message, only the private key can be used to decrypt it.

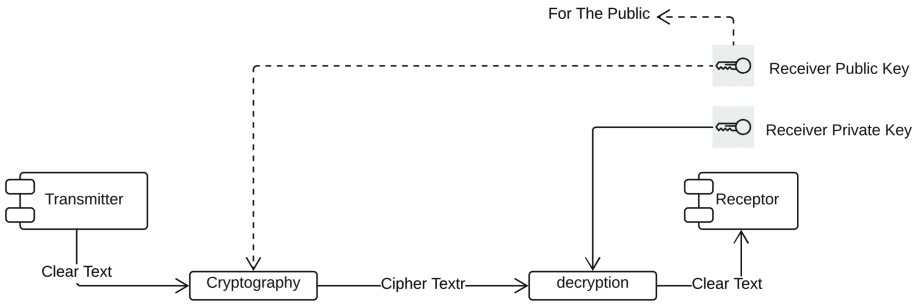

Fig. 2. Asymmetric cryptography [9]

If a message is encrypted with the private key, only the public key can decrypt it, that is, the same key is never used to encrypt and decrypt a message [9].

One of the most common algorithms used is RSA. This algorithm was proposed by Rivest et al. [18]. It is a public key algorithm used to generate a secure asymmetric signature system [19]. This algorithm uses two very large prime numbers, p and q to create public and private keys [9]. For creation, the following steps are followed, as shown in Fig. 3:

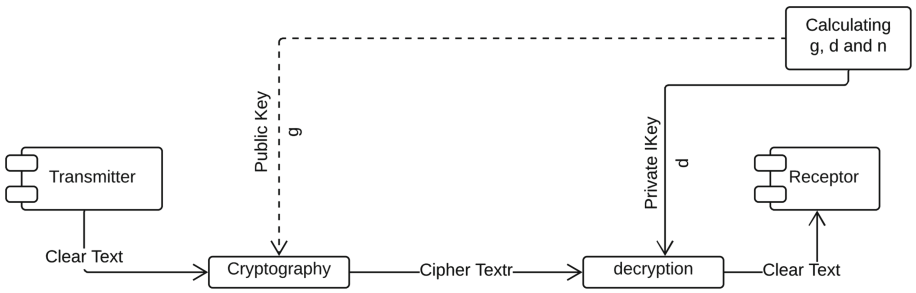

Fig. 3. RSA [9]

- The two prime numbers chosen are multiplied to find out n, which is the module for encryption and decryption, $n = p\ x\ q$.
- Calculate another number $z = (p\ -\ 1)\ x\ (q\ -\ 1)$.
- Choose a random integer g. Then, calculate d so that d is equal to mod z.
- Announces g and n to the public, keeping z and d secret.

To encrypt a message using the RSA algorithm, it is necessary to calculate the clear text with the values of g and n to generate the ciphertext to be sent. The formula used to encrypt clear text is as follows [9]:

$$C = P^g (mod\ n)$$

To safely decrypt a message, the values of z and d must be private. When receiving a ciphertext, the private key d is used to decrypt the message [9].

$$P = C^d (mod\ n)$$

2.2 Digital Signature

The digital signature uses asymmetric cryptography. The public key cryptographic system protects against any third party who is not authorized to access the message. However, it does not protect the two parts of each other [4]. Suppose Bob and Alice exchange messages using the asymmetric encryption scheme, and some problems can arise:

- Alice can forge a different message and claim that it came from Bob.
- Bob can deny sending the message to Alice.

When there is no complete trust between the sender and the receiver, more than asymmetric key authentication is required to exchange messages. To solve this problem, a digital signature is used. The digital signature must have the following characteristics [4]:

- Check the author and the date of the signature.
- Authenticate the content upon signature.
- Be verifiable by a third party.

When there is no complete trust between the sender and the receiver, The digital signature can be based on several algorithms. The scheme used in this work is based on the RSA algorithm. This algorithm is widely used in several applications, including financial, hence the importance of this scheme being considered safe. The guarantee that the RSA function is secure comes from the signature generation operation used to embed the hash value and the message consistency check. Along with RSA, the Probabilistic Signature Schema (PSS) technique is used [4], [20].

