UNIVERSITY of RWANDA

Research and Postgraduate Studies (RPGS) Unit

Research thesis title:

"Analysis on Digital Signature, based on Digital Certificate"

By: Jean René MUNYESHYAKA

Reference Number:

219014181

Supervisor: Dr. Frederic NZANYWAYINGOMA, PhD

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Science, in the department of computer science, option of software engineering

In the College of Science and Technology

NYARUGENGE CAMPUS, KIGALI / RWANDA

2024

Dedication

To

The Almighty God

My Family

All my relatives

All my friends and colleagues

I dedicate this work.

Declaration

I, Jean René MUNYESHYAKA, declare that this research thesis titled "Analysis on Digital Signature Based on Digital Certificate" was my own work and that it was not submitted to any organization or academic or otherwise. This work was done in candidacy for a Master of Science degree at the University of Rwanda, College of Science and Technology, School of ICT, Department of Computer Science, Option of Software Engineering. All the sources of information, data and material that were cited in this research work (including the Internet) have been fully identified and properly acknowledged as required.

Signature : …… …… **Date : 16th / August / 2024**

Jean René MUNYESHYAKA **Kigali**

Certification

The undersigned certify that I have read and hereby recommend for acceptance by the University of Rwanda, College of Science and Technology (UR/CST); a dissertation: "**Analysis on Digital Signature, based on Digital Certificate**" submitted in partial fulfilment of the requirements for the degree of Master of Science in software engineering, at the University of Rwanda, College of Science and Technology, School of ICT, department of Computer Science, option of Software Engineering.

Signature: …….

Date: 16th /August/2024

Jean René MUNYESHYAKA

Signature: …… **Signature:** ……

Date: 16th /August/2024 **Date:** 16th / August/2024

Dr. Frederic NZANYWAYINGOMA, PhD **Mr. Theoneste MURANGIRA**

Supervisor **Head of Computer Science Department**

Acknowledgements

First of all, this dissertation is dedicated to the Almighty God our Father and my entire family.

Secondary, it's my pleasure and honour to take this opportunity to thank first and foremost the University of Rwanda for the immense support towards the completion of my thesis, without their support I would never have finished this journey.

I am greatly indebted and thankful to the Doctor Frederic NZANYWAYINGOMA and Doctor Omar SINAYOBYE for their extra guidance, support and help in both my academic and social life. Thanks also go to my classmates whom we studied together, had sleepless nights for their continued encouragement and advise in one way or the other.

Finally, I am deeply touched and humbled by the love, care, resilience and patience given to me by my entire family. They were instrumental in proving me with necessary support and psychological comfort, right from the start to the end of my final thesis.

Abstract

Motivated by the importance of Software Development and Ethics to fight against forgery and tampering in our society, this research study the use of Digital Signature based on Digital Certificate to provide digitally signed documents among users.

This thesis pays special attention to the current problem by evaluating the change in performance once Digital Signature based on Digital Certificate is used to strengthen the existing signing schemes for long-term improvement and security. Specifically, the thesis explores application of Digital Signature based on Digital Certificate: predicting signing system performance.

Basically, the Reed Solomon method is an algorithm that was used to implement the QR code, incorporating associated digital signature and important user information. The Reed Solomon Correction Method allows QR codes to be scanned even if a certain amount of the QR code is covered up or blocked. This algorithm permits above necessary verifications; and eventually Digital Signature based on Digital Certificate, is a framework that permits users to make wrongfully binding electronic documents that are reliable and predictable.

The thesis identifies potential challenges, current limitations, and suggestions for further improvement. Rigorous analysis using JMeter will lay solid foundation for further study within the domain.

This research provides a way of verifying the reliability and validity of digitally signed documents to build trust among users. The results analysis tested, verified and validated the work as sufficient evidence that the assignable, verifiable, portable, linkable, and verifiable digital signature schemes are reliable, predictable, and of minimal repudiation. The results predicted are in the range between 65 and 98 out of 100, with an accuracy of 97%. From the results also we detected the need of increasing the dataset size, especially increasing quantitative dependent variables for prediction.

Throughout this research we also noticed that Digital signature based on Digital Certificate cannot be accomplish without scanning system for verification method as a consequence to build trust among users.

Keywords: Digital signature, Digital Certificate, Reed Solomon, QR codes, signing system.

Acronyms and Abbreviations

1	CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
2	CRL	Certificate Revocation List
3	DevOps	a portmanteau of “development” and “operation"
4	DRA	DevOps Reference Architecture
5	DSbDC	Digital Signature based on Digital Certificate
6	ETSI	European Telecommunications Standards Institute
7	FRBR	Functional Requirements for Bibliographic Records
8	FRIR	Functional requirements for information resource
9	HSV	Hue, Saturation, Value
10	HTML5	Hypertext Markup Language
11	HTTP	Hypertext Transfer Protocol
12	IEC	International Electrotechnical Commission
13	ISO	International Organization for Standardization
14	iTANplus	Indexed TAN (iTAN) and iTAN with CAPTCHA
15	JCE	Java Cryptography Extension
16	JDK	Java Development Kit
17	JRE	Java Runtime Environment
18	MAC	Message Authentication Code
19	OWL	Web Ontology Language
20	PKI	Public Key Infrastructure
21	PubSubHubbub	open, simple, web-scale, Publish/subscribe communication over internet
22	QR	Quick-Response code
23	RDF	Resource Description Framework
24	RSA	Rivest–Shamir–Adleman
25	SDLC	Software Development Life Cycle
26	SMS	Short Message Service
27	sparqlPuSH	Proactive notification of data updates in RDF
28	TAN	Transaction Authentication Number
29	URI	Uniform Resource Identifier

List of Figures

List of Tables

Table of Contents

Chapter 1 INTRODUCTION

1.1. Preamble

Nowadays, additional and more folks and organizations are using digital documents rather than paper documents to conduct regular transactions. Digital Signature based on Digital Certificate is a web-based digital signature scheme that uses coded signature and certificates to express digitally signed documents, to strengthen existing digital signature schemes, and build a reliable mechanism that minimizes the risk of rejection while fighting against forgery [1].

The "Analysis on Digital Signature, based on Digital Certificate" is system that has different users' accounts using multi factor authentications and different level of privilege. A system that provides QR code to sign documents and barcode to identify unicity of issued documents, to secure authenticate exchanged documents among users [2].

Regularly updated Digital signatures and timestamp are used to detect unauthorized changes to data and to authenticate the identity of the signer. The Quick Response (QR) code was developed for quick readability and information storage. This research proposed a method where the QR code contains a digital signature with the applicant's details such as the national identity number or name of the holder, date of birth, position, work facility, personal identification, which is signed by the facility to use this system, all interested institutions must register in the central system. To verify the digital signature signed with a QR code, a QR scanner application on any smartphone scans and authenticates the certificate without having to go to the institution that issued the certificate and gain access to important user information [3].

To apply for a request a user must fulfil a form. The form is sent to the first agent signer (probably a direct supervisor) for further verifications and decision (approval/rejection). A request can be rejected if it doesn't fulfil required criteria. But if it does, it is signed and sent to the next signer. The process of verification restart and when a decision is ready, the document is signed or rejected and sent back to the previous level with necessary comments or sent to the last destination.

The system provides two different signing levels and privileges, where different users fulfilling needed adjustments and signs. Not all users have the same privileges. Those who will have to

edit/sign have the privileges of read and write. Those who share the role of verification only (viewers), will have the right to read information only. Thus, an acknowledge notification message is sent to concerned user by mail/SMS in real-time.

The system confirms that the person signing is trustworthy and that the digital signature is still valid. As an evidence, the proof of (i) ownership, (ii) verification, (iii) sympathy, (iv) reversibility or revocation, (v) performance and (vi) computing power in reliable digital signature schemes; is provided in this work [4]. The work will also provide evolutionary conditions for safety and reliability systems and show that Digital Signature based on Digital Certificate meets these criteria.

1.2.Background and Motivation

The purpose of this research is the promotion of the use of software being able to improve operation of management of Digitally Signed Document in the interest of all stakeholders. The research guaranties the easiest way of online user management, request, approval, automated digital signature system and document transfer through certificates verification in total satisfaction of all stakeholders, trough user friendly interface; that helps to run all steps, from the start to the end, in laps of time.

This research will focus on the online digital signature based on the digital certificate system. The current process of generating digital signatures is not simplified enough for users with little computer literacy, the exchange of paper documents has not been cancelled and there are numerous problems due to this method both for signers and applicants. A design will be taken to computerize the manual process to solve this problem. Problems will be identified after a series of interviews and document reviews, followed by an analysis and fully computerized process is recommended. This research will also suggest how to successfully implement the computational process and overcome the hurdle that would hinder the successful implementation of the system.

The online Digitally Signed Document system is one step in automation, and has become a routine part of human life because it offers major advantages comparatively to the tradition paper document archive and exchange system. This will contribute to build the sovereignty of our systems and data notional wide, to secure and guarantee every operation done by an online signing system which improves the traditional process to deliver online digitally signed document. It will

help to secure and to guarantee every operation done by an online signing system which improves the traditional process to deliver online digitally signed document [5].

1.3.Problem Statement

With the coming of an increasing number of complicated and linked software program systems, the safety enterprise keeps to stand growing demanding situations which have an effect on the physical, facts and Cybersecurity domain to save you, locate forgery or tampering [6]. Current means to digitally sign document, didn't nullify the use of paper documents and time to hand it to an institutional service requesting it. Acceptable levels of risk are changing constantly, media coverage is attracted to security deficiencies, loss of time is a critical issue, and security threats have gained the political attention. Trust is important issue in E-service and Business in general. The importance to ensure the four major safety elements can play an important role [7]. And the costs of security measures, under continuous pressure, is so high today. Awareness of the users and stolen certificates authority's private keys. The management of digital certificates within an organization is also a great challenge.

It is in this context we suggest "Analysis on Digital Signature, based on Digital Certificate" research as a trustful mechanism to exchange official documents and information through internet, to ensure availability, integrity, authenticity, confidentiality, non-repudiation, and utility. This will build trust among beneficiaries and in increasing the efficiency in the functioning of systems.

1.4.Study Objectives

Official Document Signing System Method must be driven smartly and economically. The use of digital signature based on digital certificate respond to this need, and Application Programmable Interfaces with customer institutions are used. This is the fundamental motive force for this research.

1.4.1. General Objective

The general objective of this research thesis is to design an online signing system which could improve the existing signing methods to positively impact the process and responses to the users to access services related to digitally signed documents in any public or/and private institution.

1.4.2. Specific Objectives

i. Analyse the existing workflow, identifying the gap for improving the documents' signing methods.
ii. Study the required systems features and inter-connection to facilitate flexible deliverance and facilitate management.
iii. Implement a user centred design for the signing system with elucidated requirements putting an accent on user interaction with the system.
iv. With the implement means for verification for the signing system, verify and validate that changes are aligned with the new work process for the designed signing system.

1.5. Research Questions:

This research shall contribute to respond to the following research questions:

i. Do the proposed solutions measure up to the identify gap and problematic?
ii. Do defined functional and non-functional requirements matching the users' needs?
iii. Can the provided prototype of digital signature be attributed, verifiable, linkable, reversible, revocable, potable and computable?
iv. Is the system load, performance and security up to the normal?

1.6. Hypothesis

"It is possible to identify gaps, encountered challenges be addressed and come up with realistic solutions for the user' s satisfaction.

Clear feedback directly collected from the users help to understand the user needs. There are great chance to elaborate features, functionalities and non-functional requirements for stakeholders' satisfaction.

The feasibility to design a new signing model with attributable, verifiable, reversible, revocable, portable and computable features; is high.

The robustness, system portability and strength ensure more flexibility, load and system performance. There is positive correlation between performance, load time and user satisfaction. It is a fact that taster load times lead to better user experiences."

1.7.Study Scope

1.7.1. Content Scope

Taking a Digital Signature based on Digital Certificate system is restricted only to the:

1. User accounts (signup/signing): To build a system through which the user can apply for the registration, the user is able to apply for member ship.
   - ✓ Applicants (user role)
   - ✓ Signers (signatory role)
   - ✓ Administrator (Admin role)
2. Documents catalogue
3. Apply for a document
4. Generate a Signature
5. Verify a Signature
6. Generate a PKI (Private and Public)
7. Digital Sign/Approval
8. Notifications
9. Final Approval
10. List of issued authorisations
11. Barcode used to provide unicity of issued documents with serial numbers

1.7.2. Signing scheme Scope

Actually, a Digital Signature based on Digital Certificate system may run different digital documents but this digital system is specific on Web Sign scheme applied to Mission Travel Clearance as an example, generated in pdf file format as the final output. In order to limit the scope of this research, we focus our efforts on Mission Travel Clearance generation system using digital signature schemes that can potentially be trustable, computable, and minimally repudiation. But we recognise that other type of official documents can be digitalized in future works.

1.7.3. Scope of Time

The Mission Travel Clearance Generation System for DSbDC project has started at the beginning of December 2023 with the feasibility and will end in May 2024 with the Verification and Validation activities.

The main challenge was to find collaborators and books related to this research. Most found paper were very expensive, relevant ones are locked from UR online library, and very few similar subjects were founded during the research study. The DSbDC should be linked to different institutional systems to verify the signing process automatically. But locally such systems are very closed and can't be directly tested together before being approved.

1.8. Significance of the Study

The findings are intended to assist the different institutions and organisations to build a trustful mechanism for digitally signed documents especially Mission Travel Clearance, among all stakeholders. The study also provides literature that forms a foundation for further research for scholars in various academic institutions and this work also contributes to Software Engineering literature.

1.9. Research Organization

This work is articulated around five chapters:

Chapter 1 related to the general description of the work:

Background of the study which overlaps the research project definition, the Motivation, Problem description, the objectives of the study, Hypotheses, Study Scope, Significance of the Study, Organization of the Study, and Conclusion.

Chapter 2 literature review: it discussed the existing theories, and contains the definition of key terms and concepts.

Chapter 3 research methodology: it explains the techniques, and procedures used in collection and processing of data.

