الجمهورية الجزَائِرية الديمقرَاطية الشعبية
PEOPLE'S DEMOCRATIC REPUBLIC OF ALGERIA
وزَارة التعليم العَالي و البحث العلمي
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH
جَامعة عمَار ثليجي بِالأَغوَاط
AMAR TELIDJI UNIVERSITY OF LAGHOUAT

FACULTY OF SCIENCES
DEPARTMENT OF COMPUTER SCIENCE

Presented to obtain the Master degree

Field: Computer Science

Option: Distributed Networks, Systems, and Applications

Presented by:

Souhila Roufida NEBEG **Samah Khouloud CHEKNANE**

Theme

DESIGN AND IMPLEMENTATION OF DIGITAL SIGNING SYSTEM

Publicly defended on 20-06-2023 before the jury members composed of:

Prof. Nasredine LAGRAA	Prof	President	Laghouat University
Dr. Nouredine CHAIB	M.C.A	Examinator	Laghouat University
Dr. Abdelmadjid BENARFA	M.C.B	Examinator	Laghouat University
Dr. Mohamed Lahcen BENSAAD	M.C.B	Supervisor	Laghouat University

Academic year 2022/2023

Dedication

I would like to start by saying Alhamdulillah for granting me strength and patience to overcome all the trials experienced during this thesis.

I dedicate my work, sincerely, to my loving parents, Mohammed and Gherbi Rabia. My brothers Belkacem, Aymen and Abd el rahmane.
My sisters Amina and Kaouthar. And my friends Ikram, Aisha, Rahil, Saida and Chahed Nour.

And to all my friends in the Quran school: khadidja, Siham, Maroua, Maria, Hined, Sabrina, Nada and Asma. And also to my teacher in the Quran Dada Radia.

Souhila

Dedication

I would like to dedicate this modest work to all those who have encouraged me throughout the period of the realization of the project particular :

- *My parents (Ali and Siham) and my dear sisters (Radia, Ines, Razika, Imane) and to my dear grandparents: (Aisha and Lazhari Chouarani).*

Samah

Acknowledgments

First, thanks to Allah for giving us the strength to complete this work.

We wish to express our sincere gratitude to our supervisor Dr. Bensaad Lahcen, who guided us and who made sure to provide us with all necessary information, valuable knowledge and advice.

Also we thank the members of the jury for their time to read and examine this work.

Finally, we would like to express our deep gratitude to our families and to all our teachers who have contributed to everything we learned throughout our academic career.

We thank everyone who helps us in this work.

ملخص:

في العصر الرقمي اليوم، يعد ضمان أمن وسلامة مستندات الشركة الحساسة أمرًا بالغ الأهمية. يمكن أن يؤدي الوصول غير المصرح به أو تعديل هذه المستندات إلى عواقب وخيمة على المؤسسات. نحاول في مشروعنا تنفيذ نظام توقيع رقمي قوي يستخدم التعمية اللا تناظرية ورموز الاستجابة السريعة ودوال التجزئة لحماية مستندات الشركة الحساسة ومنع التعديلات غير المصرح بها بشكل موثوق. يستفيد النظام المقترح من قوة التعمية اللا تناظرية لتوفير قنوات اتصال آمنة بين الموقعين على المستندات والمستلمين. يُنشئ النظام توقيعاً رقمياً فريداً لكل مستند باستخدام المفتاح الخاص، مما يضمن صحتها وسلامتها. لتعزيز قابلية استخدام النظام وإمكانية الوصول إليه، يتم استخدام رموز الاستجابة السريعة كطريقة ملائمة للتحقق من المستندات. تحتوي كل وثيقة موقعة على تمثيل رمز الاستجابة السريعة لتوقيعها الرقمي، مما يسمح للمستلمين بالتحقق بسهولة من موثوقيته وسلامته باستخدام جهاز محمول أو برنامج مخصص.

الكلمات الدالة: التوقيع الرقمي، التعمية اللا تناظرية، خوارزمية RSA، رمز الاستجابة السريعة.

Résumé:

À l'ère numérique d'aujourd'hui, garantir la sécurité et l'intégrité des documents sensibles d'une entreprise, est d'une importance capitale. L'accès non autorisé ou la modification de tels documents peut avoir de graves conséquences pour les organisations. Dans notre projet, nous essayons de mettre en place un système robuste de signature numérique qui utilise la cryptographie asymétrique, les codes à réponse rapide et les fonctions de hachage pour protéger de manière fiable les documents sensibles de l'entreprise et empêcher toute modification non autorisée. Le système proposé exploite la puissance de la cryptographie asymétrique pour fournir des canaux de communication sécurisés entre les signataires et les destinataires des documents. Le système génère une signature numérique unique pour chaque document en utilisant la clé privée, garantissant ainsi son authenticité et son intégrité. Pour améliorer l'utilisabilité et l'accessibilité du système, les codes à réponse rapide sont utilisés comme méthode pratique de vérification des documents. Chaque document signé contient une représentation de sa signature numérique sous forme de code à réponse rapide, permettant aux destinataires de vérifier facilement son authenticité et son intégrité à l'aide d'un appareil mobile ou d'un logiciel dédié.

Mots clés: signature numérique, cryptographie asymétrique, algorithme RSA, code QR.

Abstract:

In today's digital era, ensuring the security and integrity of sensitive corporate documents is of paramount importance. Unauthorized access or modification of such documents can have severe consequences for organizations. In our project we try to implement a robust digital signing system that employs asymmetric cryptography, quick response codes, and hash functions to safeguard sensitive corporate documents and prevent unauthorized modifications reliably. The proposed system leverages the power of asymmetric cryptography to provide secure communication channels between document signers and recipients. The system generates a unique digital signature for each document using the private key, ensuring its authenticity and integrity. To enhance the usability and accessibility of the system, quick response codes are employed as a convenient method for document verification. Each signed document contains a quick response code representation of its digital signature, allowing recipients to easily verify its authenticity and integrity using a mobile device or dedicated software.

Keywords: digital signature, asymmetric cryptography, RSA algorithm, QR code.

Contents

List of Figures

Acronyms:

QR-Code Quick Response code

SHA-256 Secure Hash Algorithm 256-bit

RSA Rivest-Shamir-Adleman

GCD Greatest Common Divisor

UML Unified Modeling Language

DS Digital Signature

CSS Cascading Style Sheets

HTML Hyper Text Markup Language

GnuPG/GPG GNU Privacy Guard

GUI Graphical User Interface

Chapter 1

General Introduction

1.1 Introduction

There is still a need paper-based document in certain circumstances where electronic documents cannot efficiently replace them. For example, documents issued by the government as birth certificates, driver licenses, and passports, an insurance documents, or a contracts, must be paper-based.
Despite the advancement of technology, some institutions and companies still rely on traditional handwritten signatures, which necessitates being physically present in the office to authenticate documents. This approach persists despite the availability of digital signature solution. Embracing digital signatures can unlock numerous benefits, such as accelerated business processes, reduced paper usage, and improved efficiency in a rapidly digitizing world.

1.2 Problematic

With the technological advancement of digital printing and scanning that can be obtained at low costs but has very high efficiency and quality, criminals can easily produce counterfeit documents for defrauding. This makes it difficult to differentiate the counterfeit documents from the authentic documents. By misusing modern equipment whether it is a scanner, a printer or a plotter, it is regarded as a threatening danger to the nation's security and economy.

1.3 The purpose of our project

The purpose of our project presented in this report is to verify the integrity of a text document and the author of a document using a digital signature and a QR code.
In this work, we will present the process of authenticating paper-based documents that can be used quite conveniently, quickly, and semi-automatically, by applying digital signature and QR code. This enables the verification of the documents without depending on any special institute.

1.4 Current implementations and related works

There are numerous works related to digital signatures, indicating the significance of this field. These works encompass various techniques, standards, and practices aimed at ensuring data integrity, authentication, and secure communication.

Listed below three noteworthy initiatives that utilize cryptographic principles to safeguard and maintain the security and integrity of data and communications. GNU Privacy Guard (GnuPG) relies on encryption and digital signatures, OpenTimestamps leverages cryptographic hashes and the Bitcoin blockchain for timestamping data, while Keybase employs end-to-end encryption.
In Figure 1.1, we will represent a table of comparison between GnuPG, OpenTimestamps and Keybase in terms functionality, encryption, security, identity verification, usability and accessibility:

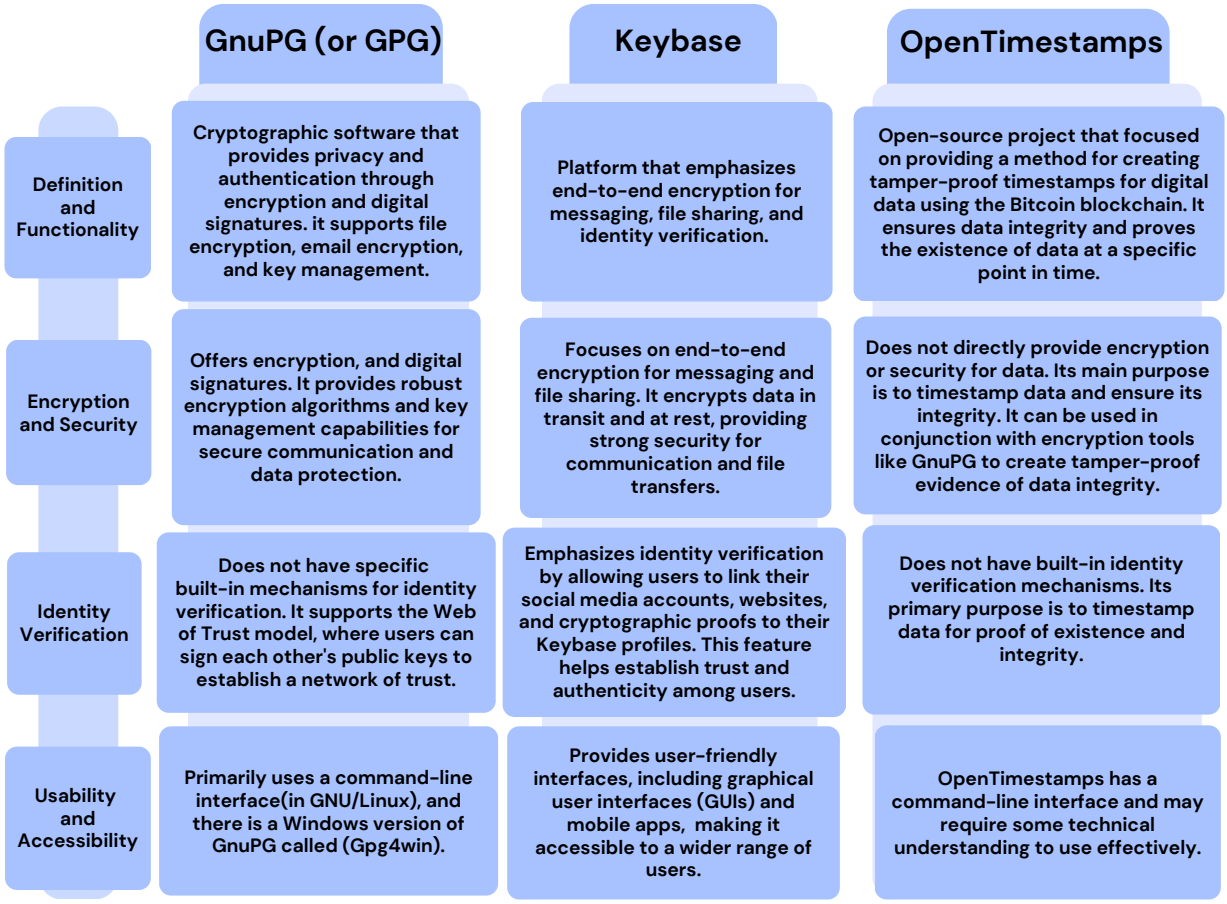


Figure 1.1: Comparison between GnuPG, OpenTimestamps and Keybase

It's important to note that OpenTimestamps, Keybase, and GnuPG serve different purposes and can complement each other in various scenarios. OpenTimestamps focuses on timestamping data, Keybase emphasizes secure communication and identity verification.
GnuPG, which stands out as the tool most closely aligned with our system, provides encryption and digital signatures.
Unlike the others, our system not only encrypts to generate digital signatures but also decrypts to validate the integrity and authenticity of signed documents.
The choice of which tool to use depends on your specific requirements and the level of security and functionality you need for your use case.

1.5 Thesis organization

Apart from this introductory chapter, this report includes three other chapters: the first is dedicated to learning about the techniques and algorithms used to implement our system. The second is dedicated to the design of our system. The third is dedicated to implementation and explanation of the system. We wrapped it up with a general conclusion.

Chapter 2

Definitions of used techniques and algorithms

2.1 Introduction

In this chapter we will introduce the techniques and algorithms used in this project and explain how they are used to implement a digital signature system.

2.2 Cryptography

Cryptography is the practice and study to secure information from unauthorized access, it is the art and science of converting the plain text into cipher text.
The process of retrieving the plain text from the cipher text is called decryption. Here are four main objectives of cryptography:

- Confidentiality: Ensuring that no one can read the message except the intended receiver.
- Data integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Authentication: The process of proving one's identity.
- Non-repudiation: Prevents individuals from denying their responsibilities or actions [1].

2.2.1 Symmetric cryptography

Symmetric cryptography algorithms use the same key for both encryption and decryption. Simply it can be understood as both the sender and the receiver uses same key to send or receive the message [2].

2.2.2 Asymmetric cryptography

Asymmetric cryptography algorithms use two keys which can be referred to as public key and private key. Public key is given to everyone and is used for encryption purpose and private key have to be secret, and is used for deccryption purpose. These two keys are mathematically related, but it is very difficult to obtain one from the other unless one knows the transformation [2].

2.3 RSA algorithm

Rivest-Shamir-Adleman (RSA) algorithm is an asymmetric cryptography algorithm. It works by using two different keys (public key and private key), the public key is given to everyone and the private key is kept private.

The RSA algorithm takes two main steps:

- Key generation:

  1. Choose two large prime numbers (p and q)
  2. Calculate

  $$(1) \quad N = p * q \ and \ \Phi(N) = (p - 1)(q - 1)$$

  $$Where \ \ \Phi(N) \ \ represents \ Euler's \ totient \ function.$$
  $$And \ N \ is \ a \ positive \ integer.$$

  3. Choose a number e where:

  $$(2) \quad 1 < e < \Phi(N) \ and \ GCD(e, \Phi(N)) = 1$$

  4. Calculate:

  $$(3) \quad d = e^{-1} mod \, \Phi(N)$$

  5. We get the private key pair (d, N) and the public key pair(e, N)

- Encryption/Decryption function:
  Once the keys are generated, you can encrypt/decrypt a text:
  Encrypt with this equation:

$$(4) \quad Ciphertext = plaintext^e \; mod \; N.$$

  Decrypt with this equation:

$$(5) \quad Plaintext = ciphertext^d \; mod \; N.$$

For more information you can check this article [3].

2.4 Hash functions

Hash functions, map a large collection of messages into a small set of message digests and can be used for error detection, by appending the digest to the message during the transmission. The errors can be detected when the digest of the received message is not equal to calculated message digest [4]. Cryptography hash functions are one of the most important tool in the field of cryptography and are used to achieve a number of security goals like authenticity, digital signatures, pseudo number generation, digital stenography.

2.4.1 Secure Hash Algorithm 256-bit(SHA-256)

The SHA-2 family is a set of cryptographic hash functions. The SHA-2 family includes six hash functions named SHA-224, SHA-256 or SHA-512/256, SHA-384, SHA-512, SHA-512/224. They are actually the same algorithm but with different word lengths, constant parameters, and initialization values. SHA-256 is known as representative of the SHA-2 family and is currently applied to secure data in many applications [5].

- SHA-256 calculates a 256-bit hash value for an input message.
- The message is divided into many 512-bit data blocks.
- If the last block is smaller than 512 bits, padding is added.
- The SHA-256 algorithm computes intermediate hash values for data blocks one by one. where the current block's hash value serves as the input beginning hash for computing the hash of the next data block.
- The result of the final data block is considered to be the hash value of the entire message.

2.5 Digital signature

A digital signature is formed by encrypting the entire message or the hash code of the message with the sender's private key. Confidentiality can be provided by further encrypting the entire message plus signature with either the receiver's public key encryption or the shared secret key, which is conventional encryption [6].

2.6 QR code

Quick Response (QR) codes are versatile. A piece of long multilingual text, a linked URL, an automated SMS message, a business card or just about any information can be embedded into the two-dimensional barcode. Coupled with moderate equipped mobile devices, QR codes can connect the users to the information quickly and easily [7].

2.7 How these techniques are used?

What we want to achieve is the process of signing the documents in PDF formats, in addition to the process of verifying the digital signature's owner identity in the scanned documents.
We will use the SHA-256 hash function to generate a hash value of document and use it along with an RSA private key as an input to the RSA algorithm to encrypt it and generate a digital signature, then create a QR code for the digital signature generated and add it to the document to produce a signed document Figure 2.1.

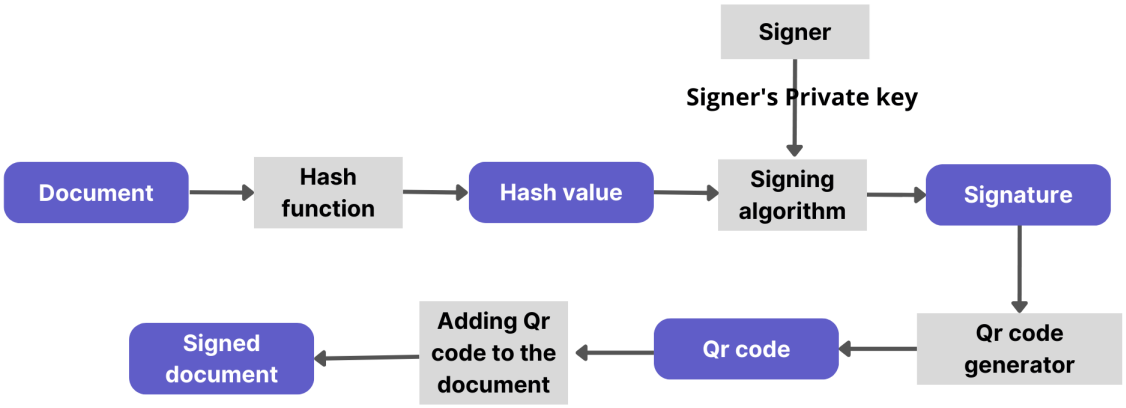


Figure 2.1: Document signing scenario

In the process of verifying the signature, we decrypt the signature using an RSA public key to obtain the hash value, then we compare it with the hash values in the database to ensure the validity of the document and the owner of the signature Figure 2.2.