The RSA scheme uses exponential expressions. The clear text is encrypted in blocks, with each block being smaller than the n message. Both the sender and the receiver need to know the value of n. The sender knows the value of g, and only the receiver can know the value of d. RSA has two keys: a public one with PU = g, n and a private one PR = d, n. For encryption to be efficient, it must be impossible to determine d from g and n [4]. To encrypt a message using RSA, the following function is used:

$$m^e = c\ mod\ n$$

To decrypt an RSA encrypted message, the following function is used:

$$c^d = n \ mod \ m$$

To introduce greater security in RSA encryption, a PSS padding scheme has been added. A proven secure completion scheme for producing signatures is typically used as a secure encryption scheme. The PSS function uses two functions and the hash for security. Random data is inserted in the message M before the hash algorithm [20] is executed. The main objective of the PSS is to ensure mathematical proof of the real security of the RSA algorithm for encryption [9]. Figure 4 shows the RSA flow.

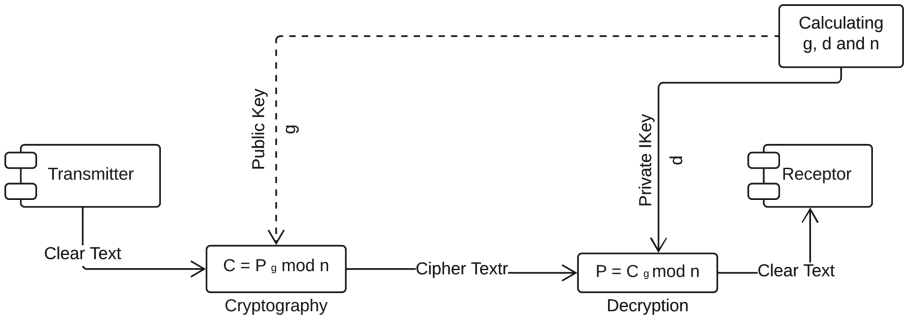

Fig. 4. RSA flow [9]

To encrypt a message with the RSA algorithm, the following steps are performed as shown in the Fig. 4:

- Choose two very large prime numbers, p and q.
- Multiply the two chosen cousins to discover n, which is the module for encryption and decryption.
- Choose a random integer g. Then the value of d is calculated.
- Announces the values g and n to the public. Keeps the value of g and d secret.

2.3 Related Works

Boneh et al. [21], presented the concept of aggregated signature applied in several applications. Aggregation of signatures are useful for reducing the size of the certificate chain and for reducing messages in secure routing protocols. The aggregated signatures, as well as the single signature, are verifiable encrypted. One of the practical applications of signature aggregation is with the X.509 certificate chain that can be aggregated into a single signature.

Shamir [22] presented research on how to divide the data into parts, so that they are easily reconstituted from any piece. Using this technique, it was possible

to build robust key management schemes for cryptographic systems, which can work reliably.

Kumar et al. [23] investigated the need for encryption for images to ensure security against attacks. The work proposes a new algorithm for image security using Elliptic Curve Cryptography (ECC). This algorithm first encodes the RGB image using DNA encoding followed by asymmetric encryption based on Elliptic Curve Diffie - Hellman (ECDHE). The algorithm was applied to test images to analyze the patterns. The results of this study concluded that the proposed algorithm could withstand exhaustive attacks and is suitable for practical applications.

Perin et al. [24] presented a comparison of two modular multiplication architectures. A fully systolic matrix and a parallel implementation. Modular multiplication is used in the modular exponentiation process. One of the most famous cryptographic algorithms is the RSA encryption scheme. The fully systolic matrix architecture features a high-root implementation with transport propagation between the processing elements. The parallel implementation consists of multiplier blocks in parallel with the processing elements and providing a pipeline mode of operation. Time efficiency was compared between the two architectures cited using RSA. The time for the systolic architecture to decrypt 1024 bit using RSA was 3.4 ms, and the parallel architecture was 6 ms. There is a competitive performance between both architectures.