Chapter 4 System Analysis and Design: it explains the system models, proposed simulation models, simulation parameters, simulation scenarios. It gives details about how the system is built, its processes and how does the system work.

Chapter 5 Results and Analysis/Experimental results interpretations: This chapter is about the analysis, interpretation, and describe summarized data and statistical results.

Chapter 6 Conclusion and Recommendations: is concerned with the summary, conclusions, and recommendations that were based upon the results of the study.

1.10. Conclusion

This chapter is a fundamental which presents background of the aspirational research trough the research problem. The proposed objectives and research questions are presented in relation to the research methods.

Chapter 2 STATE – OF - THE ART

2.1.Introduction

This chapter discusses the issue of concern to the research topic. Section 2.2 presents the different approach of electronic and digital signing systems. Section 2.3 discusses digital certificates. Section 2.4 introduces other proof of identity techniques. 2.5. Comparison. In the next chapter, we are going to see the literature review discussing the existing theories, which contain the definition of key terms and concepts by various researchers before.

2.2.Related Works

The review of all studies around digital signature and digital certificate present a large spectrum ranging from programming, cryptography, information system and cybersecurity. The first consulted research paper was centred to the huge security, personal rights and usefulness shortcomings encountered in current structures for identification management. Some of those troubles are properly known, whilst others are plenty less understood. This paper brings them collectively in a unique single, complete study and proposes hints to solve or to mitigate the troubles. A part of those issues can't be addressed without deep studies and development effort. The second is an article that explains identity management and profiling in relation to e-inclusion. E-Inclusion is a priority of the EU Commission within the framework of the i2010 initiative, and in particular the data protection challenges in E-Inclusive ICT are clearly defined in various national strategies for e-Inclusion in Finland, Norway, Portugal, Romania and Spain in (CE 2007). Inclusive information systems are tailored to the specific needs of users based on a profile of user skills [8]. In the aim of solving problem of some application a transitive signature to cross-certification was presented.

The next research has the aim of providing mediated signer-anonymity offered by 'group signatures. In another work, the author wrote to provide a formal hidden IBS model and two efficient constructs that explain the new primitive. Information security and digital signatures, non-repudiation improve the trust among users. ISO / IEC present specific, communication related, non-repudiation services using asymmetric cryptographic techniques. Similarly, in the document, a non-objection service was defined as a service that generates, gathers, manages, provides, and

reviews evidence relating to a claimed event or action to resolve disputes about the occurrence or non-occurrence of the event or action [9].

The fifth work explains why the cloud technology in the next generation has a must to focus on existing mitigation techniques form a deep analysis of security threats. Another reviewed article provides a general note on denial attacks by analyzing previous security issues in a cloud environment. Extensive reviews were presented on the same topic with satisfactory countermeasures [10].

The internet has made possible the creation of a worldwide information space including linked documents. This book, got here to shed a mild on an outline of the concepts of Linked Data, and the Web of Data that has emerged via the utility of those concepts. And in 2013, the authors showed us how we can ensure that only intended third parties have access to users' personal data. Trust was added to their Privacy Preference Framework to provide a more granular application of access control when exchanging information. This work is an improvement on the previous one [11].

The two authors present a configurable framework for signing any diagram data provided in RDF (S), named diagrams or OWL. The framework supports the signing of chart data at different levels of granularity as follows: Minimum Standalone Charts (MSG), MSG Sets and Full Charts. Supports iterative signing of chart data, e.g. For example, when different parts provide different parts of a common diagram, and allows multiple diagrams to be signed. Both can be done with constant and low overhead to result in instructions to be signed, even when diagram data is iteratively signed [13].

The HSV are alternative representations of the RGB colour model. HSV is one of the bio-metric verification which authenticates whether the signature is genuine or forged. In their work, Shashidhar Sanda & Sravya Amirisetti, proposed a new for online signature verification using classifier model and comparing techniques. The classifier model like Gaussian mixture models (GMM) is used to extract the physical and behaviour features. The comparison technique such as Longest Common Sub-Sequence (LCSS) is used for comparing extracted features [14].

Therefore, every time a company introduces a new technology, methodology, or approach, that introduction must be driven by a business need. To develop a business case for adopting DevOps, you need to understand the business needs and the challenges involved [17]. Software development

methods include activities such as analysis, planning, development, testing, implementation, maintenance, and decommissioning. All of them can be divided into two main categories [18]. The computer saves time and effort in solving complex and extensive problems quickly and efficiently. For this purpose, software programs are developed that make the work of administrators, offices, banks, etc. easier [19]. According to the author, a software consists of documents and programs that contain a collection that has been established as part of software engineering procedures. In addition, the goal of software engineering is to create suitable work that creates high quality programs [20]. Many people are involved in the development of complex software systems: software developers, testers, technical managers, managing directors, customers, etc

A book on programming light on means of starting a journey, it is a good idea to have a mental map of the terrain you are going to traverse. The same goes for an intellectual journey, such as learning to write computer programs [24]. Unfortunately, much of the community lacks useful tools for understanding and organizing languages because the standard literature is stuck in ill-defined and even confusing paradigm concepts [25]. This document describes the Pegasus framework, with which complex scientific work processes can be mapped to distributed resources. Pegasus enables users to represent workflows on an abstract level without having to worry about the details of the target execution systems [26].

The author welcomes us to the field of systems analysis, design, development, principles and practices. The book teaches the basics of systems analysis, describes system design and development practices [27]. This book introduces system design, Modeling, and simulation, some of the computer models used in designing, Modeling, and simulating the system, and focuses on the Modeling infrastructure provided by Ptolemy II [28]. The book begins with important background information about the web design environment, including the different roles you can play, the technologies you can learn, and the tools that are available to you. semantic structure of the content, including new elements introduced in HTML5. It covers everything from learning the basics of using cascading style sheets to change the appearance of text, creating multi-column layouts, or adding time-based animation and interactivity to your page. It continues with an overview of JavaScript syntax, the various file formats that are suitable for the web, and describes how to optimize them to keep your file sizes as small as possible [29].

In many countries, PKI (digital certificate) services and digital signatures are owned and operated by government and semi-private authorities. Most of the time CA has “Government” in its name. A public certificate authority is an external entity that issues certificates for a fee after conducting the necessary checks on the organization requesting a certificate [48].

Asymmetric encryption is a method of combining public/private keys to encrypt plaintext and using the same private key to encrypt passwords. Asymmetric encryption relies on asymmetric cryptography, also called public key cryptography[49].

In cryptography system, each public key corresponds to only one private key. A public key is public and can be shared widely, while a private key must be known only to its owner. The public key is derived from its private key using very complex mathematical algorithms. These algorithms ensure that the relationship between the two keys is one-way, which means that it is easy to calculate the public key from the private key, but impossible to calculate the private key from the public key [50]. Reason why the asymmetric encryption is a cryptographic encryption with a digital signature directly linked to its digital certificate.

In this example, the role of the AD CS server is to enable you to create a public key infrastructure (PKI) and provide public key cryptography, digital certificates, and digital signature capabilities to your organization. [53] Many other systems that allow users to digitally sign documents use an electronic signature (scanned handwritten signature) that is then stamped into a file.PDF file as proof of signature.

Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature Algorithm (DSA) that uses keys derived from elliptic curve cryptography (ECC). It is a very effective algorithm based on public key cryptography (PKC) [61]. ECDSA is used in many security systems, is popular in secure messaging applications, and forms the basis of Bitcoin security (with the "Bitcoin address" as the public key). An important feature of ECDSA and another well-known algorithm, RSA, is that ECDSA provides a high level of security with a short length. This increases return on investment because ECDSA uses less computing power compared to competing RSAm benchmarks [61].

The main difference between ECC and RSA/DSA is the strongest cryptographic strength that ECC offers for same key size. It has been revealed that ECC key is more secured than an RSA or DSA

key of the equivalent size. With ECC you are likely able to get equivalent cryptographic strength with significantly smaller key sizes about an order of magnitude smaller. For example, to reach the equivalent cryptographic strength of encrypting using a 128bit symmetric key would require an RSA 3072 bit key, but only an ECC 256 bit key [64].

When you receive approval for a PKI certificate, the source typically sends it to you via email. You can then save it to your computer to prepare for installation. When installing a PKI certificate, you typically need to use the control number from your request form to access the certificate and import it as a file to your computer. Once the file is downloaded on your computer, you can open it and review the general settings and confirm the installation process [63].

The smaller key lengths mean devices need less processing power to encrypt and decrypt data, which makes ECC a good choice for mobile devices, Internet of Things, and other use cases with more limited computing power. There are also notable advantages to ECC versus to RSA or DSA in more traditional use cases like web servers, as shorter key sizes enable stronger security with faster SSL handshakes, this translates to faster web page load times with best results. We should also notice that ECDSA, the original version of ECC, is a variant of DSA. ECDSA permits equivalent levels of cryptographic strength per number of bits as ECC [65].

For any of these Algorithm, they are pros and cons and implementation practices, it's important to understand, DSA is only for signatures, whereas RSA provides both signature and encryption. DSA is not very popular for recent systems because you must continuously ensure exchange and appropriate key implementation. And the process is vulnerable to quantum computers [65].

2.3.Related Studies Comparison

Multi-signatures from Digital Signature Algorithm (DSA) scheme coupled with Quick Response (QR) code and barcode to strengthen the system. Multiple-time signatures to be schemes of digital signature where signer or signer can sign pre-planned number of messages of documents. This provide significant efficient benefits over standard digital signature like DSA [30].

2.3.1. Comparison Tables

Method to be used in this research	Weaknesses	Strengths	Similarities
DevOps (Combination of the terms development and operations). Multi-signatures from "RSA" digital signature scheme coupled with Quick Response (QR) code to strengthen the system.	❑ Anonymity and privacy are issues of increasing concern in the internet and the offering of services such as anonymous channels is an important aspect of the future internet infrastructure if we want to retain fundamental rights such as free speech. ❑ In other hands, it is conceivable that an increase of malicious activity trafficking through anonymous communication networks (e.g. for distribution of child pornography). Another example shows how anonymous e-cash can be	❑ The DSbDS doesn't rely on third party system for certificate. ❑ All steps are done in a single system. ❑ Involved users' identity can be verified in the system. ❑ Ownership verification, reversibility and/or revocation. ❑ Easy to use. ❑ Compatible hands-on gadgets for use and verification. ❑ Very recent technics of encryption and signing systems. ❑ Can hold more information related to the signer, ownership, etc. ❑ Can be very precise and smaller. You can print smaller labels that carry more information. ❑ Easier to read - to read a barcode you have to aim the scanner in line with	❑ All these research papers are centered on similar topics, the use of digital signature and digital certificate and its applicability (anonymously automated and manually issued). ❑ All general objectives such as security, non-repudiation of information, identity protection, etc; are the same. ❑ The worldwide context of insecurity and forgery, the use of same medium here the World Wide Web, the need to protect

	used to commit a perfect crime. ❑ For many cases, multiples interfaces (instead of simplified interface) were provided to user to handle all processes. ❑ In most cases we have observed depletion of prevention methods and encryption techniques. ❑ Failure to provide a single portal where the intervention of a third-party system in not required.	the code, while a QR code can be read from any angle. ❑ Have a high error correction margin.	environment and reduce the use of paper documents is also another common characteristic. ❑ Very recently most recurred banks adopted Indexed TAN with CAPTCHA (iTANplus) but not for the same use, but for payments method only. ❑ QR scan were adopter in China since 2016 for smart cards used in transport. ❑ SSL Certificate & encrypted messages

Table 1: Comparison Table

2.3.2. Reasons for choosing Digital Signature Algorithm (DSA)

To reach the equivalent cryptographic strength of encrypting using DSA, a 128bit symmetric key would require an RSA 3072 bit key, but only an ECC 256 bit key. This enables us to build maximum secured system with high performance and load time. In the past, the use of digital signatures used small keys, which are not considered secure today. To reduce this: 2048 or 3072 keys will help to ensure security without losing of performance and load.

DSA Key Size (bits)	RSA Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Table 2: Key Size Analysis

2.3.3. Weaknesses

Anonymity and privacy are an issue of increasing concern in the internet and the offering of services such as anonymous channels are important aspect of the future internet infrastructure if we want to retain fundamental rights such as free speech. In other hands, it is conceivable that an increase of malicious activity trafficking through anonymous communication networks. Another example shows how anonymous e-cash can be used to commit a perfect crime.

In other hands, users claimed not being the sender of a particular message. Suspensions converge to lost or stolen private key which led to a forgery digital signature. The way public/private keys are generated, verified and stored does not provide enough guaranty to not be tempered or stolen. In most cases we have observed depletion of prevention methods, encryption techniques and failure to tackle the constantly expending hackers' tips and provide a single portal where the intervention of a third-party system in not required.

2.3.4. Strengths

The DSbDS doesn't rely on third party system for certificate. All steps are done in a single system. Involved users' identity can be verified in the system. Ownership verification, reversibility and/or revocation features have been improved. The system is easy to use, portable and present very recent technics of encryption and signing systems. It can hold more information related to the signer, ownership, etc. Provided interfaces are dynamically responsive, very precise and adaptive. You can print smaller labels that carry more information. Easier to read - to read a barcode you have to aim the scanner in line with the code, while a QR code can be read from any angle. In additional the system has a high error correction margin.

2.3.5. Similarities

All these research papers are centered on similar topics, the use of digital signature and digital certificate and its applicability (anonymously automated and manually issued) [31]. All general objectives such as security, non-repudiation of information, identity protection, etc; are the same. The worldwide context of insecurity and forgery, the use of same medium here the World Wide Web, the need to protect environment and reduce the use of paper documents is also another common characteristic goal. Very recently most recurred banks adopted Indexed TAN [32] with CAPTCHA (iTANplus[1]) but not for the same use, but for payments method only. QR scan were adopter in China since 2016 for smart cards used in transport, but still preferred over electronic signature and fingerprint use[33], which may be easily stolen from the database.