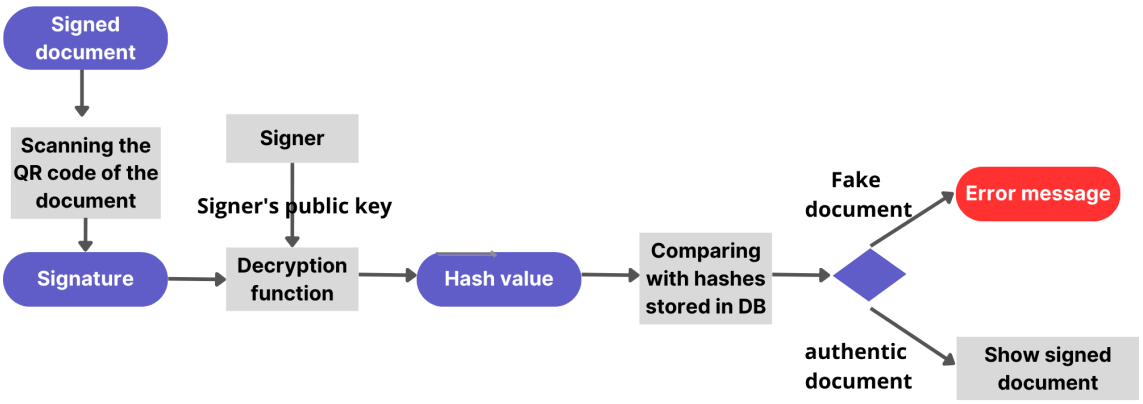


Figure 2.2: Signature verification scenario

2.8 Conclusion

In this chapter, we have explained the use of aforementioned techniques and algorithms to implement our system. We will elaborate on explaining the design in the next chapter to make it more clear how it works.

Chapter 3

Design of the System

3.1 Introduction

In this chapter, we will model our system with the UML. We will use mainly three types of diagrams: class diagram, use case diagram and sequence diagram.

3.2 Class diagram

The Figure 3.1 represents a class diagram of our digital signing system. The main classes are the signer class and the document class. When the document undergoes processing using signing algorithm and hash function, a signed document is generated.

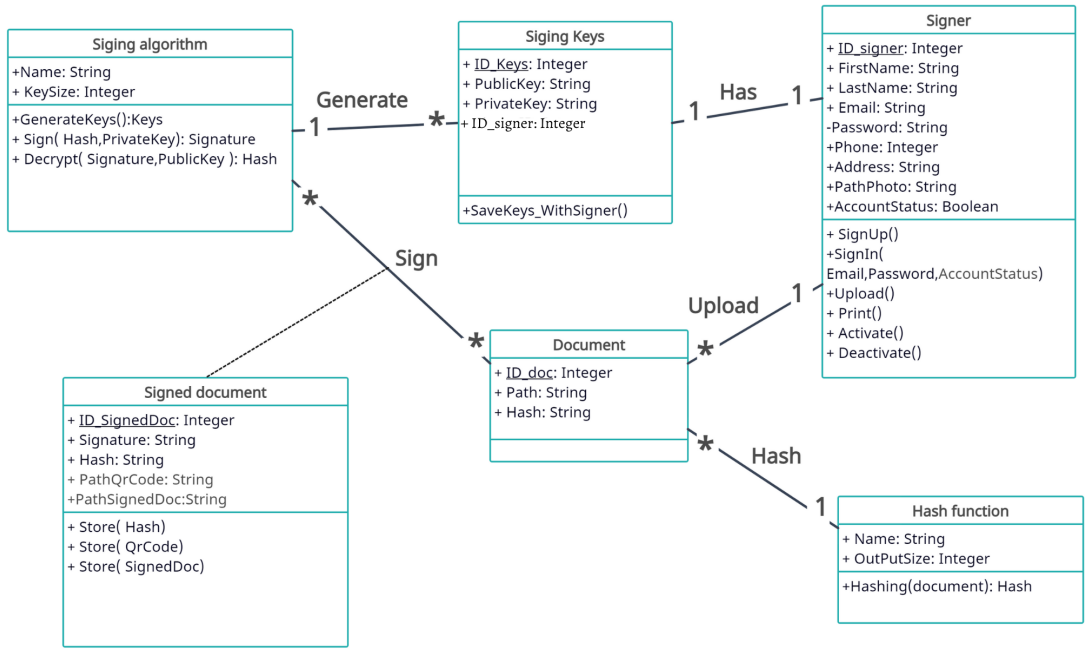


Figure 3.1: Class diagram of digital signing system

When the signer registers in the system for the first time, he gets a pair of keys to sign documents and verify their authenticity. He can then upload a document and sign it using his private key.

3.3 Use case diagram

The main use case diagram of our system is represents in the Figure 3.2 The visitor is the user who can access to the registration and login interfaces, but he can only scan the digital signature and verify its validity. The signer is the visitor who did the registration and the login process and his main role is to sign documents.

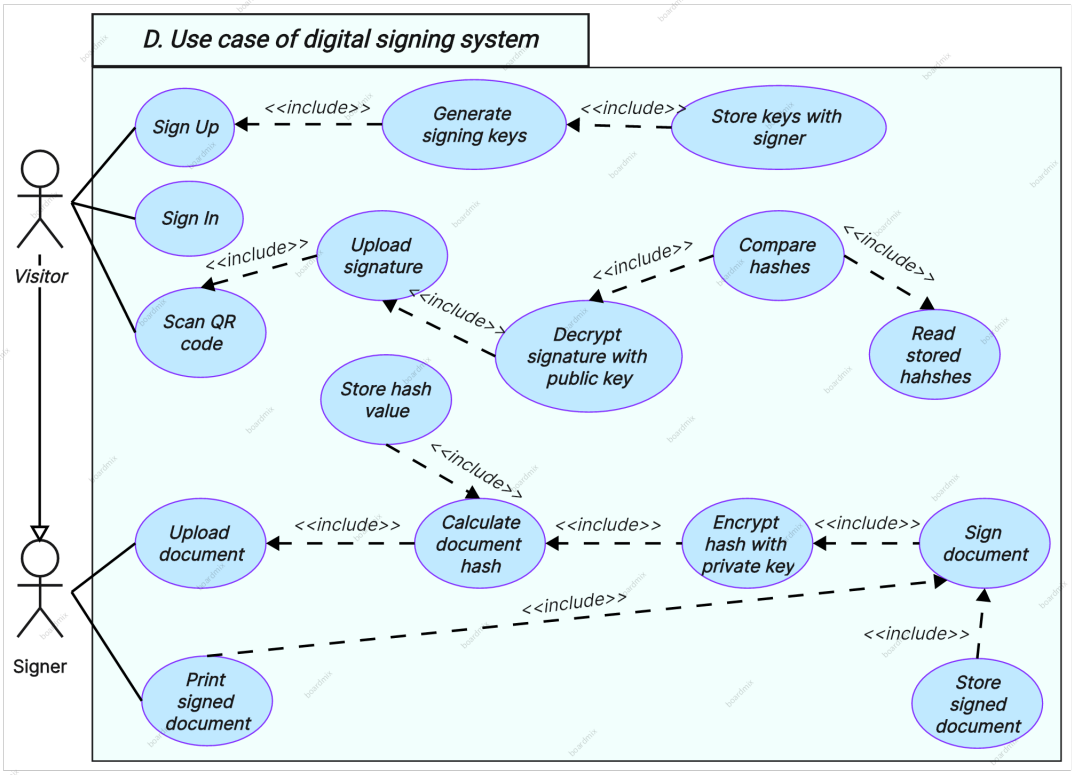


Figure 3.2: Main use case diagram

3.4 Sequence diagrams

3.4.1 Sign up sequence diagram

The sign up sequence diagram is depicted in Figure 3.3. When the visitor receives the registration form and enters his information. His information will be verified, especially that the email account has not been used before. Otherwise the account will not be created.
By default, the account status will be inactive, unless the user is an employee of the organization that uses our system. So the admin could activate his account.

3.4.2 Sign in sequence diagram

The sign in sequence diagram is depicted in Figure 3.4. After the user sign in we check if his account is active, if so, he will be able to access his personal account page and then sign the documents.