Engelbertz et al. [25] evaluated the validation logic of the open-source software library for creating and validating signed documents, provided by the Connecting Europe Facility (CEF) called the Digital Signature Service (DSS), against XML-based attacks. The discovered vulnerabilities allow you to read files from the server and bypass the protection provided by XML Advanced Electronic Signature (XAdES). There is an urgent need for proper security practice documents and automated security assessment tools to support the development of security-relevant implementations.

3 Contextualization

The Federal Government aims to provide various services digitally. In the educational area, the Ministry of Education (MEC) has as main objective the digitization of diplomas. According to the planning proposed by the MEC, all Brazilian Federal Universities must have the possibility of issuing secure diplomas in digital format by 2022 [7].

There are three ordinances created by MEC that regulate the issuance of diplomas in digital format. Ordinance No. 330/2018 establishes the digital diploma of all federal public and private higher education institutions. Article 2 mentions that the diplomas and documents must comply with the digital certification guidelines of the IPC-Brasil Public Keys infrastructure standard [26].

Ordinance Number 554/2019, in its article 2, specifies what a digital diploma is. According to this ordinance, a digital diploma is one that has the existence, its emission, and storage entirely digital, whose legal validity is presumed through

the signature with digital certification and time stamp according to ICP-Brasil [27].

The storage of the digital diploma must be done in a computational environment that guarantees: validity at any time, interoperability between systems, security technology update, and the possibility of multiple signatures on the same document. The certificate used must be A3 or higher. According to ordinance 554/2019, all diplomas must be issued in Extensible Markup Language (XML) format based on the advanced electronic signature in the XML Advanced Electronic Signature - XAdES standard and the signed XML code must be conditioned to an Uniform Resource Location - unique URL. In addition to these mechanisms, the signed diploma must have associated with it a Quick Response Code - QR Code, which redirects to the unique diploma validation URL [27].

Ordinance 1.095/2018 regulates the process of registering diplomas in digital format. All diplomas must be registered in a registration book which must contain the opening, closing and must be signed by the competent authority. The record book must be in digital format and meet the specifications of ICP-Brasil [28]. According to what was presented in the legislation above and the deadline for the implementation of a solution for signing diplomas and documents in digital format, the University of Brasília (UnB) must build a solution adhering to the standards determined by the MEC.

The current architecture of UnB's systems is focused on the integration between the systems. Software integration enables the automation of business processes with improved resource management. There are now several legacy systems that are still widely used in UnB [29]. Currently, UnB systems are focused on architecture based on the Domain-Driven Design (DDD) concept, and one of the main concepts is the subdivision of a large business domain into smaller domains. Another fundamental concept of DDD is the use of a ubiquitous language to express the domain terms as the experts refer, making it possible to create a common vocabulary that all members of the project understand [30].

Due to the use of smaller domains and with greater consistency of a ubiquitous language, it was necessary to divide the large systems into a service-oriented approach. There are several services created by UnB; each of these services offers specific functionality that can be integrated to create an application. The services can be reused in several different applications [30].

Currently, there is a separation between front-end applications, which are created using the Angular language, using the modular architecture that the language offers [31]. There is an ems-bus services bus that integrates front-end applications and back-end services, which are currently developed in the java language. Also, ems-bus has several services, called bus modules, for specific functions [30].

The language used on the ems-bus is the Erlang language, which is a functional language with a great emphasis on simultaneity and high reliability. It is a language capable of executing dozens of tasks at the same time. Erlang uses the thread model where each thread is a separate process. With this lan-

guage, several independent processes can be created, which offers the possibility of developing several modules and integrating them into the ems-bus [32].

The main modules of the ems-bus are: the service communication module through REST technology; the authentication module in the LDAP protocol format; the authentication module in the Oauth 2 protocol format [30]. This will develop an architecture for future implementation and implantation of a module inside the digital signature ems-bus in the standards determined by the Brazilian government for signing diplomas and documents in digital format. Figure 5 shows the current internal architecture of the ems-bus, the different modules, and how the new digital signature module will be inserted into the bus.