Message encryption is used to ensure that sending texts between two Android devices, including in group chats, outside actors won't be able to view or monitor your messages[34]. For every signing institution a public key certificate, also known as a digital certificate or identity certificate; is issued as an electronic document used to prove the validity of a public key[35].

[1] Combination of CAPTCHA and TAN

2.4.Conclusion

Briefly, from these research papers, we have found different approaches and technologies used to secure system, encrypt data, or transmit information to tackle certain numbers of encountered problems before. Inevitably, technologies get old and new sophisticated attacks are emerging. The trust between two parties transacting each other's, has never been compromised than today!

Generally, all these research papers were centred on similar topics, the use of digital signature and digital certificate and its applicability. All general objectives such as security, non-repudiation of information, identity protection against unauthorized users, etc.; are the same.

The worldwide context of insecurity and forgery, the use of same medium that is the World Wide Web, the need to protect environment and reduce the use of paper documents is also another common characteristic of the research papers.

Chapter 3 Research Methodology

3.1. Introduction

This chapter defines the research methods used and approach taken for the SDbDC system design. The organization of the chapter is the following: section 3.2 summarises the research objectives and questions. Section 3.3 outlines the research phases, next are principles of internet-based research method. And then, research methods. which were used in each research step. Section 3.4 defines research activities and methods for research Phase 1: requirement analysis. Section 3.5 describes the methods and tools for system design in research Phase 2, and Section 3.6 shows methods used in prototyping and JMeter in research Phase 3, including a narrative of tools used in this process. The chapter concludes by outlining the schedule for the study.

3.2. Review of Research Objective and Questions

The aim of this research is to design a software application being able to improve services related to digitally signed documents. This requires the determination of important characteristics of members in the process of DSbDC and to develop efficient functions to quickly automate admission process. To archive the aim of this research, the following questions are posed (ref: Section 1.4):

Question one: Do the proposed solutions measure up to the identify gap and problematic?

1.1. What are the main gaps identified in the current signing systems?

1.2. What are the proposed solutions?

Question two: Do defined functional and non-functional requirements matching the users' needs?

2.1. How were functional requirements addressed?

2.2. How were non-functional requirements addressed?

2.3. Were all the user needs put in consideration?

Question three: Can the provided prototype of digital signature be attributed, verifiable, linkable, reversible, revocable, potable and computable?

1.1. How can we verify the signature attributions?

1.2. Can a signing agent verify, link or revoke a signature?

1.3. Is the signature portable and computable?

1.4. How can we truck associated certificate valid?

Question four: Is the system performance and security up to the normal?

1.1. How can we truck the system performance?

1.2. How can we measure up the security of this prototype?

3.3. Adopted Methodology for Software Development

Like a human being, a software system has a life, a life time within which it is conceived, born, grow, gets old and die. In other word it starts boiling in mind as an idea and develops until it germinates, grow, subsists and at a certain point die when it is discarded. Among different SDLC Models, we have "Waterfall, Iterative, DevOps, V-Model, Spiral, Lean, Agile, Prototyping" models.

One of the newest SDLC methodologies that is being adopted by many software developers is DovOps: is a combination of the terms development and operations, meant to represent a collaborative or shared approach to the tasks performed by a company's application development and IT operations teams [17]. It is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than organizations using traditional software development and infrastructure management processes. As its name suggests, the premise of DevOps is to bring development teams together with operational teams in order to streamline delivery and support. The advantages of such an approach are that changes become more fluid, while organizational risk is reduced. Teams must have flexible resources in order for a DevOps arrangement to succeed [17].

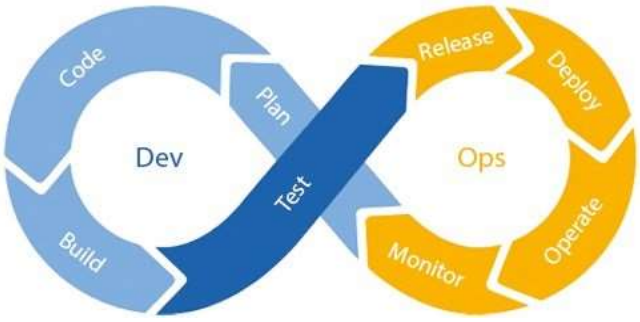


Figure 1: Eight Phases of DevOps life cycle

Source: https://intercept.cloud/en/news/what-is-azure-devops/

DevOps life cycle is constituted by: continuous development, continuous testing, continuous integration, continuous deployment, and continuous monitoring. In other words, to understand this DovOps life cycle eight phases, let us dived them into 5 familiar development steps as follows:

1. **Continuous Development (Plan and Code):** This is the phase that involves 'plan' and 'coding' of the software. The vision of the project is decided during the planning phase and the developers begin developing the code for the application.
2. **Continuous Testing (build and Test):** involves tools, teams, individuals, and services to verify and debug until the system is free of bugs. Testing for bugs early on allows them to be rectified quickly and easily. Continuous Testing is primarily a tool-driven activity. Here a new code is tested for bugs.
3. **Continuous Integration (can includes all phases):** The validated code can then be safely and continuously integrated with the master branch. Continuous Integration focuses also on interoperability of the system being developed.
4. **Continuous Deployment (Release and Deploy):** If the new version of the software has been tested and validated, it can be transferred to the production environment.
5. **Continuous Monitoring (Operate and Monitor):** When the new software is live, the operations team can use monitoring to obtain information about the performance and usage patterns of the app, to quickly report all issue and troubleshoot them.

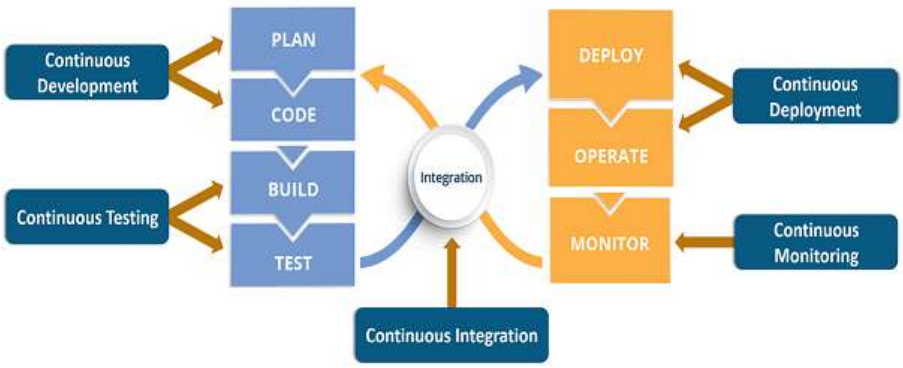


Figure 2: DevOps life cycle Phases divided into five familiar development steps

Source : https://www.edureka.co/blog/devops-lifecycle/

To effectively solve the research question as identified in this study, we have adopted a DevOps life cycle model, divided into five familiar development steps which was proposed by Patrick Debois and Andrew Clay in 2008.

As result, this customised model is composed of 5 phases (see figure X-Y):

(1) Continuous Development, (2) Continuous Testing, (3) Continuous Integration, (4) Continuous Deployment, (5) Continuous Monitoring.

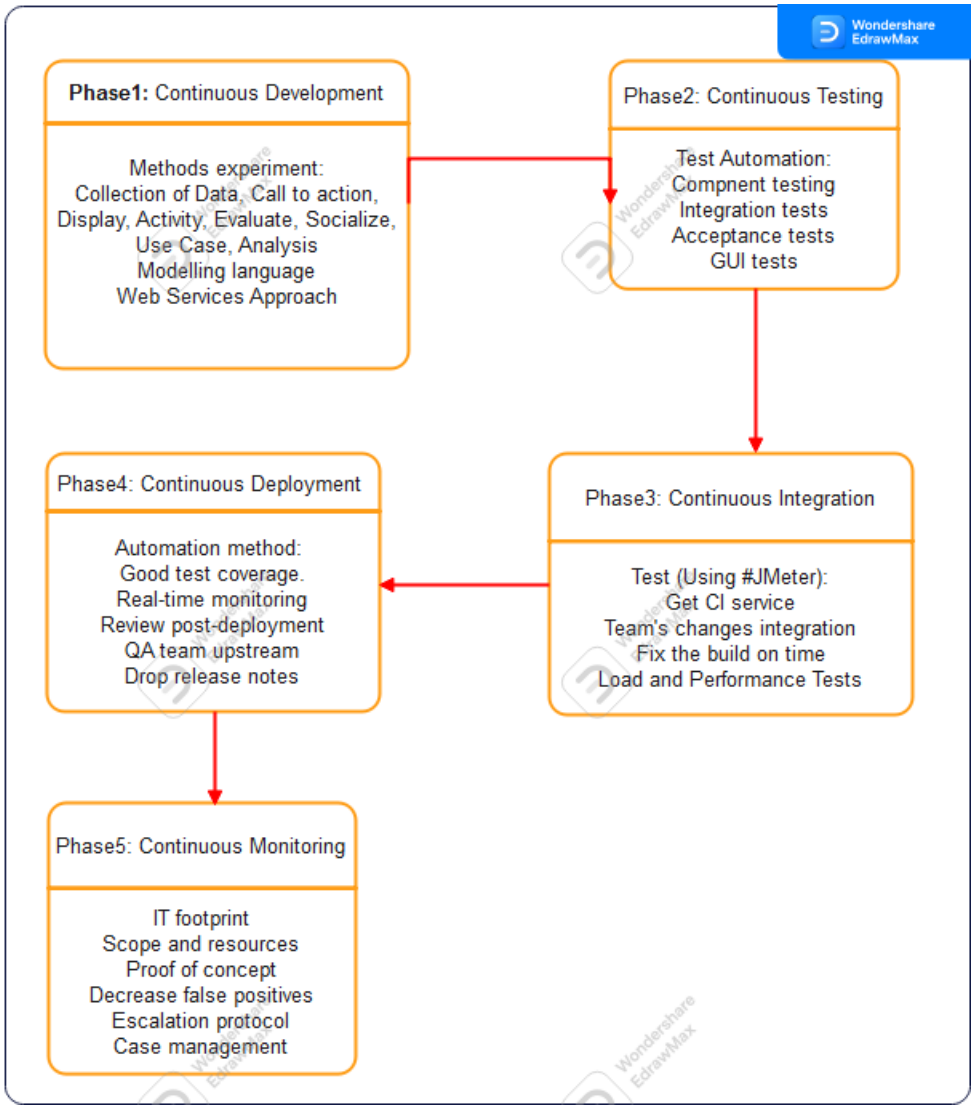


Figure 3: Methodology used in the 5 development steps

Source: own drawing

3.4.Methods employed

DevOps Research Methodology has the aim to improve collaboration and communication between Development, Operations and Stakeholders. DevOps come with a certain number of practices to enable automation of application deployment for a timely release and delivery. Users' insights were collected, analysed and put into functional and non-functional requirements to be automatically translated into required features for Digital Signature based on Digital Certificate. The general steps were represented in the figure No: 4. These features were identified, updated continuously, piece-by-piece, from the literature and collected data from the research. To address the problem in existing the literature, the user case analysis was used, to the particular case for Digital Signature based on Digital Certificate, solving the persistent issue of weak point in the existing workflow, accurately identifying it along the analysis process. Results analysis were classified in a representation figure at the end of the phase.

3.5.Data Collection Method

3.5.1. Study Population and Sampling

We have used non-probability sampling which is associated with case study research design and qualitative research. Case studies tend to focus on small samples and re intended to examine a real-life phenomenon. The scope of the study covers some of the processes (activities modules) of the whole system. The study population was all service seekers of DSbDC services. The overall target sample size of this study was 300; the achieved size 151 that is 50.33% of coverage. In all cases, customers were contacted via online platforms, calls and social media due to the COVID-19 pandemic and preferred methodology for data collection. Those who accepted to participate, passed the interview via video call. This was not easy to reach the initial sample size in the study time fame.