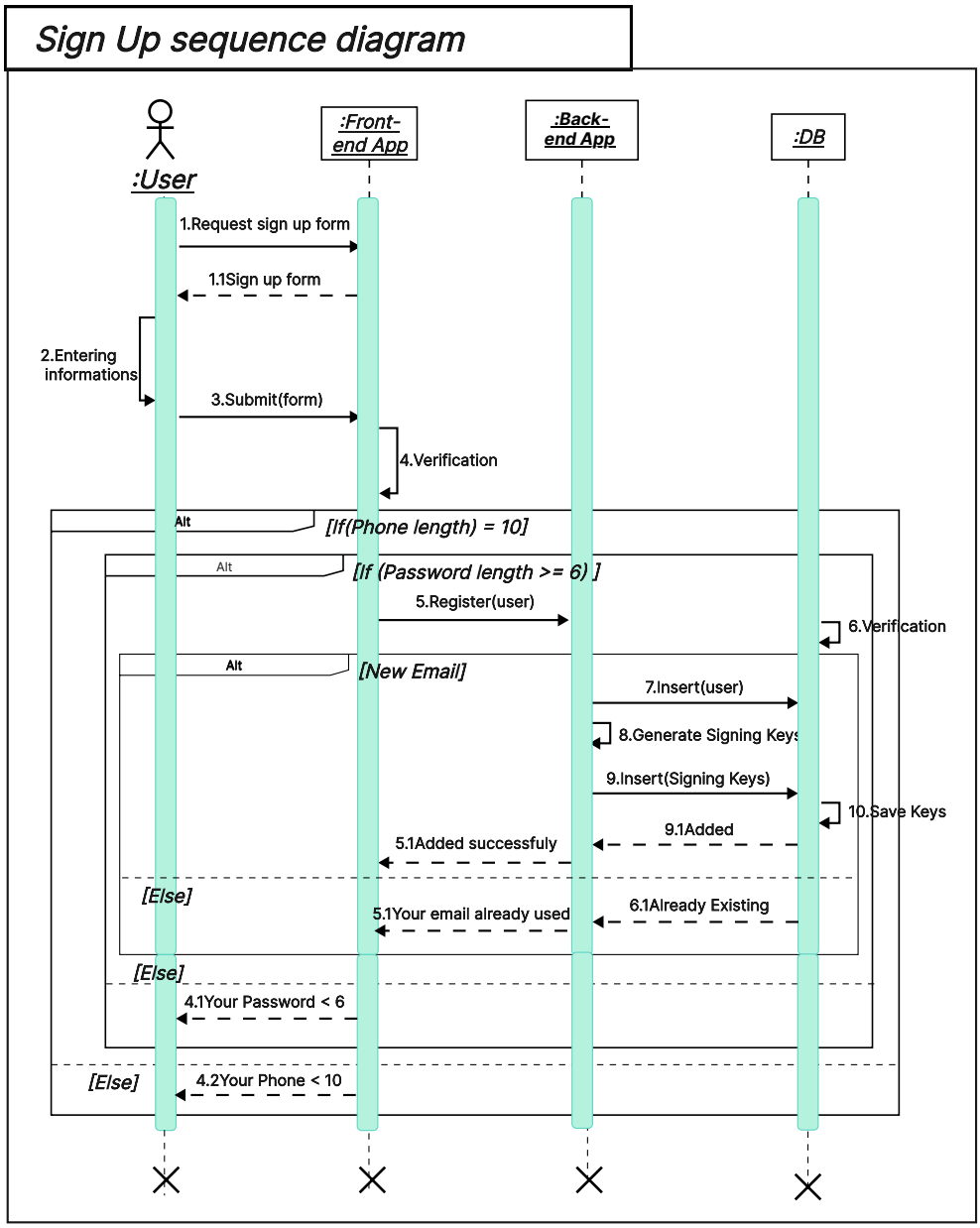


Figure 3.3: Sign up sequence diagram

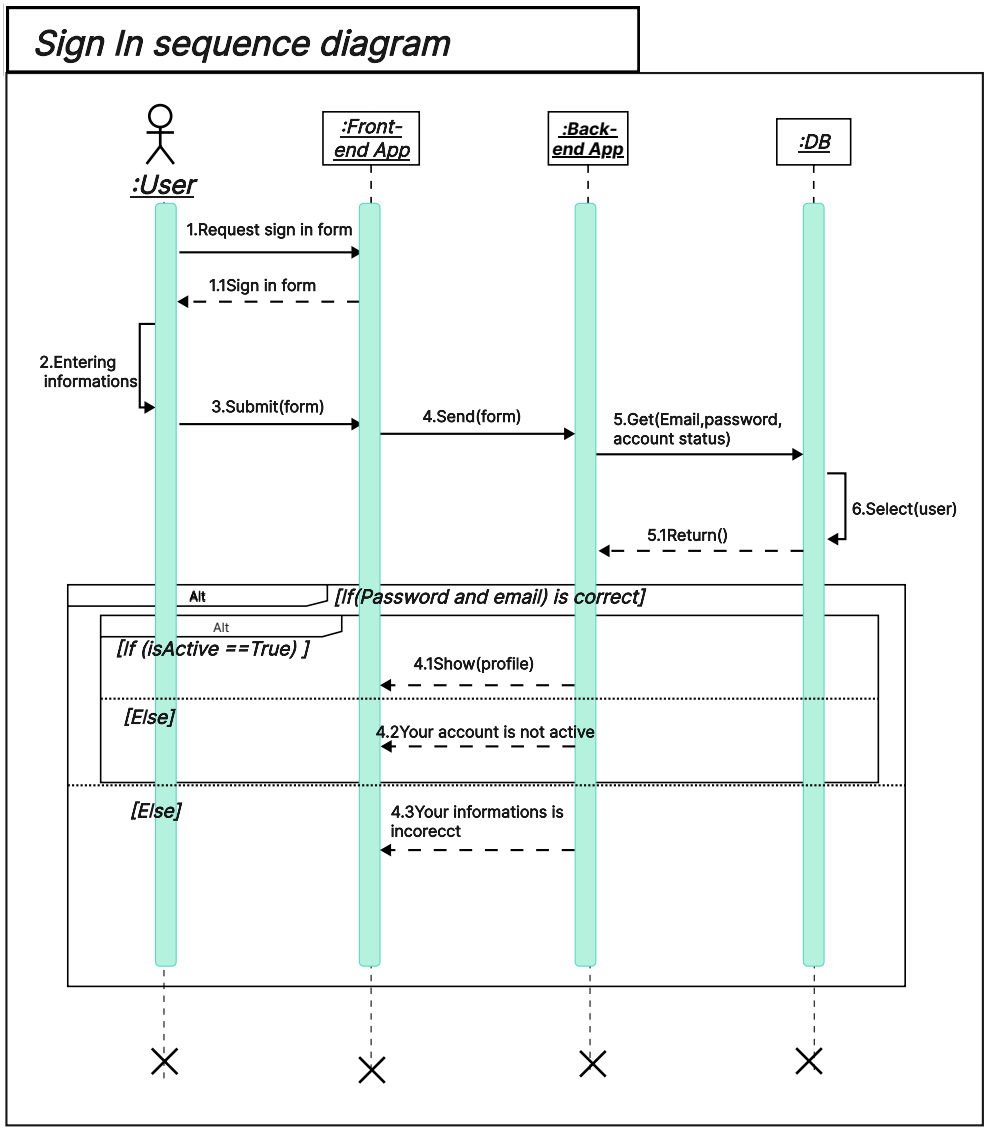


Figure 3.4: Sign in sequence diagram

3.4.3 Sign document sequence diagram

The sequence diagram in Figure 3.5 depicts the process of signing a document. Once the user has successfully completed the login process using an active account, they are able to upload the document to the system and proceed with the signing process illustrated in the figure.

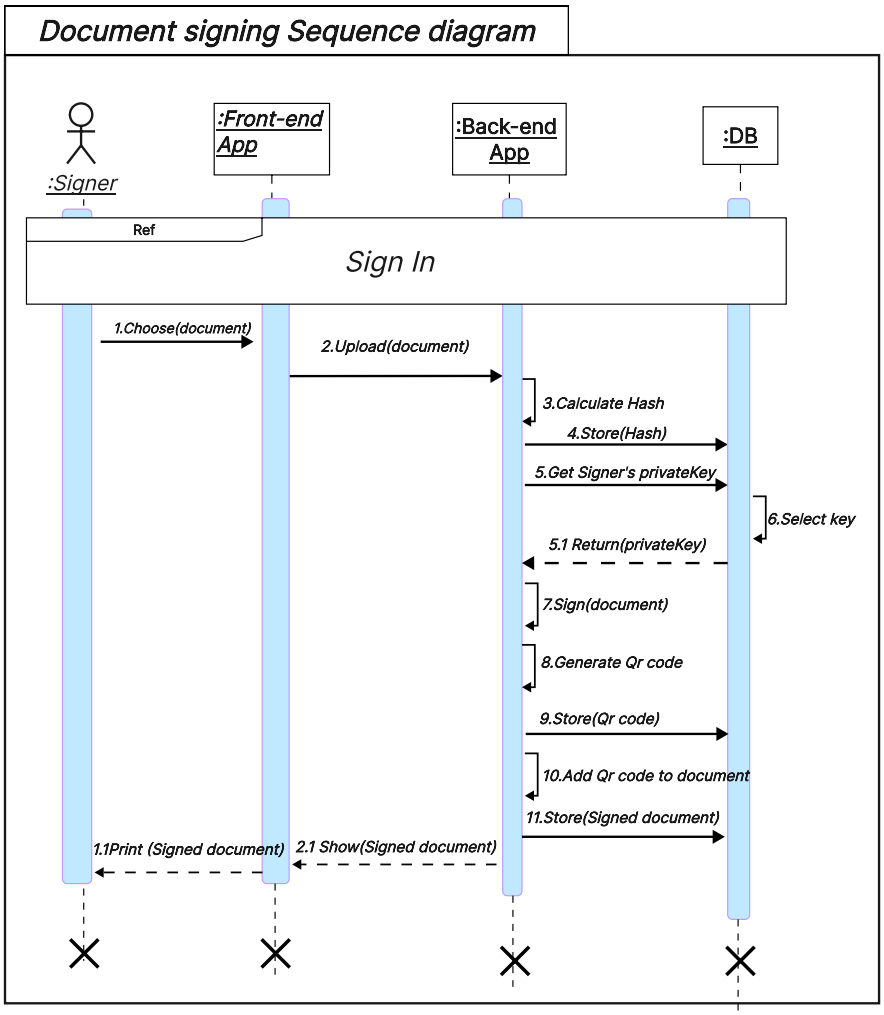


Figure 3.5: Sign document sequence diagram

3.4.4 Verify signature sequence diagram

The Figure 3.6 illustrates the sequence diagram for signature verification. If the scanned QR code is for a fake document, a warning will appear to the user that the document is fake. Otherwise the same document will be shown to him to compare its content with the document at hands.