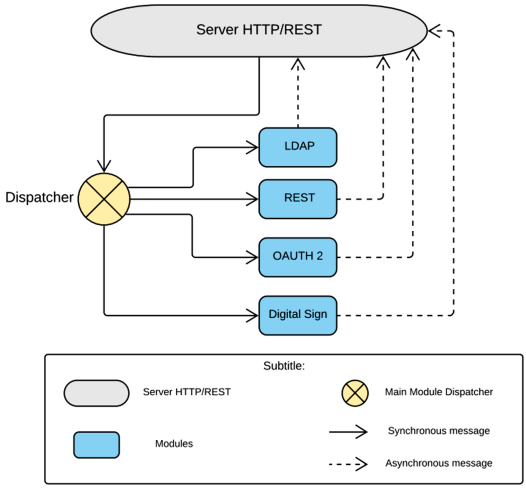

Fig. 5. Bus architecture ems-bus [30]

As shown in Fig. 5, the bus receives an HTTP request for one of the modules on the bus. The central Dispatcher module receives these requests and redirects them to the module called by the HTTP server. The module executes its functionality and returns the required response to the HTTP server [30].

The REST module is the basic module of the ems-bus, which is essential for communication between the other services. The bus works through microservices that exchange messages in the REST format controlled by the main dispatcher module, which acts as a coordinator for the exchange of services [30].

The Oauth 2 module is the main functionality of the authentication and authorization bus. This protocol must comply with the REST architecture and the JSON format for the message exchange. It is crucial because the bus works with the exchange of messages through JSON [33].

The Oauth 2 module uses the OAuth 2.0 library in Erlang available at: https://github.com/kivra/oauth2. This library generates the authentication

token required to access the bus services. The bus's Oauth 2 module controls authentication and authorization [33].

The module to be created is the digital signature module. This module aims to sign XML documents and return them signed in the XAdES standard. The module will be created in the service format, where the path of the compressed documents in zip format to be signed must be passed in the payload and also the path of the A3 token, already installed and configured on the machine, which will sign the document. The HTTP call must be made using the url "/certificate/document/sign" with the paths of the documents to be signed and the certificate in the request payload, as shown in Fig. 6:

```
{
    "zip_file":"{path of zip file}",
    "cert_file": "{path of the cert}"
}
```

Fig. 6. Subscription Service Call Payload

The return of the digital signature module must be all XML documents signed in the XAdES standard compressed in zip format. For this functionality, an HTTP call must be made to the url "/certificate/document /verify" passing the signed XML document in the payload. The HTTP callback includes the document url and a Boolean attribute to check whether the document is valid or not.

Each of the digitally signed documents must be accessible on the internet at an address. For this purpose, it is necessary that each of the signed diplomas has its own access url.

3.1 Internal Architecture of the Digital Signature Module

Within the ems-bus, we have created a new digital signature module within the certification package. Figure 7 shows how this module is organized.

The CriptoSign.erl class is the class that has the methods responsible for signing an xml document in the XAdES standard. The class CryptoVality.erl is the class responsible for checking signed documents and returning the document's storage url. The class CriptoUtil.erl is the class that performs tasks such as reading certificates, converting formats, generating dates, and converting to the format accepted by XAdES, in addition to generating the structure of the XAdES standard.

For the subscription system to be recognized by the bus, it must be mapped within a catalog. Catalogs are the configuration files of the bus modules, with the mapping of a module within a catalog, the main module, dispatcher, can see it. After configuring the catalog correctly, the main dispatcher module is able to redirect calls made to the digital signature module.