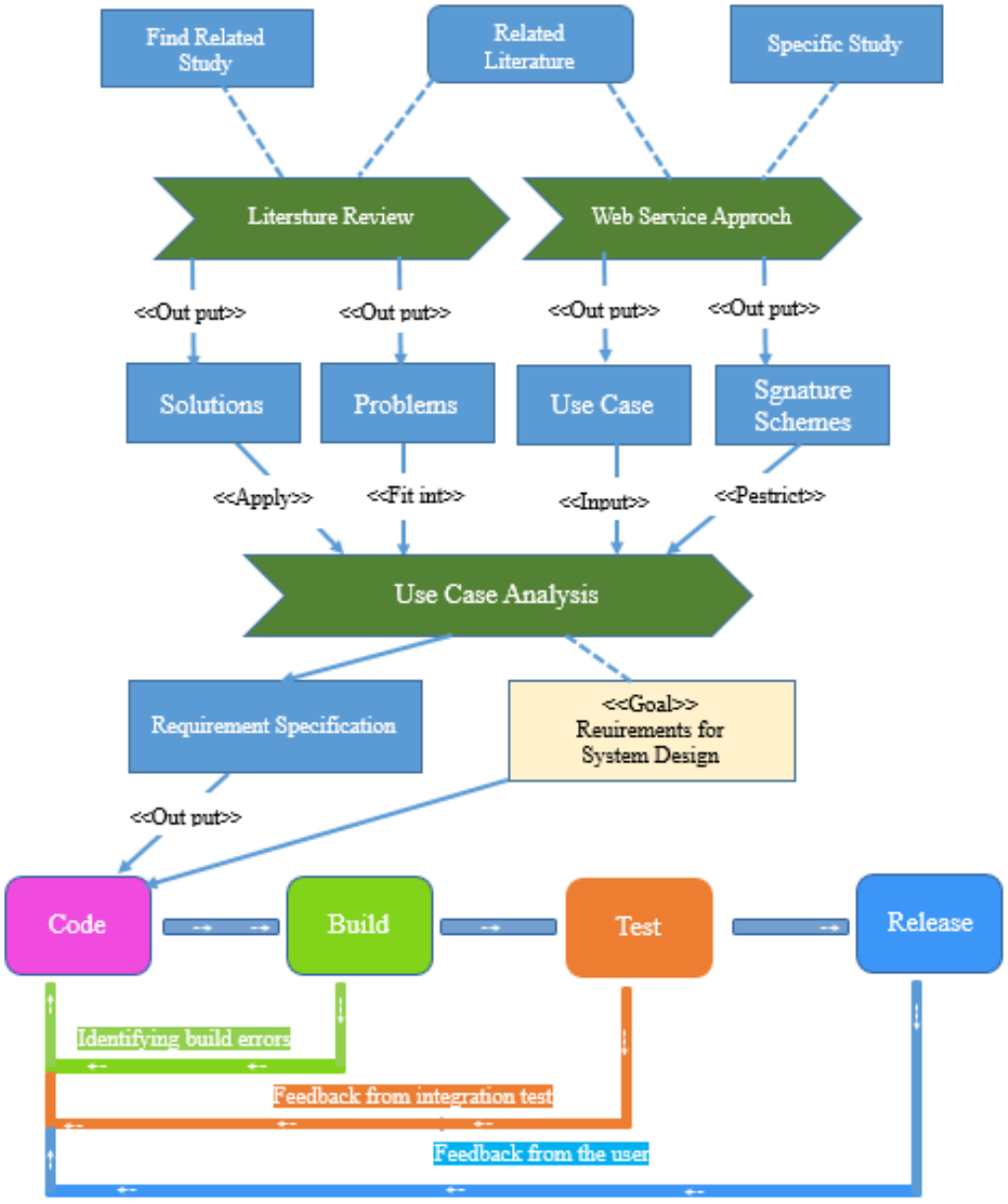


Figure 4: Input and Output in each step of this research phase

Source: own drawing

3.5.2. Data collection and Analysis

Design a workflow for improving the steps of digitally signed document is a must of a lots of requirements, enables elimination of difficulties in the processes that may eliminate the delay and forgery. The ability to review the literature review is important, but crucial is analysis process for this research paper, considering the existing policy, standards protocols. Operational protocols are required to deliver certificates and CRLs (or status information) to certificate using client systems. Management protocols are required to support on-line interactions between PKI user and management entities [36]. For this phase, the literature review was indubitably the main method for data collection in this research. With the objective to strengthen and intensify the research knowledge on the "Analysis of Digital Signature based on Digital Certificate". This implies to consolidate and intensify the solid knowledge, reviewing all details of problematic as presented in in the literature and possible environment to affect or/and cause these problems; come out with possible and suitable solutions as proposed in some studies.

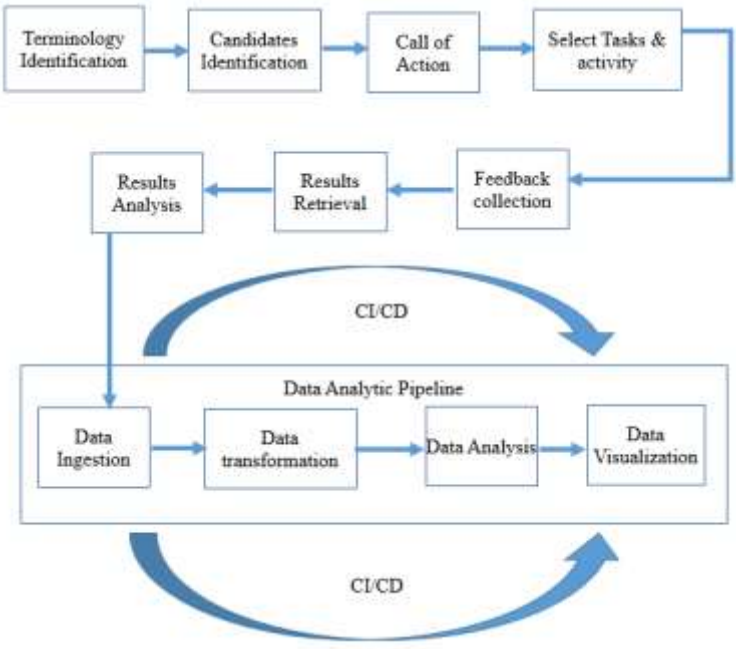


Figure 5: Data Collect Procedure

Source: own drawing

Aadil Hasan (2020) explained DevOps Methodology as the new tech-word that is creating buzz in the software field and the software development strategy that bridges the gap between the development and operational team. Lucy ellen lwakatare (2017) provided the concepts, practices, benefits and challenges of DevOps adoption and implementation in software development practice [37]. According to system and software life cycle standards used for designing software intensive products and services [38], technical processes and corresponding activities in software development are well expressed in DevOps.

Step 1: Data Presentation

Primary and secondary data were observed together depending on the elements used in data gathering. As explained by the interviewees, it enables people to understand the current workflow for updating Digital Signature Based on Digital Certificate. Establishing a model through BPML (Business Process Modeling Language) and the workflow of application request of digitally signed documents is the focus of this research.

Step 2: Data Analysis

The modeling workflow was analyzed, which shows the current situation in the request of digitally signed documents. This analysis is supported by both interviews and direct observations. The mixture of this data enables us to identify the achievements of the signing process so far and the remaining barriers that may interfere with the right of applicant and signatory in another hand to possess and legal documents.

Step 3 Design Requirement Definition

As the last part of the process, the validation will be conducted in this way:

- Evaluating requirement: Compare the current situation with the new situation proposed by the new workflow. Evaluation is to check whether the design requirements are complied with and whether the main obstacles are eliminated.

3.5.3. Evaluation Method

The DRA has been evaluated using an empirical evaluation approach. The empirical evaluation includes an industry case study and survey. The case consists of five steps: design, prepare, collect, analyse, and report. The industry survey comprises different five stages: plan, prepare, develop, deliver, and report. The empirical evaluation process is presented in figure N° 7.

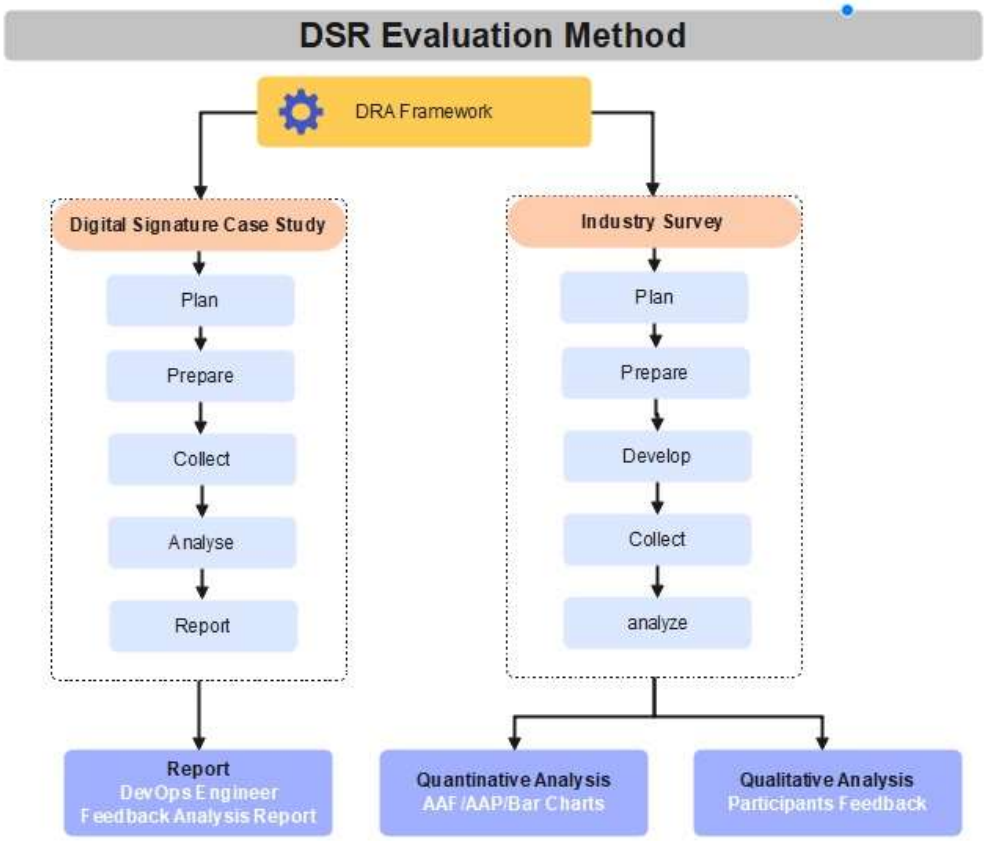


Figure 6: DevOps Reference Architecture (DRA)

Source: own drawing

DevOps Reference Architecture (DRA) empirical evaluation present the evaluation stages (case study and survey). During these stages the evaluation data is verified and analysed to find out the applicability of the DRA.

3.6. Justification behind the analysis

The importance of this research lays in users' participation, the simplicity of the system for users, the performance and level of security attained when securing sensitive information and documents. It is a jump into cryptography and security for the world today. It is another proof that software development can provide significant benefits to businesses. It can improve the speed, efficiency, and quality of software development, while also improving communication and collaboration

between development and operations teams. Additionally, it can help to improve the scalability and maintainability of software.

To answer our research question to know if the proposed solutions measure up to the identify gap and problematic, different algorithms pro and con were analyzed and continuously tested with users to improve the speed, efficiency, and quality of software development, while also improving communication and collaboration between stakeholders.

The algorithm uses low numbers of keys comparatively to Elliptic curve cryptography (ECC) and the Rivest-Shamir-Adleman (RSA). For example, to reach the equivalent cryptographic strength of encrypting using DSA, a 128bit symmetric key would require an RSA 3072 bit key, but only an ECC 256 bit key. This permit to acquire better performance in security load time with low consumption in memory. In other hands ECC in very complex to implement. DSA was proposed by the National Institute of Standards and Technology (NIST).

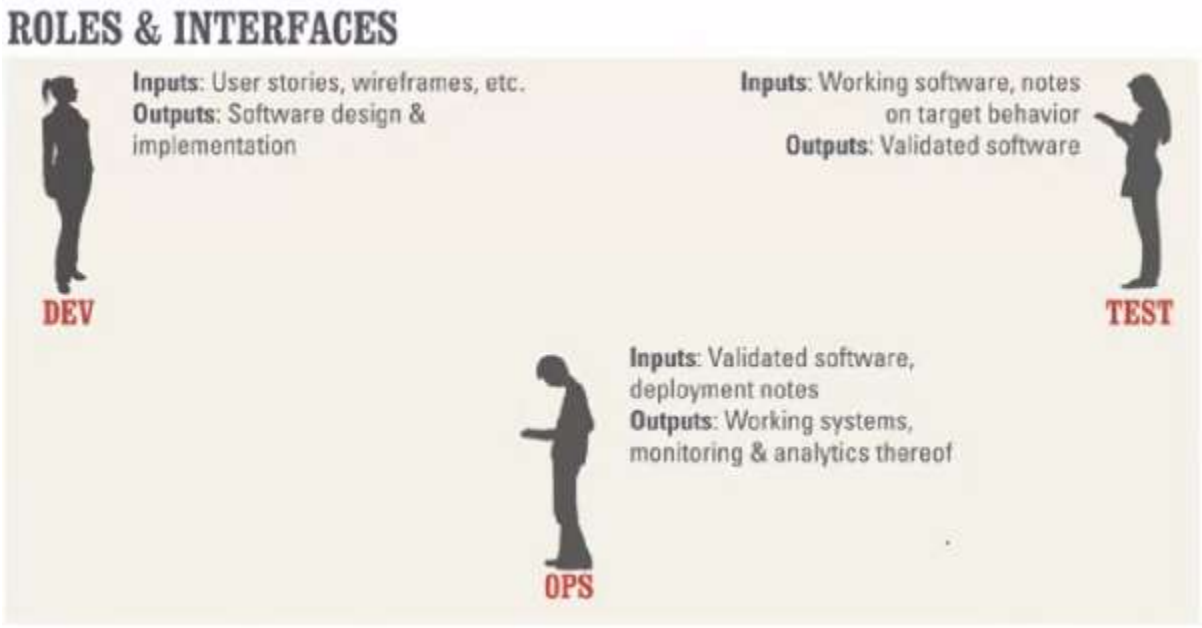


Figure 7: roles and interface involved in DevOps analysis

Meanwhile, the team works smart and fast and provides good quality to their customers. Greater use of automation and collaboration reduces complexity and errors, improving mean time to recovery (MTTR) in the event of incidents and outages.

Chapter 4 System Analysis and Design

4.1. Introduction

In many situations, business process improvement results from examining business processes, creating new and redesigned processes to improve process flows, and/or leveraging new technologies that enable new process structures.[39]

This chapter presents in detail the results of the field study in Research Requirement Analysis. Section 4.1 introduces the workflow Modeling technique. Section 4.2 presents the signing system workflow. Section 4.3 presents Transaction Behind. Section 4.4 details the Finding behind the analysis. Lastly section 4.5 presents the system design.

4.2. Workflow Modeling technique

Business process modeling has been essential to businesses for many decades, and organizations successfully apply modeling techniques and tools. Although modeling systems are intended to be visual, they are often accompanied by varying levels of documentation to provide more detailed information when necessary. [40]

In reality, the situation is usually like this: "We all know, more or less, how our part of things works" and "We all know what a problem or symptom is, but not the root cause." Now it's time to talk about it to think about how to address this and find a common understanding with everyone involved.[41]

The goal of most process modeling projects is to document, understand, and analyze an organization's key business processes. [42]. Therefore, there are important activities of understanding (description) and specification. We can divide these interoperability specifications into two categories: workflow modeling specifications and workflow description (i.e.design time) and runtime interoperability specifications.

Workflow management is about optimizing, improving and automating workflows wherever possible to increase throughput, eliminate rework and reduce errors. Using a workflow system, various processes can be automated in a linear sequence according to business rules. Both mechanical and human tasks can be automated using a workflow system.[43] In this studio,

Process Modeling is a technique for describing the current situation in Digital Signature based on Digital Certificate.