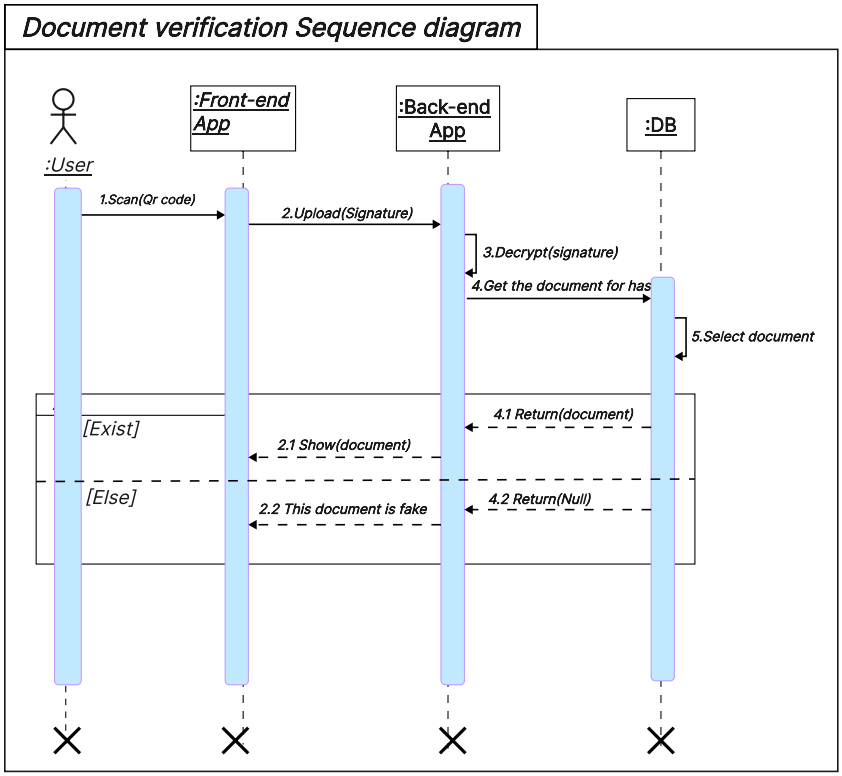


Figure 3.6: Verify signature sequence diagram

3.5 Conclusion

In this chapter, we presented three UML diagrams. Firstly, a main class diagram was presented, followed by a comprehensive main use case diagram that summarized all the system's use cases. Additionally, we constructed the most important sequence diagrams to capture the key interactions and processes within the system.

Chapter 4

Implementation and Presentation of our System

4.1 Introduction

In this chapter, we will present the tools used in developing this project and the developed system, which is the result of the work mentioned in the previous chapters. We will explain it in detail through its interfaces.

4.2 Development tools

Our system is a web application. The back-end was developed using the Python language in a Visual Studio Code development environment. The front-end was developed using HTML, JavaScript and CSS based on Bootstrap and local CSS. In addition to Flask framework that connects the back-end and the front-end. For the database we have used MySQL database management system.

4.3 Presentation of our system

This system is approved for the main purpose of digitally signing papers in addition to detecting forged documents.

Below we present a set of its functions:
The home interface of the system Figure 4.1 allows the user to navigate between the login interface, the registration interface, and an interface to verify the scanned QR code, in addition to an interface that carries information about the system.

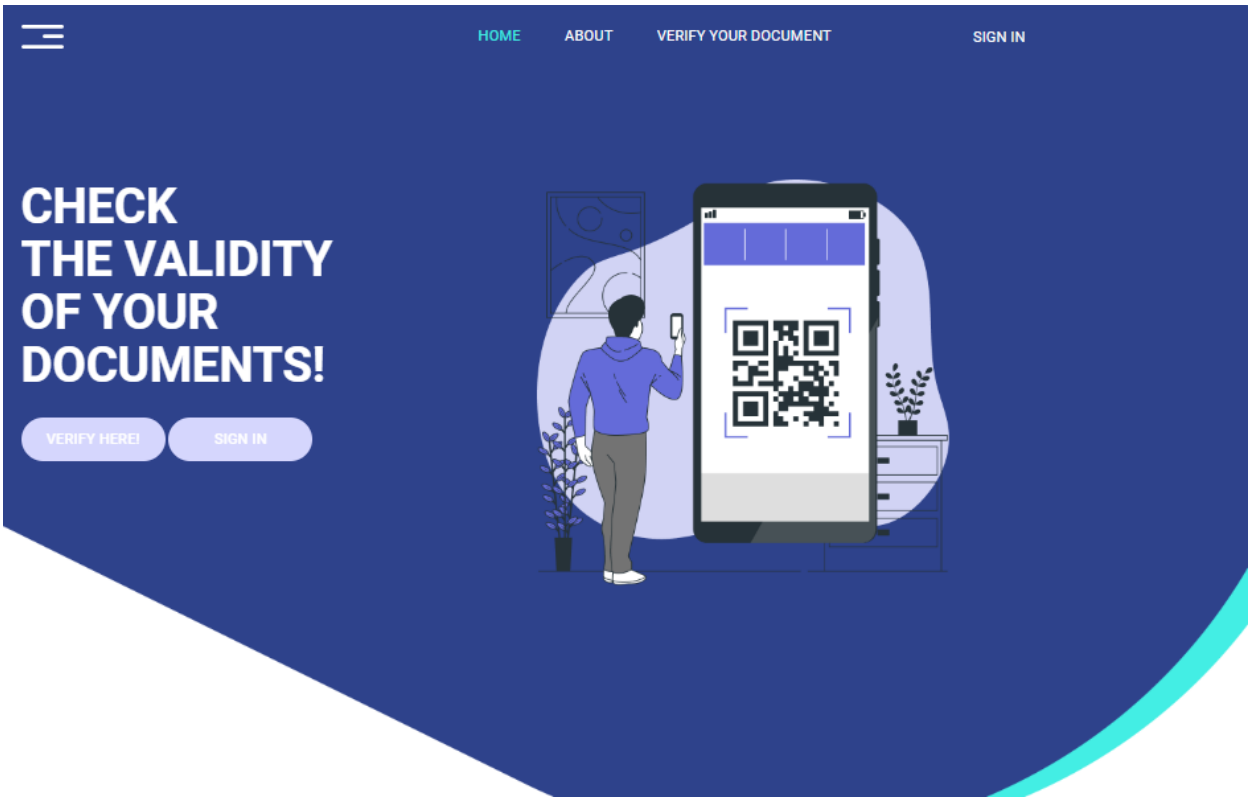


Figure 4.1: Home page

If the user is an employee of an organization that uses our system, he will be able to register Figure 4.2 and login Figure 4.3 through the following interfaces:

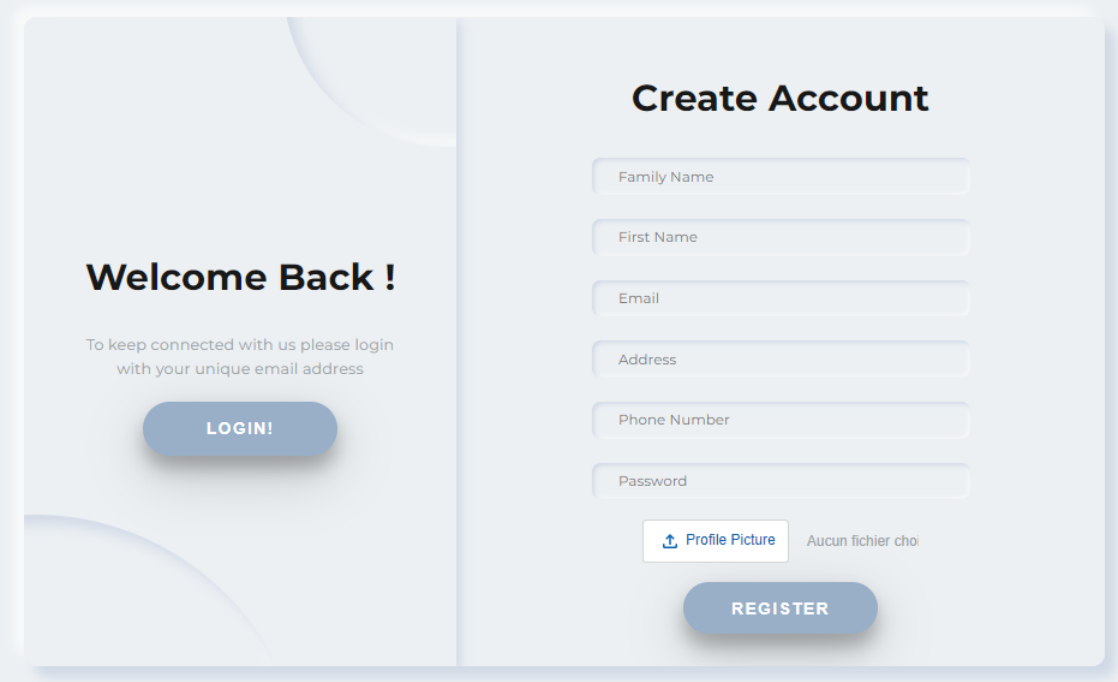


Figure 4.2: Registration page

The visitor can register for an account in our system, but he is unable to use the main interface for signing documents.
The user will have access to the system if his account is active. If not, he will receive warning message that his account is inactive.