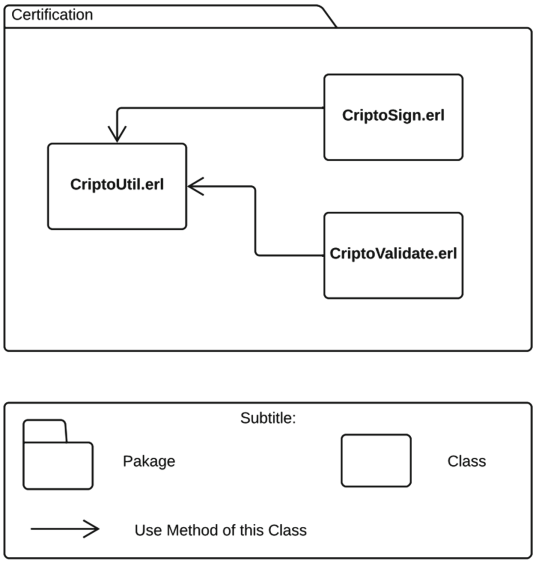

Fig. 7. Digital signature module architecture

Figure 8 presents an example of a document signed by a prototype of the digital signature system developed as a solution for UnB. The implementation proved to be correct, and the digital signature was carried out successfully on the documents. The current system does not fully sign the standard determined by the MEC, and the certificate used for testing is A1. This prototype will be evolved so that the proposed solution is in accordance with that determined by MEC.

4 Threats to Validity

During this work, we tried to select the primary references related to the topics covered in this research. However, we cannot guarantee that all relevant papers were selected during the literature review. Some relevant articles may not have been selected during the process. To minimize this threat, we conducted searches on digital databases using a Search String in the following digital databases: web of Science, Scopus, IEEE Xplore Digital Library, and ACM Digital Library. Also, we use the VOSviewer software that selects the most relevant articles from the total selected articles [34].