Process Modeling requires identifying workflow elements such as tasks, participants, information systems and human resources competencies. Requirements Modeling in software development identifies the requirements that a software application or system must meet in order to solve the business problem. Requirements are divided into functional (what the system must do) and non-functional (constraints within which the system must function).[44]

Many requirements were obtained from surveys, online meetings, feedback and various literature and used to evaluate current business processes. This allows us to identify potential for improvement and suggestions.

4.2.3. Other Modeling techniques

Process flow Modeling is the core technique, but additional techniques are required to establish the context and visibility of the process to ensure that critical factors are taken into account alongside workflow. [45]

Further Modeling techniques include (1) Flow charts; (2) Data flow diagram, (3) Gantt Chart, (4) Role activity diagram, (5) role interaction diagram, (6) Data Flow Diagrams, (7) Colored Petri-net, (8) Integrated Definition for Function Modeling (IDEF) and (9) Object Oriented methods.

4.2.4. Unified Modeling language (UML)

UML was used to find a common understanding among all parties involved in building, documenting and visualizing systems. Around the year 1997, the Unified Modeling Language (UML) was accepted as the standard language for object development. The goal of the Unified Modeling Language is to provide a common vocabulary of object-based terms and diagramming techniques comprehensive enough to model any systems development project from analysis to design. The current version of UML, version 2.0, was accepted by the Object Management Group (OMG) in 2003.This version of UML defines a set of 14 diagramming techniques for Modeling a system. [46]

The common Unified Modeling Language (UML) diagrams used in this phase include activity, sequence, collaboration, state (transition), and interaction overview diagrams. [System Analysis

and Design.pdf]. It is a modeling syntax that is primarily intended for creating software-based system models, but can be used in several areas. UML uses object-oriented design concepts, but is independent of a specific programming language and can be used to describe general business processes and requirements.[47] To show how the system works, we use a special modeling language called UML. We even show human actors as puppets interacting with business functions called use cases.

4.3.Presentation of Finding

To understand the process of acquiring a PKI certificate, the protocols and procedure were explained by IT guys interviewed from different institutions. They are the ones who are directly involved in the request, installation and calibrating on PKI certificates for the mass users. They provided detailed list of needed documents and system requirements.

4.3.1. Digital Signature Algorithm (DSA)

Digital Signature Algorithm (DSA) uses a different algorithm than RSA to generate public/private keys based on regular expression and the logarithm problem. It provides the same level of security as RSA for keys of the same size. DSA was proposed by the National Institute of Standards and Technology (NIST) in 1991 and was approved by the Federal Information Processing Standard (FIPS) in 1993 [59].

The purpose of digital signatures is to authenticate and verify documents and data. This is necessary to prevent fraud, digital manipulation or falsification in the publication of official documents.

With one exception, they work on building public private keys. In general, asymmetric keys encrypt using the public key and decrypt using the private key. On the other hand, the opposite is true for digital signatures. The signature is encrypted with the private key and replaced with the public key. Because the keys are linked, generating a statement using the public key verifies that the correct private key was used to sign the document, verifying the source of the signature [60].

Digital Signature Algorithm (DSA)

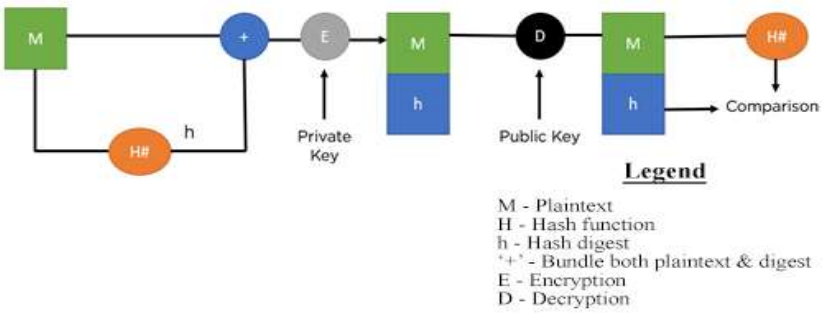


Figure 8: Digital Signature Algorithm (DSA)

Source: own draw

4.3.1.1. How does DSA signature work?

A. DSA signing

Alice composes a message M that she wants to transmit to Bob. He also creates a digital signature S of the message using his private key. She then sends the message with a digital signature to Bob. Then the process follows,

- ✓ Alice has created a message M that she wants to send to Bob.
- ✓ Alice then generates a random number k with the computer = (g^k mod p) mod q.
- ✓ After that, compute s = (k^-1 * (H(M) + x*r)) mod q, where H is the cryptographic hash function and x is Alice's secret key.
- ✓ Alice's digital signature, S, is the pair (r, s).
- ✓ Alice pushes a message M with its digital signature S to Bob.

A. DSA verification

Bob receives Alice's message M and digital signature S. He then uses an authentication method using the public key (p, q, g, y) that Alice shared with him to verify his signature.
Bob uses the public key to verify that Alice's digital signature is valid and matches M's message. He does this by entering the following information:
We consider;

- ✓ H(M): hash of Alice's message,
- ✓ s: Alice's signature
- ✓ r: the first part of Alice's signature
- ✓ g: the generator
- ✓ y: Alice's public key,
- ✓ p: the modulus, and
- ✓ q: the prime number.

To verify the message that Alice signed, Bob first reads it

- ✓ r = (g ^ x mod p) q.
- ✓ Bob then calculates:
- ✓ s = (y^r * r^x mod p) current q.

The verification is done by checking if s = M, then the message is verified.

4.3.1.2. DSA Key generation, Sign file, Verify Signature

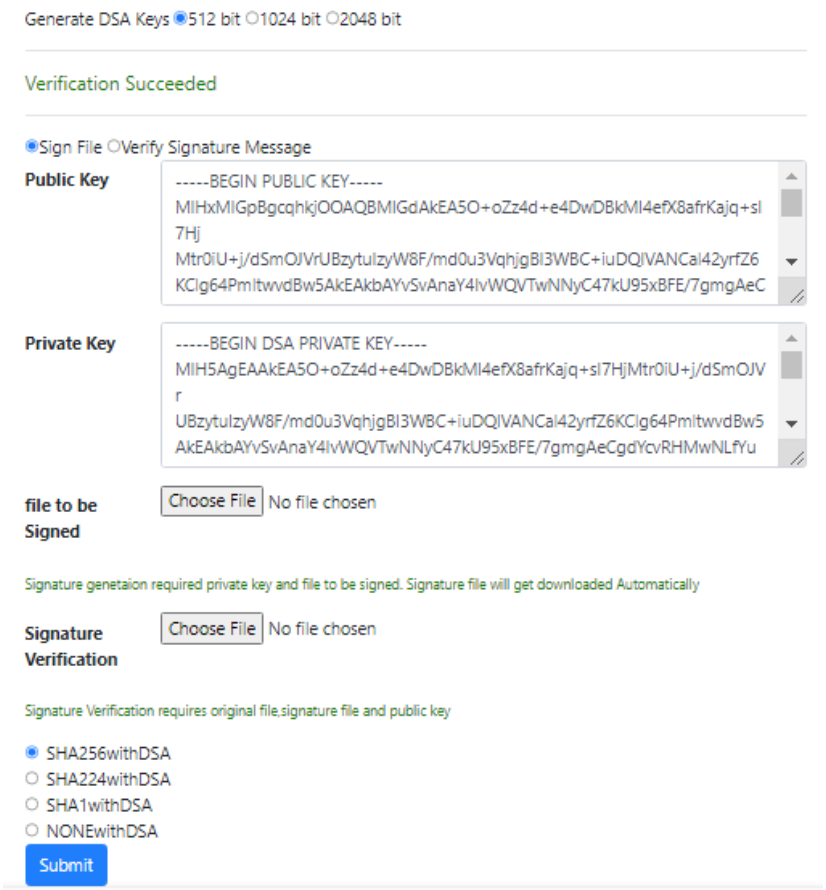


Figure 9: Sign a file and verify signature with DSA

4.3.2. QR code and Barcode

4.3.2.1. QR code

Contains useful personal information of the signer, such as contacts number, email, identity number, staff ID, positions and system user ID. We generate a QR code with text in Java using ZXing Library from Maven Repository.

In QR code, error correction is done using Polynomial Long Division in some specific method from two professors Reed and Solomon and it is called Reed and Solomon error correction. The awesome thing in it is that if you are missing part of the message and you have an error corrector, you can reintroduce the missing parts by looking at the error correction and perform some Mathematical steps.

The so called Polynomial long division is slightly more complicated than standard long division. To understand the process let us take an example of a simple polynomial long division, below:

$3x^2 + x - 1$ (the dividend) divided by $x + 1$ (the divisor).

The above polynomials are first put into a small table (reference made from Wikipedia long division for more details on this notation)

$x + 1 \mid 3x^2 + x - 1$

For every step of the long division, multiply $x + 1$ by anything to make its first term equal that of the polynomial at the bottom of the table.

At the first step, $3x^2 + x - 1$ is at the bottom of the table, so multiply $x + 1$ by $3x$. This solution in $3x^2 + 3x$, which has the same first term as that of the polynomial at the bottom of the table. Thus, the updated table becomes:

$$\begin{array}{rl} & 3X \\ X + 1 & \mid 3x^2 + x - 1 \\ & 3x^2 + 3x \end{array}$$

Next, subtract $3x^2 + 3x$ from $3x^2 + x – 1$. Now, the result is $-2x – 1$ (because $x – 3x$ is $(1 - 3)x$, or $-2x$). This $– 1$ at the end is usually carried over from the original polynomial. Thus, the updated table becomes:

		3X
X + 1	$3x^2 + x -1$	
	$3x^2 + 3x$	
	$- 2x – 1$	

For this time, multiply $x + 1$ by a term that will result in the polynomial whose first term is the same as that of the bottom polynomial. It is clear that we use $-2(x + 1)$ to get $-2x – 2$. Thus, the updated table becomes:

		3X - 2
X + 1	$3x^2 + x -1$	
	$3x^2 + 3x$	
	$- 2x – 1$	

A. Maven dependencies (Core image dependency and Java Client dependency)

```
<dependency>
   <groupId>com.google.zxing</groupId>
   <artifactId>core</artifactId>
   <version>3.5.0</version>
</dependency>

<dependency>
   <groupId>com.google.zxing</groupId>
   <artifactId>javase</artifactId>
   <version>3.5.0</version>
</dependency>
```

Table 3: ZXing Library dependencies

4.3.2.2. Barcode

Barcodes encode document information into bars and alphanumeric characters, making it much faster and easier to record and track on any stored document

A. Maven dependencies

```
<dependency>
   <groupId>com.google.zxing</groupId>
   <artifactId>core</artifactId>
   <version>3.5.0</version>
</dependency>
<dependency>
   <groupId>com.google.zxing</groupId>
   <artifactId>javase</artifactId>
   <version>3.5.0</version>
</dependency>
```

Table 4: ZXing Library dependencies

4.4.System Design

4.4.1. Use Case Diagram

The "use case diagram" presents a short explanation of the use of use cases. Every single use case is represented by an eclipse and a name of its use case. A rectangle denoting the system limitations serve to encircle the use case. A concerned actor who is represented in a scenario is symbolized by a stick figure with a label of the actor below [66]. [Hans van Vliet - Wiley 2007]

Use case diagram

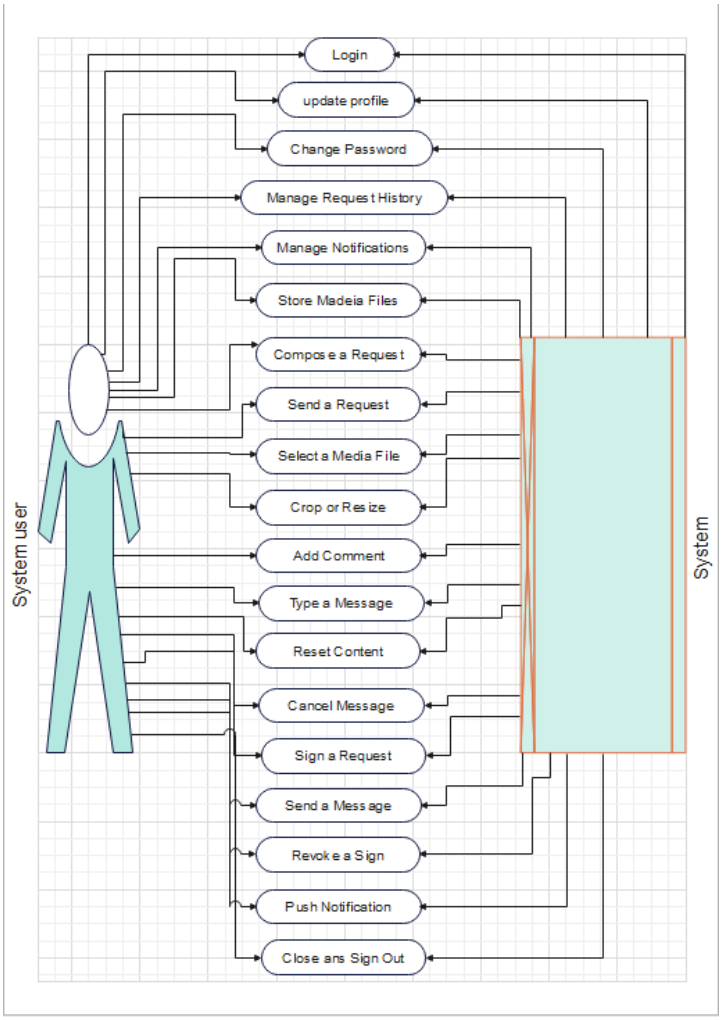


Figure 10: use case diagram

Source: own drawing

4.4.2. Workflows of Digital Signature (flowcharts)

First of all, workflows static. They are also technical activities organized within a single phase which may be used during the development phase to reach goals at every step [67].