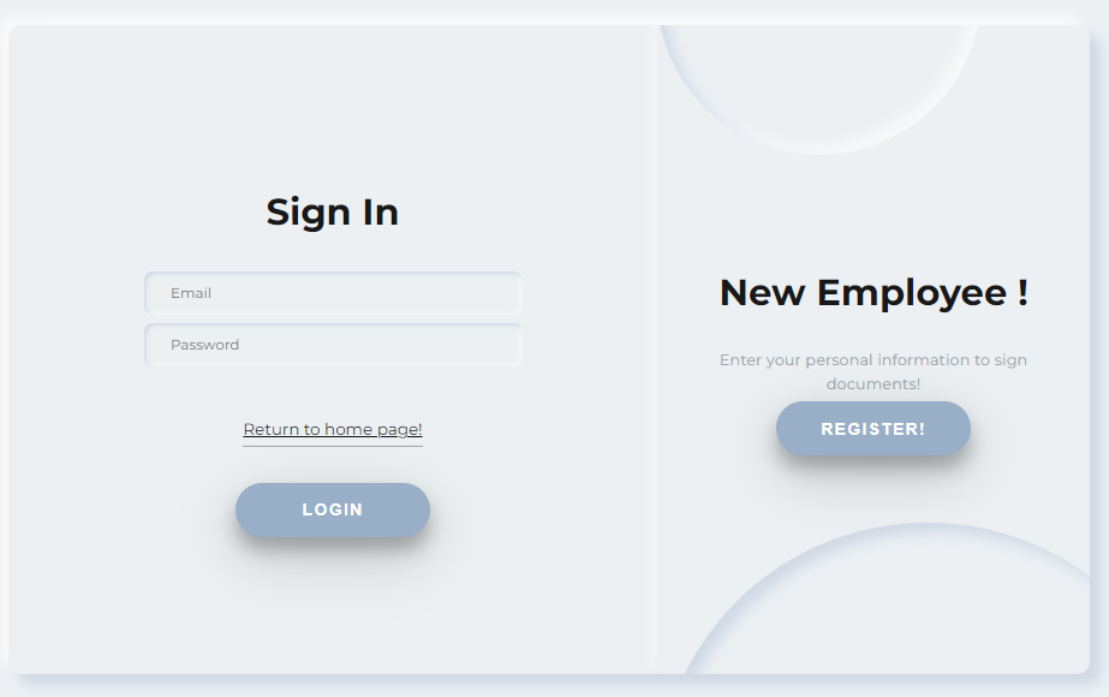


Figure 4.3: Sign in page

After verifying that the employee has an account with his unique email and his account is active. He could then access his profile page Figure 4.4.

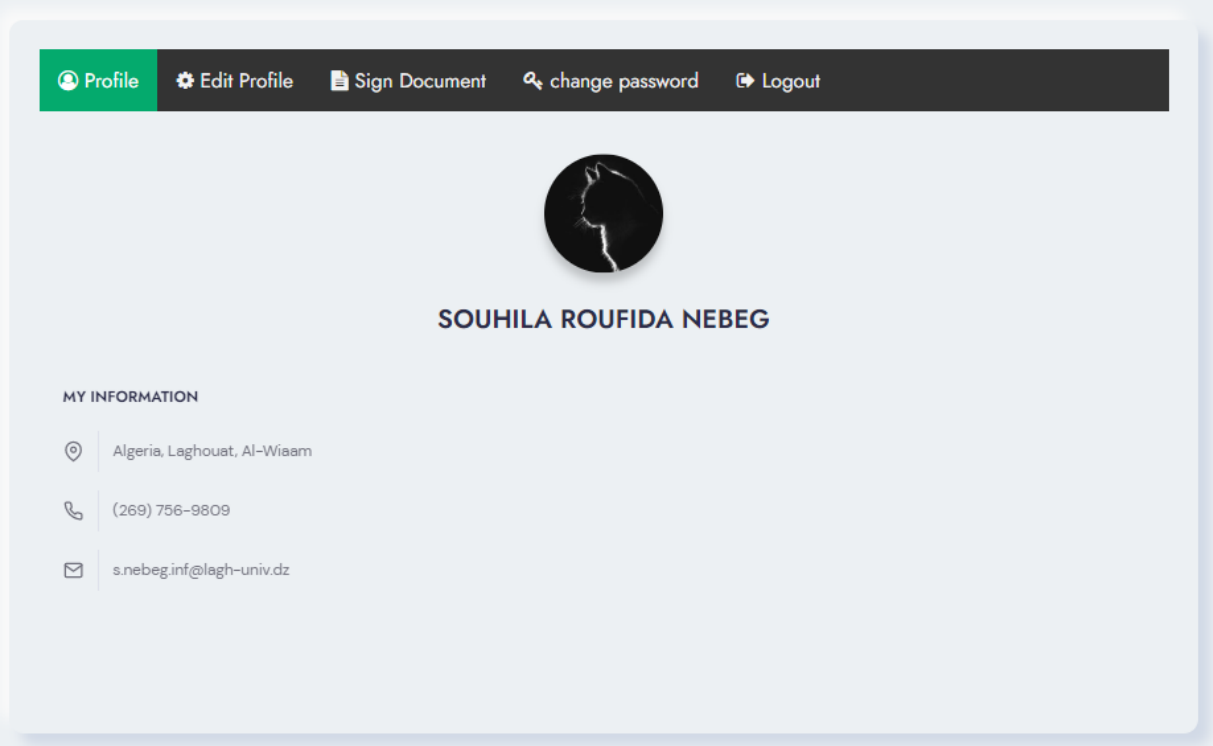


Figure 4.4: Profile page

Through the information change interface, he can modify his information Figure 4.5.

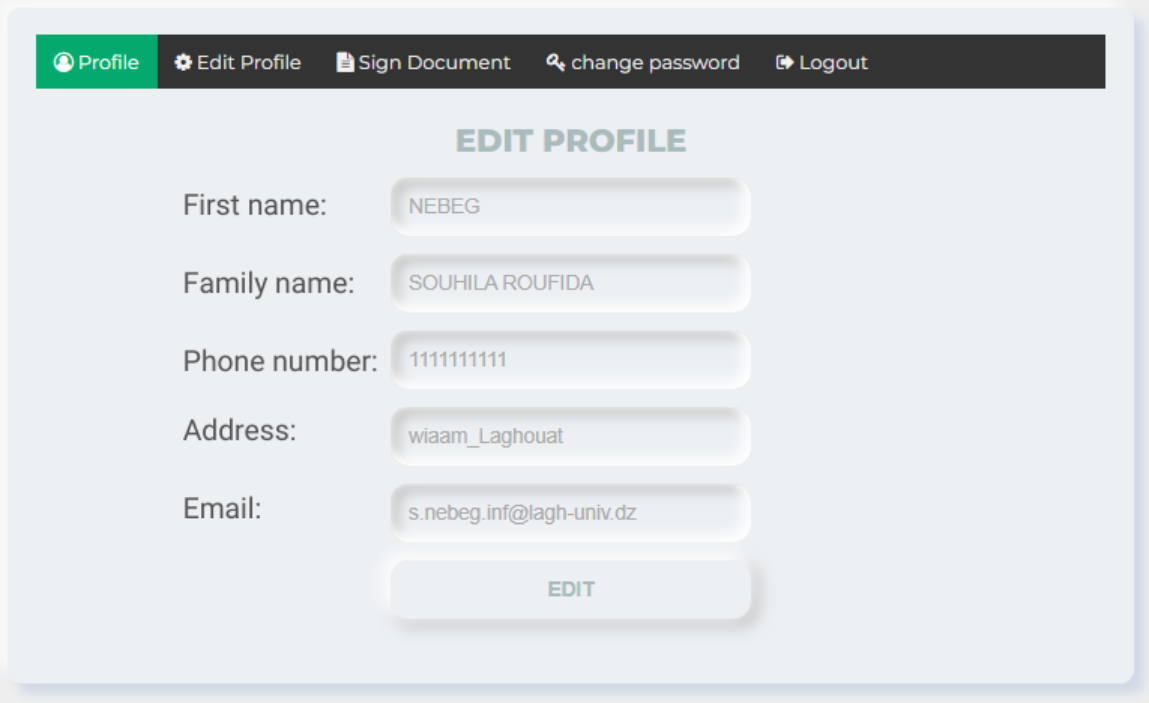


Figure 4.5: Edit information page

To give the signer the possibility to change his password we created this interface Figure 4.6.