Another threat to the implementation of the digital signature system at UnB if MEC changes the guidelines on the digital signature system, such as changing XAdES to another form of signature, or imposing the use of a third-party system. To minimize this problem, we made a system that can be adapted to other subscription standards. The system to be developed will be presented to MEC



```
<?xml version="1.0" encoding="UTF-8"?>
<Diploma ID="941ce80d-a2ff-4896-a900-8f44fdb905d8">
   <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
         <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
         <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
         <ds:Reference URI="#941ce80d-a2ff-4896-a900-8f44fdb905d8">
            <ds:Transforms>
               <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
               <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
            </ds:Transforms>
            <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
            <ds:DigestValue>l6AXbMecAzLWi898YhIhyQ/BZi5ktbSS/SWi5b0KbVo=</ds:DigestValue>
         </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>lm9XGKZm2O/wIdDMqTlhrgpyJE5FK3tkAqSSQsf/mZOjJiG/Ac/L+Mu8a1sZfUr6SevF6dzVTSn0u7WEAfY85PbcEicevrH+t+
      gTSPXqbvkkmg2l/jlyzu8hVIoml7gHBzBDHe1lc2mczKhOvEn3QV5Z1YaWPvTvyQjMVbnJmlxejIlUgITVrZpPkYTNQH/8XVK2jwUCK7hFN+QVWSW43aT
      AQLtVbtFneqpdwRRzaeXjD9EqKhhc39VcwP10HLgz5rSG/UchndikIqQ6hUF/GMT9mwm6Nz5BNWwImb9zqav3Nvs6xqug+vh6lrk20GgQEBwxH0EtYvaK
      tlhmJwMgeA==</ds:SignatureValue>
      <ds:KeyInfo>
         <ds:X509Data>
            <ds:X509Certificate>MIIGrDCCBJSgAwIBAgIRAJU2pTS6KVlBglk8rau46AkwDQYJKoZIhvcNAQELBQAwUDELMAkGA1UEBhMCQlIxGDAWBgNV
            BAoTD0xhY3VuYSBTb2Z0d2FyZTELMAkGA1UECxMCSVQxGjAYBgNVBAMTEUxhY3VuYSBDQSBUZXN0IHYxMB4XDTE5MDEyMTIwMzQ1OFoXDTIyMDEy
            MTIwMzQyNFowRjELMAkGA1UEBhMCQlIxGDAWBgNVBAoTD0xhY3VuYSBTb2Z0d2FyZTEdMBsGA1UEAxMUQWxhbiBNYXRoaXNvbiBUdXJpbmcwggEi
            MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDFBybE4UxKh1LxYfzM6dYK9Qfcx5mDXGd3RDP/O1l3lVeDNCnNt2aHxEkzpeYH5OrHf+fXGWl/
            FGyWpRg0wbve8DJLwzKjW0IcK1qTJx78mTu84UHwHZFbHg5XEo+uYJD/66GwKhfsJNlFtsOITTkC2Ogx/mtPsReFoWZSM1RdYcoDK4/egI4DYaBO
            +7prF82yNQZQ3zjnbmOntLObfQEIFOY3zBGQCJwuUSh8i5LVl94vrKWTJwchVRRXI8LcXqpO0H+6RC3ppw6WshAZNcI4iBDFT/HJNu/0ondKpkHH
            BIBULYZmn2dvQvg9N4Y9JWUXElWPXngg/PCxQYjHxnzNAgMBAAGjggKJMIICChTAJBgNVHRMEAjAAMIGdBgNVHREEgZUwgZKgOAYFYEwBAwGgLwQt
            MDAwMDAwMDA1NjA3MjM4NjEwNTAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
            MDAwMDAwMDAwMDAwMDAwgR10ZXN0dHVyaW5nQGxhY3VuYXNvZnR3YXJlLmNvbTCB3QYDVR0fBIHVMIHSMESgQqBAhj5odHRwOi8vYW1wbGlh
            LXIxLmxhY3VuYXNvZnR3YXJlLmNvbS9jcmxzL2xhY3VuYS1jYS10ZXN0LXYxLmNybDBEoEKgQIY+aHR0cDovL2FtcGxpYS1yMi5sYWN1bmFzb2Z0
            d2FyZS5jb20vY3Jscy9sYWN1bmEtY2EtdGVzdC12MS5jcmwwRKBCoECGPmh0dHA6Ly9hbXBsaWEtcjMubGFjdW5hc29mdHdhcmUuY29tL2NybHMv
            bGFjdW5hLWNhLXRlc3QtdjEuY3JsMIH3BggrBgEFBQcBAQSB6jCB5zBLBggrBgEFBQcwAoY/aHR0cDovL2FtcGxpYS1yMS5sYWN1bmFzb2Z0d2Fy
            ZS5jb20vY2VydHMvbGFjdW5hLWNhLXRlc3QtdjEuY2VyMEsGCCsGAQUFBzAChj9odHRwOi8vYW1wbGlhLXIyLmxhY3VuYXNvZnR3YXJlLmNvbS9j
            ZXJ0cy9sYWN1bmEtY2EtdGVzdC12MS5jZXIwSwYIKwYBBQUHMAKGP2h0dHA6Ly9hbXBsaWEtcjMubGFjdW5hc29mdHdhcmUuY29tL2NlcnRzL2xh
            Y3VuYS1jYS10ZXN0LXYxLmNlcjANBgkqhkiG9w0BAQsFAAOCAgEAmM4tBC3kq4j2D6V+KPc3eg0ILn7Yj6qvfG/pJT0AW5V4SXNTyFX34WAtPzer
            vauVwFBhyq/7XiiAQNfgwvU9FMyoxApQnVPMIy3PEoJTqC+C5R0JDjHcQUdNxIv7djPeFAkadVfiWoxhov+k3MzOu0lfnxes/sEEmEHYD0aZgxtm
            1atD3SGsmHV6T7gpj1ZfKu3ZFpxNhPXb3TPEyPSzsbTfnqoPPD/u4s8uU2Anatwccx96eWzDB4ThSqgC5zlqK3QOTMwJ4gZPNey+3Y6Cctl3en5a
            gTVpMQwSpGj1P87kho1qi9oHYGY5ESuWcPYhpwx9dnfzmjGoZNuLxtIh3ceOBMO8X6IWID5sQArvAzZm8smfudBYhcaZf7wlW2NFWmvD3wD1uxn2
            16ILs2wJTs0VKu/sZ17bnWw5mY07Gfm6XfBuBYDIAVQu5v4s/R9hwjLMOgek3Qx3ILlZnsS8LiuIVfm+f52OsAY/D7XYo7PCfJOzOttDKQ07PkC7
            8SZ+hoN46uUHc1Sdb7l5RAKK66g2z3jccgs4+S432iyJAIjxdUcOTJE4m9+p5tJISCI2hkCQ6mo8TgfHkgRvELlgi9bCZxAUec2ibtgZnLt2QjgV
            16uK4UfphxBNgKnPmpAlvpW47N0Mz1mxae81Te5IwefUlP8j/mQx1KVQ5kq81MQ=</ds:X509Certificate>
         </ds:X509Data>
      </ds:KeyInfo>
   </ds:Signature>
   <content>Content of the certificate...</content>
</Diploma>
```