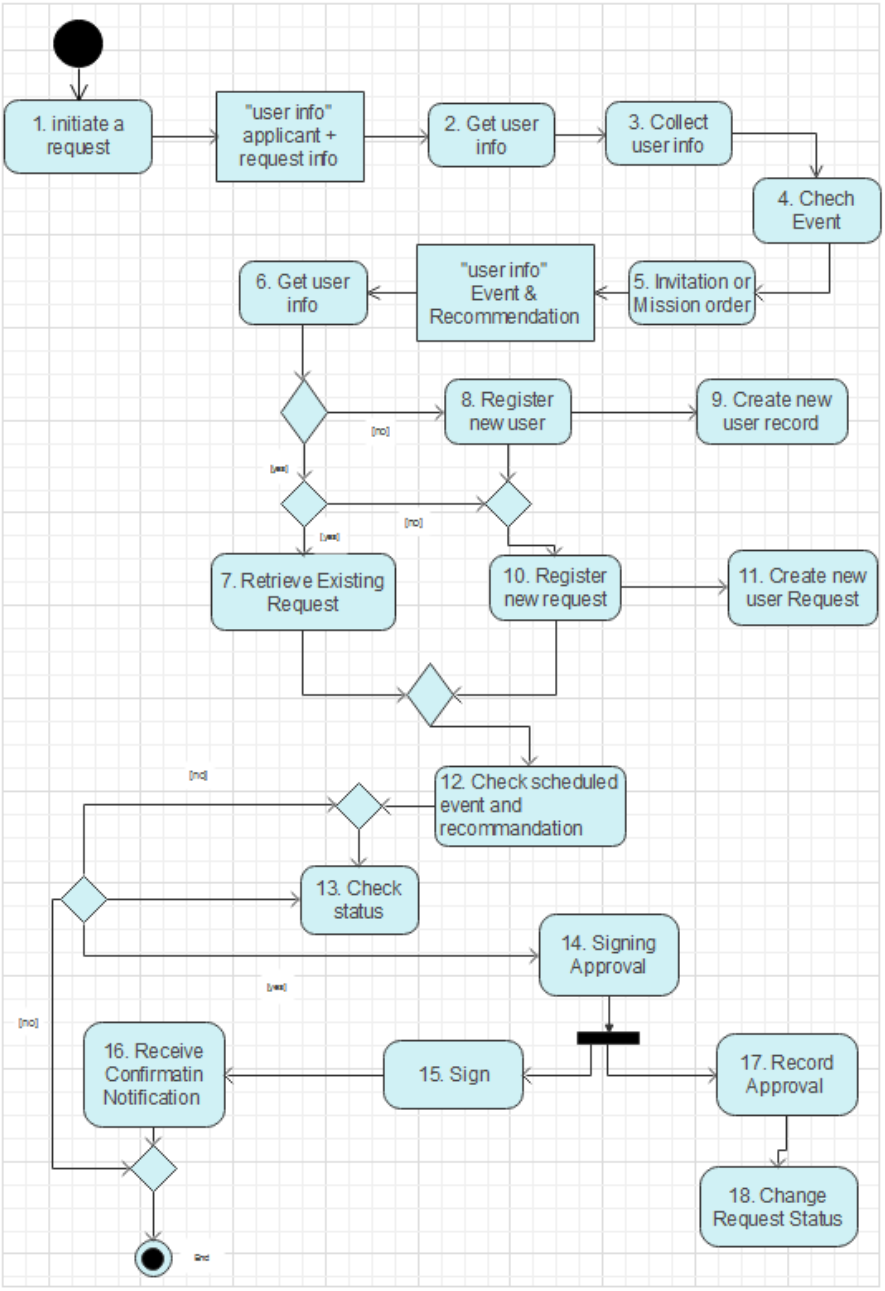
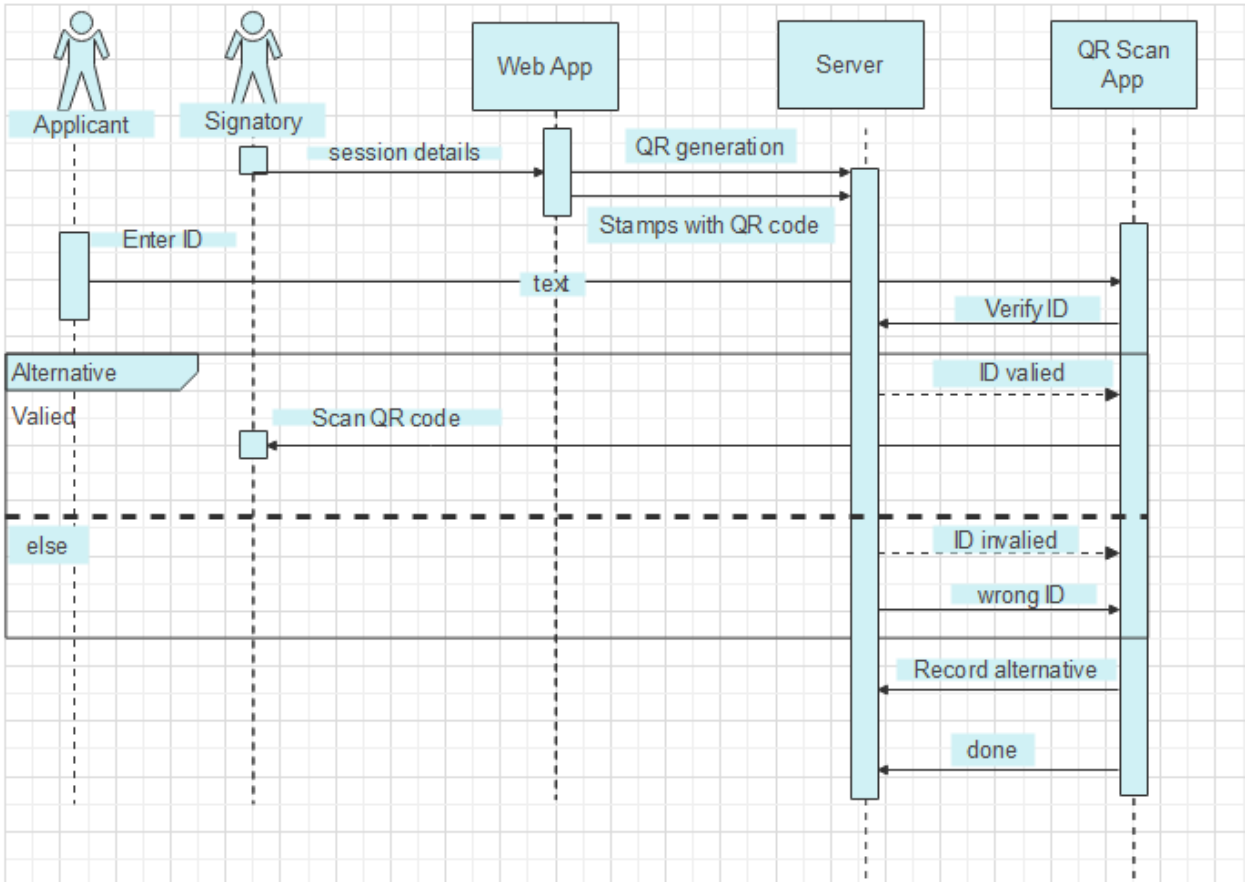


Figure 11: Digitally Signing Request

Source: own drawing

4.4.3. Role interaction Diagram (Sequence Diagram)

A "Role interaction Diagram" is a kind of diagram that shows an interaction representation, which is a group of messages transmitted between objects during a well-coordinated exercise to accomplish an assignment of a project [27].



Interaction Sequence Diagram for QR signing

Source: own drawing

4.4.4. Role Activity Diagram (activity diagram)

For "activity diagram", each block of column represents an activity or task. An arrow linking one activity to another describes the cause of relationship between two activities. An activity in shape of diamond tests for a condition, and it is a direct cause for the activity on one of its outgoing branches to happen. "Activity diagrams" are also classified into split and join activities, which generate multiple concurrent activities, and wait until its completion [28].

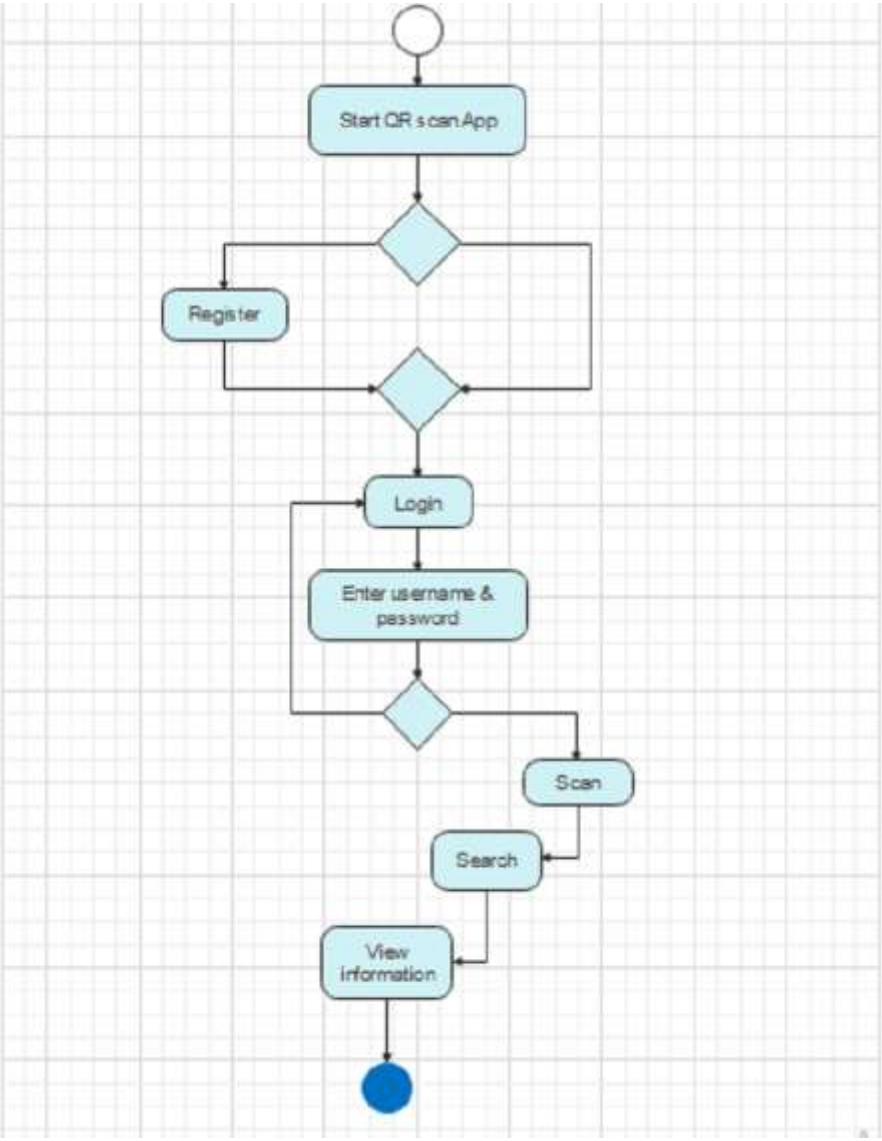


Figure 12: Activity Sequence Diagram for document verification

Source: own drawing

4.4.5. System Architecture Design

"System Architecture Design" is way to efficient and effective spawn systems, by presenting overviews with an idea of keeping integrity, balancing and consistency. In other hands, "System Architect Design" serves to find way to reach goals in a very complex, dynamic and none guaranteed World [68].