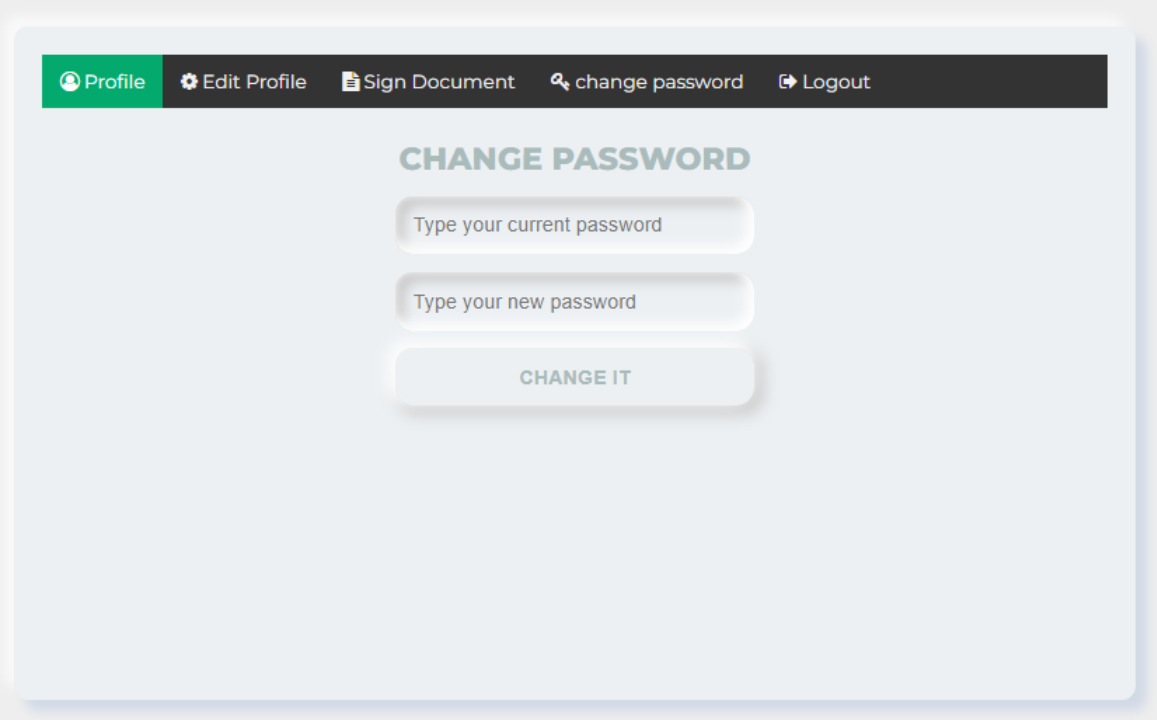


Figure 4.6: Edit password page

When an employee needs to sign a document, he uploads the document and then signs it using the private key Figure 4.7 that was generated when the account is created, which is stored in the database. Then the signed document is shown to him so that he can download or print it.

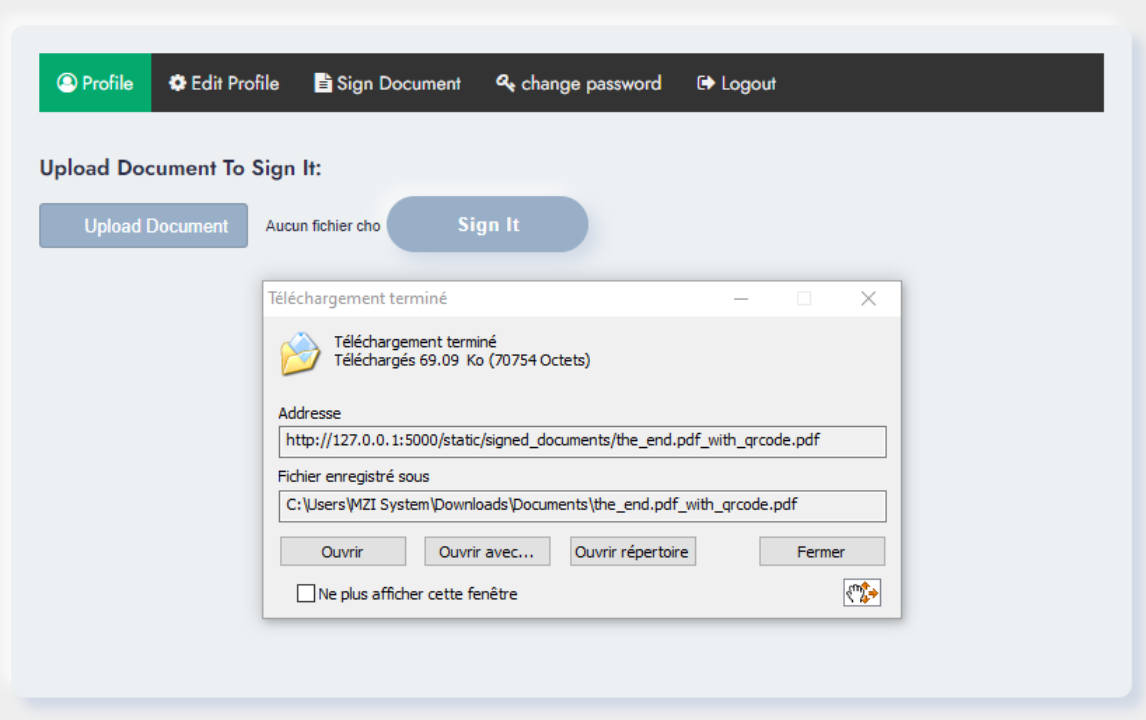


Figure 4.7: Sign document page

As for the visitor, he will be able to scan the QR code in a document signed by an institution that uses our system to be able to verify the digital signature. If it is authentic, it will show him the same document to compare it with the document he owns. If it is fake, he will know that it is fake Figure 4.8.

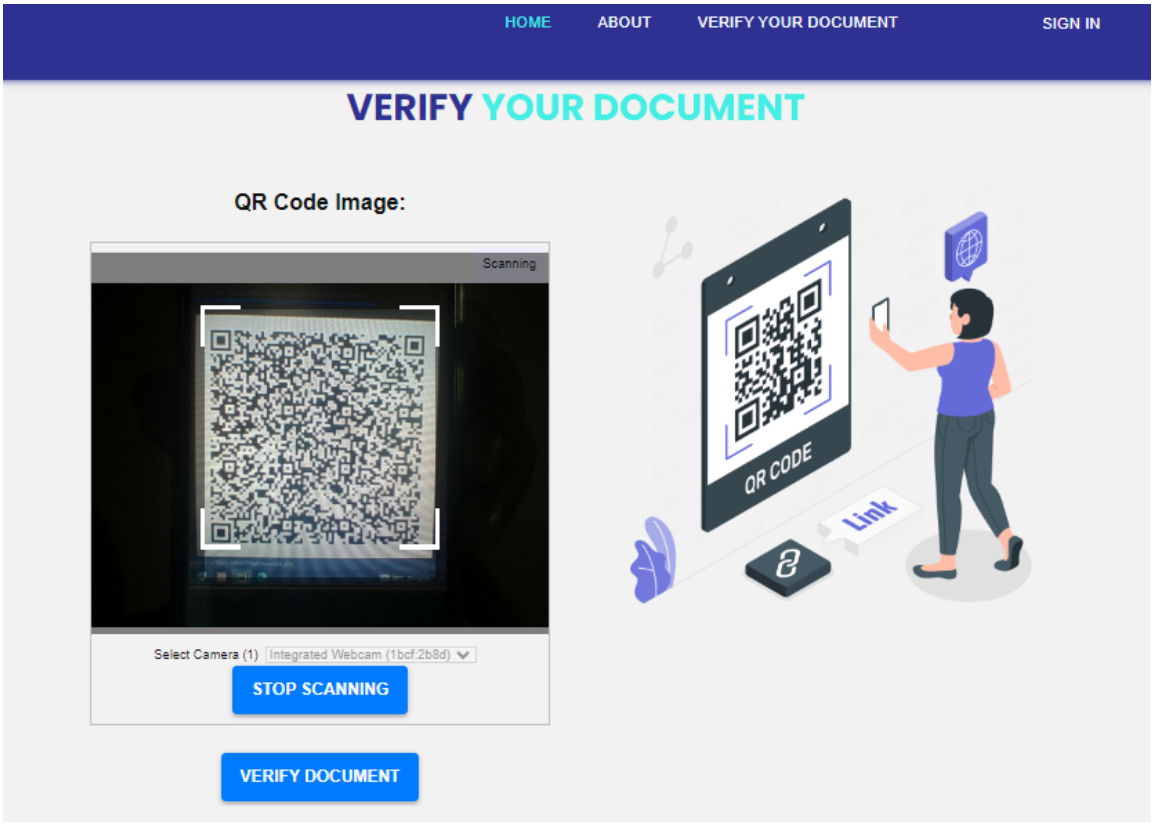


Figure 4.8: Verification page

In addition, he will be able to browse the interface that shows our system information Figure 4.9.