Fig. 8. Digital signature example

for validation and possibly be one of the systems accepted by MEC and ICP-Brasil for signing documents in digital format.

One of the threats to the implementation and implementation of a digital signature solution is the fact that the system performs the signature quickly and reliably for signing multiple certificates. Most signature solutions take about minutes to execute the signature of a large number of documents. The solution that UnB needs is to sign a large number of documents in a short time and reliably, that is, that all documents are signed correctly. To minimize this threat, the Erlang [32] language was chosen for the development of this solution. This language is a robust language and has a high fault tolerance.

5 Conclusion

In Brazil, the current government aims to digitize a large part of public services. In the educational area, two essential services must be in digital format. The generation of documents such as: school history, declaration of active student, among others. Another valuable service is that of diplomas that must be issued in digital format. The MEC standardized how documents and diplomas should

be generated in digital format and how they should be signed so that they have a valid format.

This work presented the central norms and requirements for the creation of a solution for signing documents and diplomas in digital format. Also, it was shown how the new UnB systems architecture works and how the digital signature system will be inserted into that architecture. It was shown each of the components to be developed and how these components interact with each other and how they will interact with the current architecture created.

We also present the possible threats that could compromise the creation of a digital signature solution for UnB. It was also shown the possible solutions to be taken for each threat to try to minimize the effects of the threats in this project.

In the future, the digital signature system will be developed in accordance with all ordinances and regulations of the MEC. It is essential for future work to verify the real security implemented in the signature systems using a signature using the XAdES standard and to compare it with the other primary existing standards such as CAdES and PAdES.

References

1. Whitman, M.E., Mattord, H.J.: Principles of information security. In: Cengage Learning (2011)
2. Regulation, G.D.P.: Eu data protection rules. In: European Commission (2018). https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en. Accessed 9 Oct 2019
3. da República, P.: Lei geral de proteção de dados pessoais (LGPD). In: Secretaria-Geral (2018). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html. Accessed 9 Oct 2019
4. Stallings, W.: Network and Internetwork Security: Principles and Practice. Prentice Hall, Englewood Cliffs (1995)
5. Rivest, R.L.: A method for obtaining digital signature and public-key cryptosystems. Communi. ACM **21**, 2 (1987)
6. Tycksen Jr., F.A., Jennings, C.W.: Digital certificate, uS Patent 6,189,097, February 2001
7. da Educação, M.: Diploma digital, Ministério da Educação (2020). http://portal.mec.gov.br/diplomadigital/. Accessed 12 Feb 2020
8. Middelkamp, A.: Online. Praktische Huisartsgeneeskunde **3**(4), 3 (2017). https://doi.org/10.1007/s41045-017-0040-y
9. Forouzan, B., Coombs, C., Fegan, S.C.: Introduction to Data Communications and Networking. McGraw-Hill Inc., New York (1997)
10. Narendra, S.G., Tadepalli, P., Spitzer, T.N.: Symmetric cryptography with user authentication, uS Patent 8,477,940, 2 July 2013
11. Omran, S.S., Al-Khalid, A.S., Al-Saady, D.M.: Using genetic algorithm to break a mono - alphabetic substitution cipher. In: 2010 IEEE Conference on Open Systems (ICOS 2010), pp. 63–67, December 2010
12. Kurniawan, D.H., Munir, R.: Double chaining algorithm: a secure symmetric-key encryption algorithm. In: 2016 International Conference On Advanced Informatics: Concepts, Theory And Application (ICAICTA), pp. 1–6, August 2016

13. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: Proceedings 38th Annual Symposium on Foundations of Computer Science, pp. 394–403. IEEE (1997)
14. Szerwinski, R., Güneysu, T.: Exploiting the power of GPUs for asymmetric cryptography. In: Oswald, E., Rohatgi, P. (eds.) CHES 2008. LNCS, vol. 5154, pp. 79–99. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85053-3_6
15. Forouzan, B.A.: Cryptography & Network Security. McGraw-Hill Inc., New York (2007)
16. Jakimoski, G., Kocarev, L.: Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Trans. Circuits Syst. I Fundam. Theor. Appl. **48**(2), 163–169 (2001)
17. Chunguang, H., Hai, C., Yu, S., Qun, D.: Permutation of image encryption system based on block cipher and stream cipher encryption algorithm. In: 2015 Third International Conference on Robot, Vision and Signal Processing (RVSP), pp. 163–166, November 2015
18. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
19. Bellare, M., Rogaway, P.: The exact security of digital signatures-how to sign with RSA and Rabin. In: Maurer, U. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 399–416. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-68339-9_34
20. Coron, J.-S.: Optimal security proofs for PSS and other signature schemes. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 272–287. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-46035-7_18
21. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 416–432. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_26
22. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979). https://doi.org/10.1145/359168.359176
23. Kumar, M., Iqbal, A., Kumar, P.: A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. Signal Process. **125**, 187–202 (2016). https://www.sciencedirect.com/science/article/pii/S0165168416000347
24. Perin, G., Mesquita, D.G., Herrmann, F.L., Martins, J.B.: Montgomery modular multiplication on reconfigurable hardware: fully systolic array vs parallel implementation. In: 2010 VI Southern Programmable Logic Conference (SPL), pp. 61–66, March 2010
25. Engelbertz, N., Mladenov, V., Somorovsky, J., Herring, D., Erinola, N., Schwenk, J.: Security analysis of XAdES validation in the CEF digital signature services (DSS). In: Rossnagel, H.D., Wagner, S. (eds.)Gesellschaft fur Informatik (GI), vol. P-293, pp. 95–106, cited By 0 (2019)
26. da Educação, M.: Portaria n 330, de 5 de ABRIL de 2010. In: Ministérioda Educaçñ (2018). http://www.in.gov.br/materia/-/assetpublisher/Kujrw0TZC2Mb/content/id/9365055/do1-2018-04-06-portarian-330-de-5-de-abril-de-2018-9365051. Accessed 15 Feb 2020
27. da Educação, M.: Portaria n 554, de 11 de março de 2019. In: Ministério da Educaçã (2019). http://www.in.gov.br/materia/-/assetpublisher/Kujrw0TZC2Mb/content/id/66544171/do1-2019-03-12-portarian-554-de-11-de-marco-de-2019-66543842. Accessed 20 Feb 2020

28. da Educação, M.: Portaria n 1095, DE 25 DE OUTUBRO DE 2018. In: Ministério daEducaçã (2018). https://abmes.org.br/arquivos/legislacoes/Port-MEC-1095-2018-10-25.pdf. Accessed 22 Feb 2020
29. Agilar, E., Almeida, R., Canedo, E.: A systematic mapping study on legacy system modernization. In: SEKE. KSI Research Inc. and Knowledge Systems Institute Graduate School, pp. 345–350 (2016)
30. Agilar, E.D.V.: Uma abordagem orientada a serviços para a modernização de sistemas legados, Universidade de Brasìlia (UnB) (2016)
31. Angular.io: Agnular fundamentals Angular.io (2020). https://angular.io/guide/architecture. Accessed 01 Mar 2020
32. Erlang/OTP: Erlang getting started with erlang user's guide Erlang OTP (2019). https://erlang.org/doc/getting_started/conc_prog.html, Accessed 03 Mar 2020
33. Ribeiro, A.D.S.: Uma implementação do protocolo oauth 2 em erlang para uma arquitetura orientada a serviço, Universidade de Brasìlia (UnB) (2017)
34. Van Eck, N., Waltman, L.: Software survey: VOSviewer, a computer program for bibliometric mapping. Scientometrics **84**(2), 523–538 (2009)