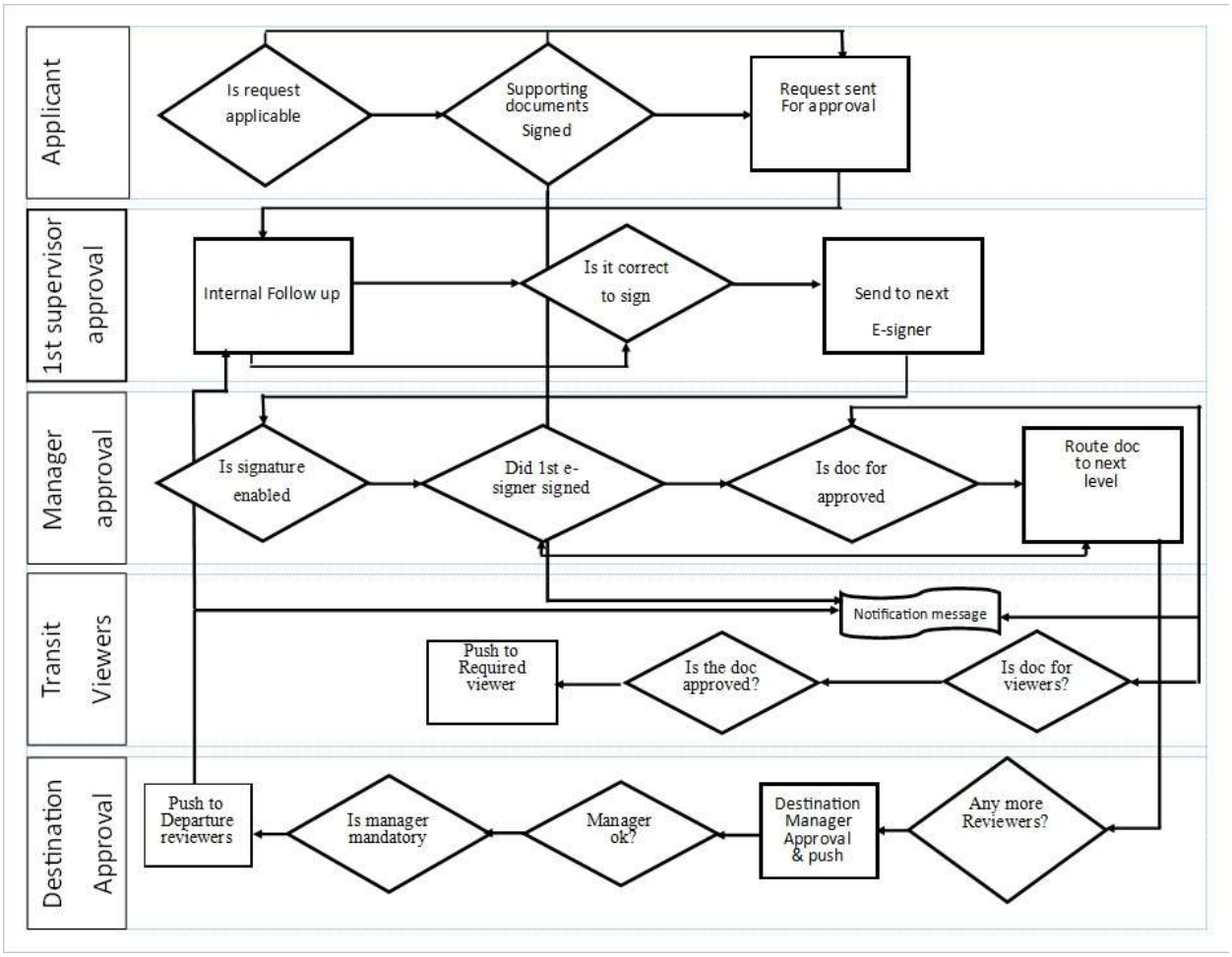


Figure 13: System Architecture Design

Source: own drawing

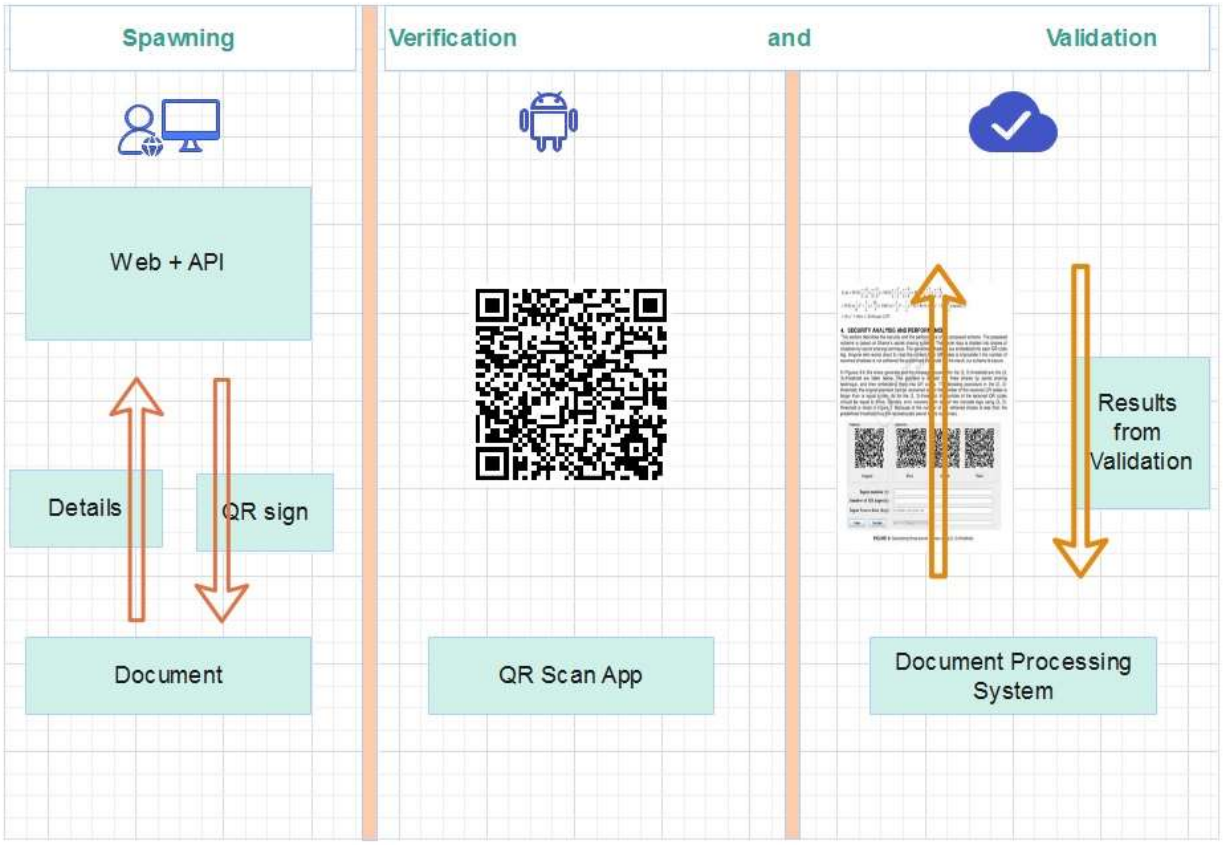


Figure 14: DSbDC, QR Spawning system

Source: own drawing

The system presents the four main components: Multiple Authentication Login Register, Request Recording, Request Approval and Sign, Document Authentication Verification via QR Scan.

Chapter 5 Results and Analysis

5.1. Introduction

The previous chapters define the current situation of official document signing service, request and signing process. The requirements design is presented in a way to eliminates the constraints and barriers of users when requesting for an official signed document and match the study objectives. This chapter serves to define a new work flow to improve official document signing service by the use of digital signature based on digital certificate. The proposed model is derivative from the defined requirements, whereby the chapter presents the validation of the designed workflow.

All the functionalities implemented in the prototyping are subject and defined by the boundaries of the presented scope of this thesis. If it cannot cover all the type of digital signatures and features, the development of digital signature based on digital certificate were centered on a certain number of features to provide an integrated digital signature scheme, the use of website portal and a database, coupled with verification and validation methods [38].

Section 2 covers the Java Cryptography Architecture/Extension (JCA/JCE) model and based on Linux Ubuntu platform. Section 5.3 introduces the components design. Section 5.4 present the database model. Section 5.5 Evaluation of online Digital Signature based on Digital Certificate. The end point of this chapter is a short summary.

5.2. Proposed workflow for official document signing service

The design of the proposed workflow is based on the stated demands. The strategy starts with an interconnection of systems for which databases are required in the human resources identification, reducing the number of documents submitted, saving the time and enabling user to complete the application while working on their daily tasks without taking hours between offices. With this we have met our objectives. "Analyse the existing workflow, identifying the gap for improving the documents' signing methods, Study the required systems features and inter-connection to facilitate flexible deliverance and facilitate management, implement a user centred design for the signing system with elucidated requirements putting an accent on user interaction with the system."

System interconnection is made easy by the use of API to access on request needed information for staff/user registration and application. No need to compiler documents, fulfil a form nor hand the file physically to different offices. The whole process can be done in a single portal.

Implementation of QR code helps us to show signature on the approved documents. Anyone can scan the QR code to verify the authenticity of any documents. Embedded information tells us more about the signing institution, the signer, purpose, dates and validity of the document.

The PKI use facilitate the encryption of data using public-key cryptography, information sharing, and storing which strengthen the authentication, trust and security among users. The main benefits of traditional PKI are that it provides a high level of security and can be used to encrypt data in transit. [69] By this, we completed our last objective "With the implement means for verification for the signing system, verify and validate that changes are aligned with the new work process for the designed signing system." This enables us to perform a simulation of the current signing methods through the new designed workflow.

The below listed systems and technologies are involved into singing of official documents among institutions:

1) **Institution/Enterprises:** any entity willing to collaborate with us. Employers has database records for their respective employees. Employers are fully responsible of their database, employees' records, signers chosen among other staff to represent the institution or enterprise.
2) **QR code:** A QR code (quick-response code) is a type of two-dimensional matrix barcode, invented in 1994, by Japanese company Denso Wave. A quick response (QR) code is known as a type of barcode that has the ability to store information and can be decoded and read by a digital device, such as a cell phone.[70]
3) **PKI:** A public key infrastructure is composed by roles, policies, hardware, software and procedures important to generate, control, issue, use, reserve and revoke digital certificates and manage public-key encryption. The principal idea is to have one or more trusted parties digitally sign documents to certify that a particular cryptographic key is owned by a particular user or device. PKI is associated to asymmetric encryption, digital signature and encryption services.

4) **Confidentiality:** A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized actor rather than endangered, at-risk, or potentially exposure. Confidentiality is archived by the use of Public Key Infrastructure. The last signer uses a public key to encrypt the message. The applicant uses its private key to decrypt the message. At this level the signature is attributable signatory and linked to the applicant.
5) **Integrity:** Translate the state of a message that has not been tampered with or altered. The best way is to use a hash function that combines all the bytes in the message with a secret key and produces a message digest that is difficult to decrypt. A cryptographic checksum that is computed to ensuring that the data has not been tampered with or modified during transmission. In this way a receiver runs the cryptographic hash function again and compares the new digest with the previous one.
6) **Authentication:** authentication ensures the identity of an individual, device or application is advertising the message is accomplished using digital signature. Authenticity is the quality of being genuine or real for both sender and receiver and vice-versa (linkable). Mostly coupled with authorization, and accounting to form the triple A (AAA) is taken as a security framework that is in charge of controlling access to computer resources, enforces policies, and audits usage. Non-Repudiation: Non-repudiation means a user cannot deny, in any way, having performed a transmission.

With this new model, the entire process will be done online. The physical application, the use of hard copy document is nullified. With the use of PKI, users can process their applications and signatories receive and subsequently approve them. In this way, we can conclude, the new model secures electronic data exchange with the PKI.

To address the gaps exposed in the current model of official document signing system we have designed the new proposed model as shown below. A unified single system is shared by all stakeholders. Every institution has a subdomain from the main domain which is secured with a self-signed security socket layer certificate. A sign server system is coupled to the main portal to implement SSL every time a signing entity register for the service and then a subdomain is organized for that particular purpose. External links are built via API (product[post] and consumer[get]), Spring Security is configured to use JWT. The application is secured and protected

using JSON web Tokens. The information exchange and sharing and the new integrated model for official document signing described in the above linkage are explained below:

Step 1: Applicants for official document are for most of them individuals with acceptable level of computer literacy as they are mainly employers from government institutions and private sector. At this particular step, the new model requires them to have an active account. If new, the it is advised to sign-up for the first time, create and do profile update. The right owner should have logged in to proceed with application for official documents or any other profile related modification.

Step 2: At this level, the owner proceeds on requirement verification depending on the nature of the document the user is applying for. Once the request is specified, a list of required documents is specified for the user to compile them.

Step 3: Fulfil the form providing all necessary information, add required attachments for submission and send them. If everything is fine, the request will be sent. Otherwise, the applicant must verify mandatory fields.

Step 4: The first signer login to receive the request, goes through it to verify if provided information is correct and make the notification using PKI digital Signature, and approves for the next process to next signer. If the process does not require a next signer, this signer may only update the application with missing information and record the document into the database after signing it with QR code.

Step 5: The second signer login to receive the application request, goes through it to verify if provided information is correct and make the notification using PKI digital Signature, and approves for the next process to last signer. If the process does not require a next signer, this signer may only update the application with missing information and record the document into the database after signing it with QR code.

Step 6: The last signer login into the system to receive the application request, goes through it to verify if provided information is correct. The signer updates the application with additional information, approve and sign the document with QR code. The signatory records the document

into the database and push the notification using PKI digital signature. An original copy is sent to the applicant and the authority requesting it.

Step 7: The applicant, here the document owner, receive the notification, log into the system to check and download the signed document.

Step 8: Depending on the use, the owner may decide to hand the document to the authority requesting it but they already have it from the last signer. In case of mission additional information such as arrival and departure date will be updated and another signature for the responsible authority is needed. Before signing the destination, signatory will proceed to a systematic verification comparing the document received from the signing institution and the owner of the document.

Contribution of the new workflow

Current process workflow	**Proposed workflow process**	**Solution**
Requirements verification for submission documents is done manually and mostly in informal ways.	Required documents for submission are specified by the system according to their category.	We have prepared a list of required documents and mandatory information to be provided during application process.
Compiling required hardcopy documents and enormous gymnastics to collect documents.	Needed documents will be retrieved from the interconnected databases from respective partners and users.	Remove the burden to print, copy, move to different offices, pay the cost, lost, stolen or misplaced document and even risk of forgery. API implementation serve us to retrieve such documents and information from our partners.

Application submission and reception of the requested documents require physical presence for applicant. Supervisors know their staff by heart and identification require only physical identification, expect for some big fishes who can make a call or drop an email for their requests to be completed.	User authenticate themselves with their login credentials, access and refresh tokens. User are also identified with their respective PKI. Digital sign, approval and some details are imbedded in QR code by every signer.	Implementation of multiple authentication (username with strong password and something you have such as OTP), Public Key Infrastructure and QR code to strengthen encryption and security.