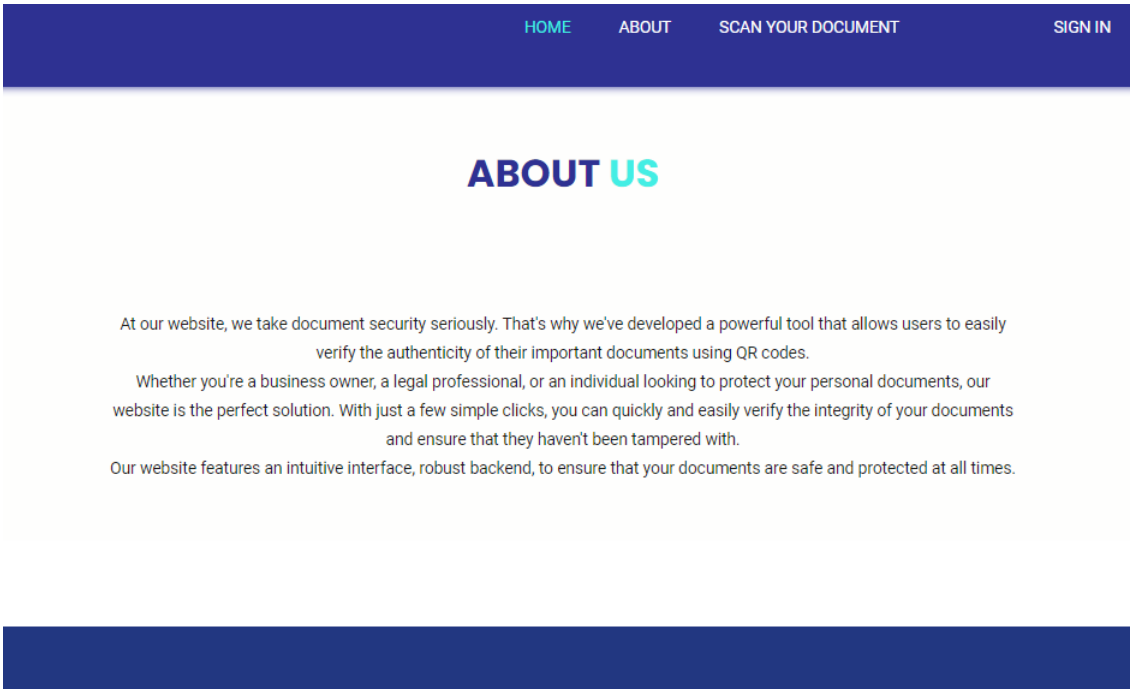


Figure 4.9: About us page

4.4 Conclusion

In this chapter we have presented the practical aspects related to the realization of our system. Showing the main pages, and naming the development tools necessary for the operation of our system.

Chapter 5

General conclusion

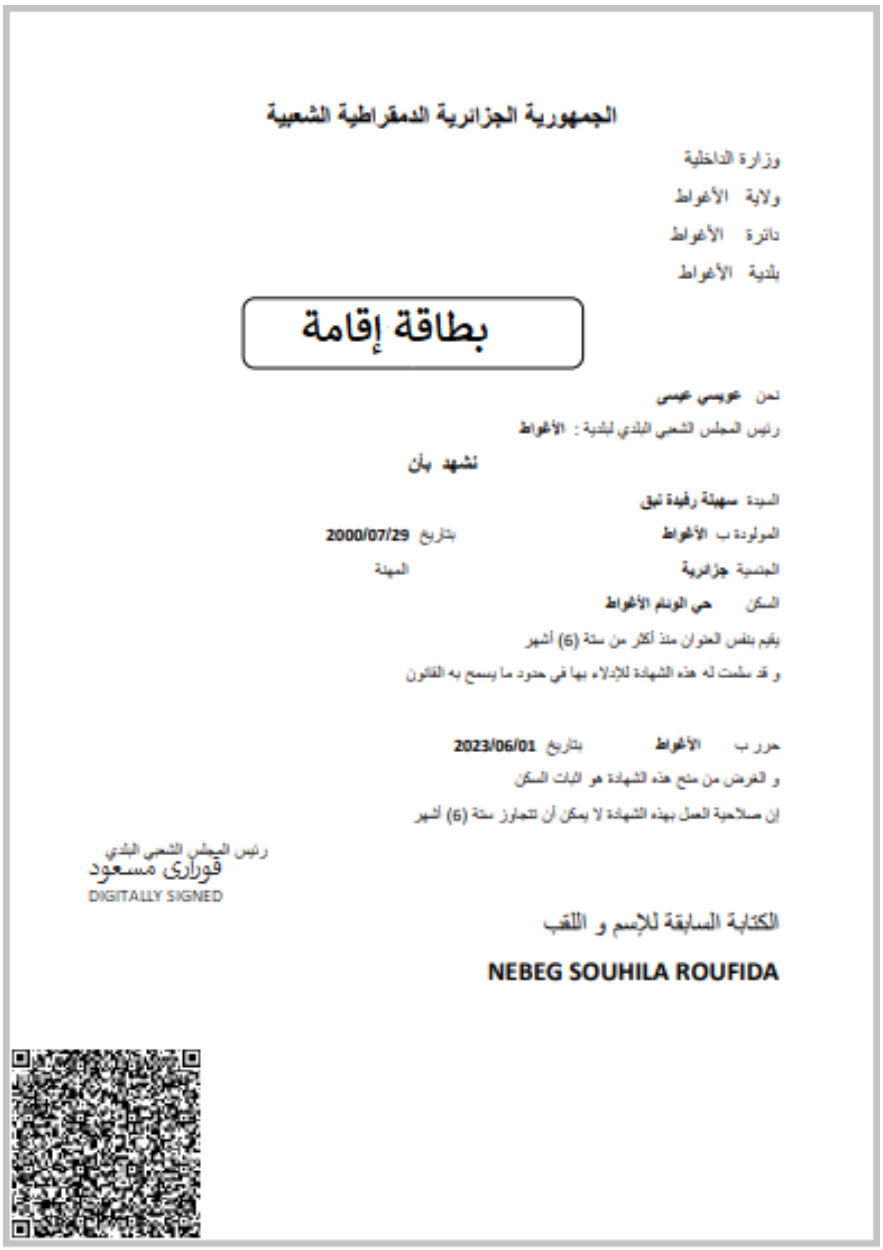
In conclusion, this graduation report aimed to address the crucial issue of document security in the digital era and provide organizations with a trustworthy and user-friendly tool for signing and verifying important documents. Throughout the implementation of this project, we acquired valuable knowledge and skills in Python and Flask, which were essential in developing the web application. The project served as a valuable learning experience for us, as it marked our first practical application of Python. We gained a comprehensive understanding of Python's capabilities and learned to utilize Flask, a powerful web framework, to develop a robust and efficient web application.
For recognizing the iterative nature of any project, it is important to acknowledge that our digital signature system, despite its functionality, has room for improvement. Like any handmade creation, it carries the potential for refinement and enhancement as we strive for perfection. Therefore, we have decided to implement additional features and improvements in the future.

- One of our planned enhancements is to incorporate a comprehensive document content scanning, rather than solely relying on QR codes. This will ensure that the signature is not used on counterfeit documents.
- Additionally, we aim to implement a policy of not retaining visitor (who has inactive account) information in the database for extended periods. Instead, this information will be automatically deleted after a certain period of time.

- We will attempt to find a way to automatically activate employees' accounts without relying on the admin to activate their accounts, eliminating the need for waiting.
- Furthermore, we will be add other signing algorithms and hashing functions to provide the system with a greater degree of choice and versatility. These additions will allow signers to tailor the signature process to their specific needs.

By implementing these enhancements and additions, we aim to continually improve our digital signature system and provide users with an even more secure and customized experience.

Annex



الجمهورية الجزائرية الدمقراطية الشعبية

وزارة الداخلية

ولاية الأغواط

دائرة الأغواط

بلدية الأغواط

بطاقة إقامة

نحن **عويسي عيسى**

رئيس المجلس الشعبي البلدي لبلدية : **الأغواط**

نشهد بأن

السيدة **سهيلة رفيدة نبق**

المولودة ب **الأغواط** بتاريخ **2000/07/29**

الجنسية **جزائرية** المهنة

السكن **حي الوئام الأغواط**

يقيم بنفس العنوان منذ أكثر من ستة (6) أشهر

و قد سلمت له هذه الشهادة للإدلاء بها في حدود ما يسمح به القانون

حرر ب **الأغواط** بتاريخ **2023/06/01**

و الغرض من منح هذه الشهادة هو اثبات السكن

إن صلاحية العمل بهذه الشهادة لا يمكن أن تتجاوز ستة (6) أشهر

رئيس المجلس الشعبي البلدي
قوراري مسعود
DIGITALLY SIGNED

الكنية السابقة للإسم و اللقب

NEBEG SOUHILA ROUFIDA

Figure 5.1: Exemple of signed document by our system

Bibliography

[1] N. Garg and P. Yadav, "Comparison of asymmetric algorithms in cryptography," *J. Comput. Sci. Mob. Comput.(IJCSMC)*, vol. 3, pp. 1190–1196, 2014.

[2] D. P. Joseph, M. Krishna, and K. Arun, "Cognitive analytics and comparison of symmetric and asymmetric cryptography algorithms," *Int. J. Adv. Res. Comput. Sci*, vol. 6, no. 3, pp. 51–56, 2015.

[3] E. Milanov, "The rsa algorithm," *RSA laboratories*, pp. 1–11, 2009.

[4] S. Bakhtiari, R. Safavi-Naini, J. Pieprzyk, *et al.*, "Cryptographic hash functions: A survey," tech. rep., Citeseer, 1995.

[5] T. H. Tran, H. L. Pham, and Y. Nakashima, "A high-performance multimem sha-256 accelerator for society 5.0," *IEEE Access*, vol. 9, pp. 39182–39192, 2021.

[6] S. Subramanya and B. Yi, "Digital signatures," *Potentials, IEEE*, vol. 25, pp. 5 – 8, 04 2006.

[7] C.-y. Law and S. So, "Qr codes in education," *Journal of Educational Technology Development and Exchange (JETDE)*, vol. 3, no. 1, p. 7, 2010.