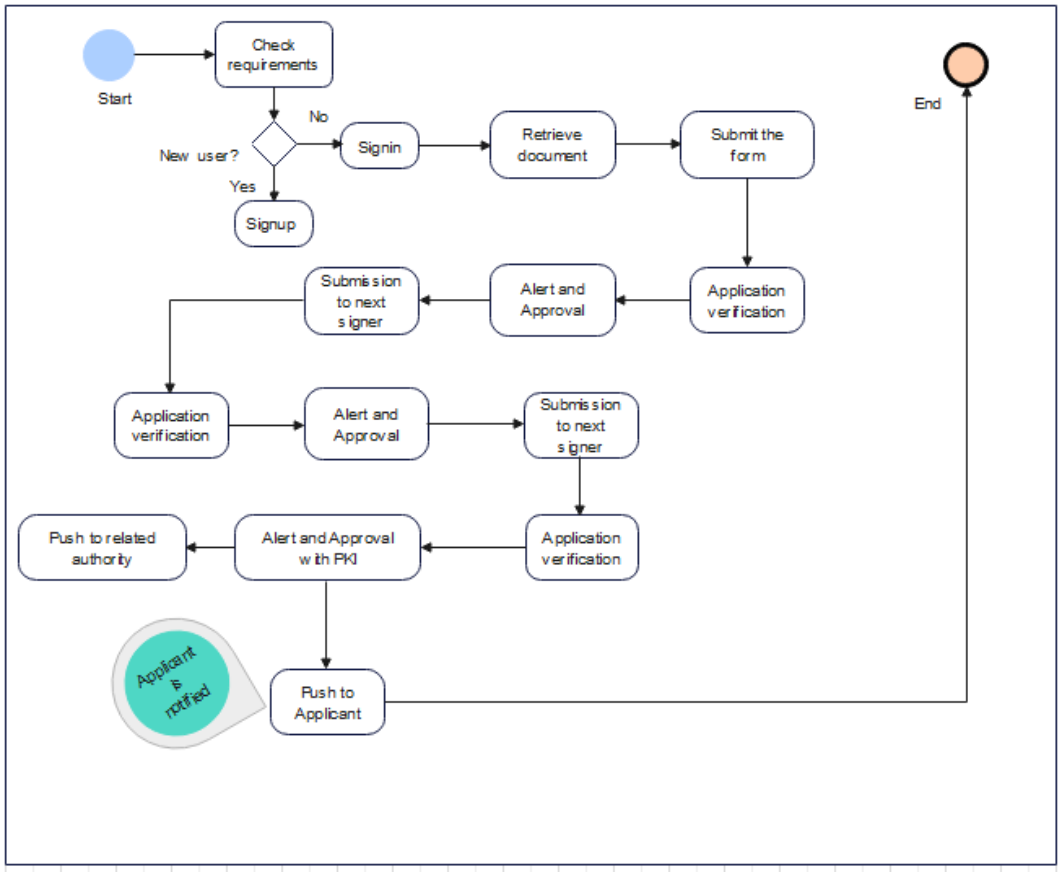


Figure 15: Proposed workflow for application and signing for official documents

5.3. Java Cryptography Architecture/Extension (JCA/JCE)

This model is firstly a java cryptography model provided to be a web-based services application which is fully compatible to runs on Linux Ubuntu 22.04 server as shown in the figure 9 with 18 Java Runtime Environment (JRE) and 18 Java Development Kit (JDK), [71]. The "Java Cryptography Extension (JCE)" provides a complete framework and implementations for cryptography encryption, key generation, and/or key agreement, Message Authentication Code (MAC) algorithms. Its support for encryption includes symmetric, asymmetric, block, as well as stream ciphers. Library used in this prototype were adopter to support functionalities such as sending and receive mails, language integration and execution into PostgreSQL.

Java Cryptography Architecture

Source: own drawing

Figure 16: The architecture of system prototype

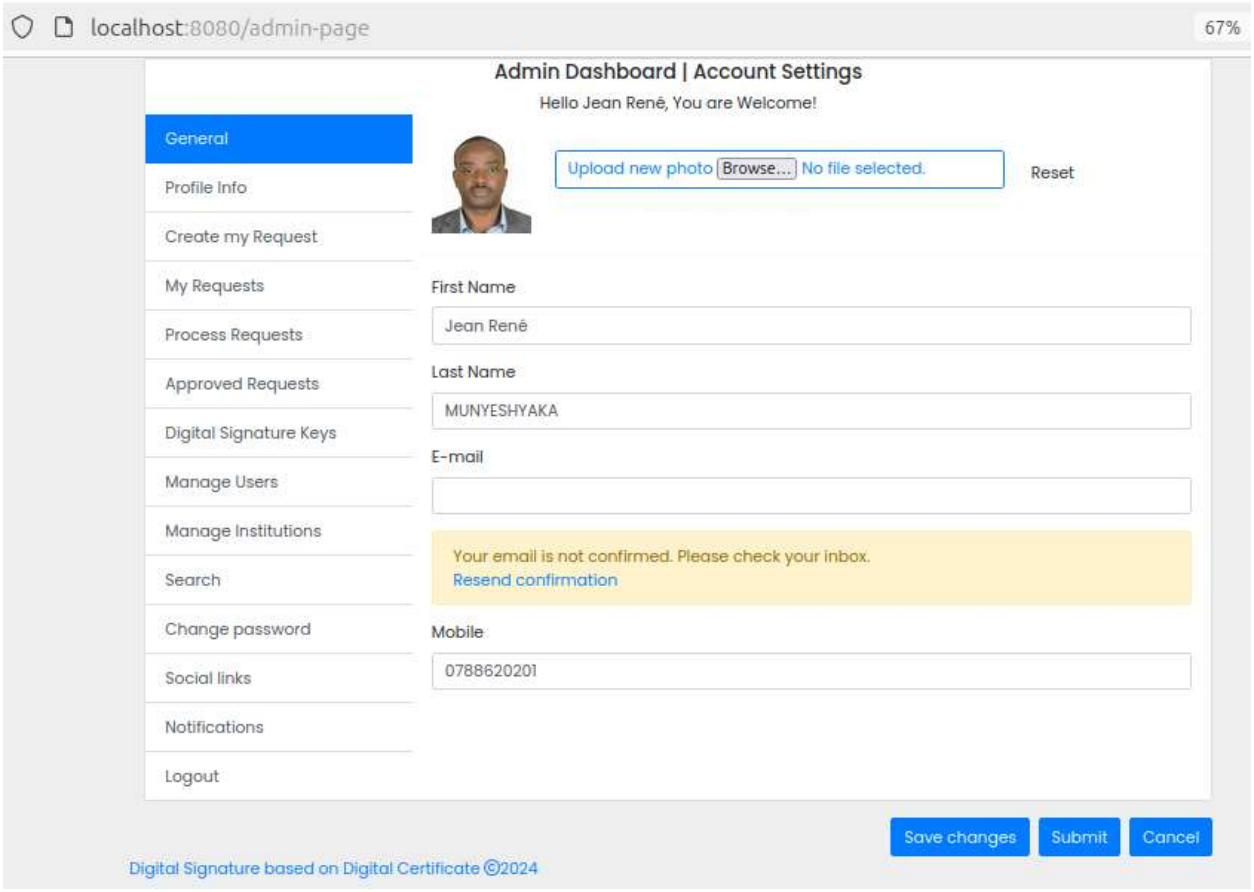
5.4. Components Design

Previously, in chapter 6 have been proposed 4 components: Multiple authentications, Request Submisstion, Requested Approval (with sign) Document Authentication Verification via QR scan. The Section 5.3.1 shows the system Design of web services. Section 5.3.2 covers the verification and validation process, in other term the correctness of the codes.

5.4.1. Web Service interface

A user can sign in or sign up to get the right to process a request. A request is verified, processed and signed by authorised users, generated into a printable document which can later be verified again for validity and authentication. Each operation is presented into a web file meaning a web service page [15].

Admin Dashboard:



Source: system screenshot

Figure 17: System interface for approval sign

The administrator has the full rights to use or features and options provided by the system.

Signatory Dashboard

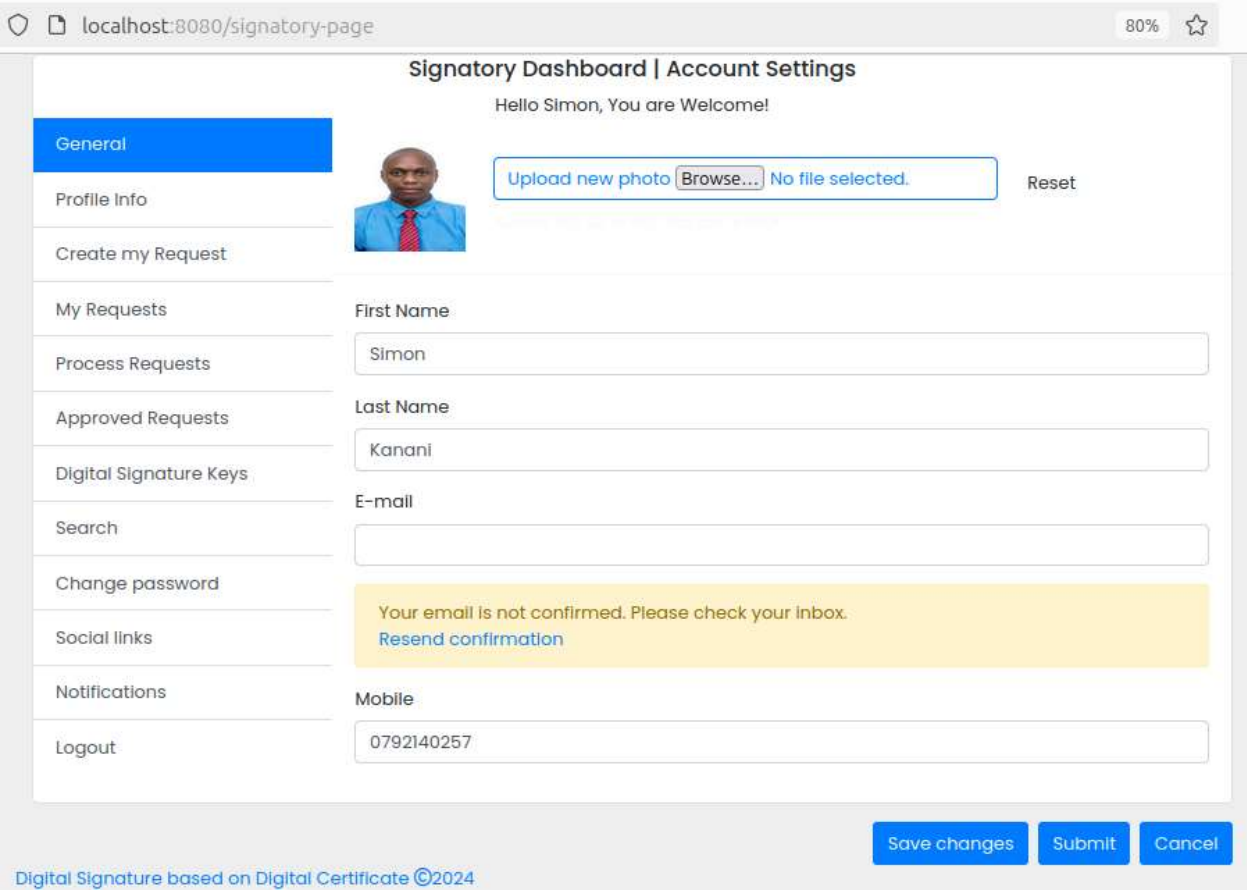


Figure 18: signatory dashboard with different features

The signatory has of rights of Administrator except the privileges to manage users and institution. Signer approves and signs or reject a request. The signer decides the next process for any request in her/his possession. Signatory has no right to sign for themselves.

User Request Dashboard

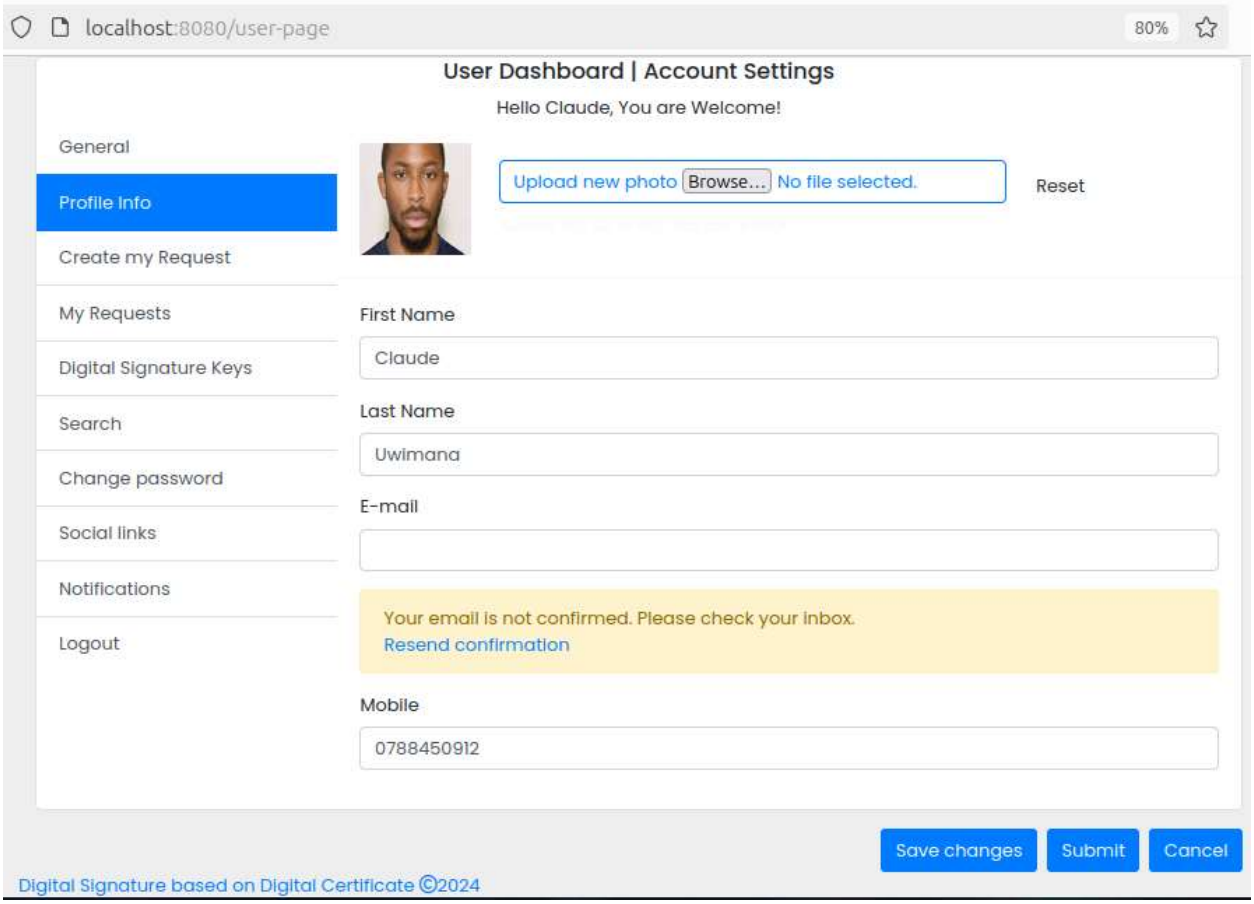
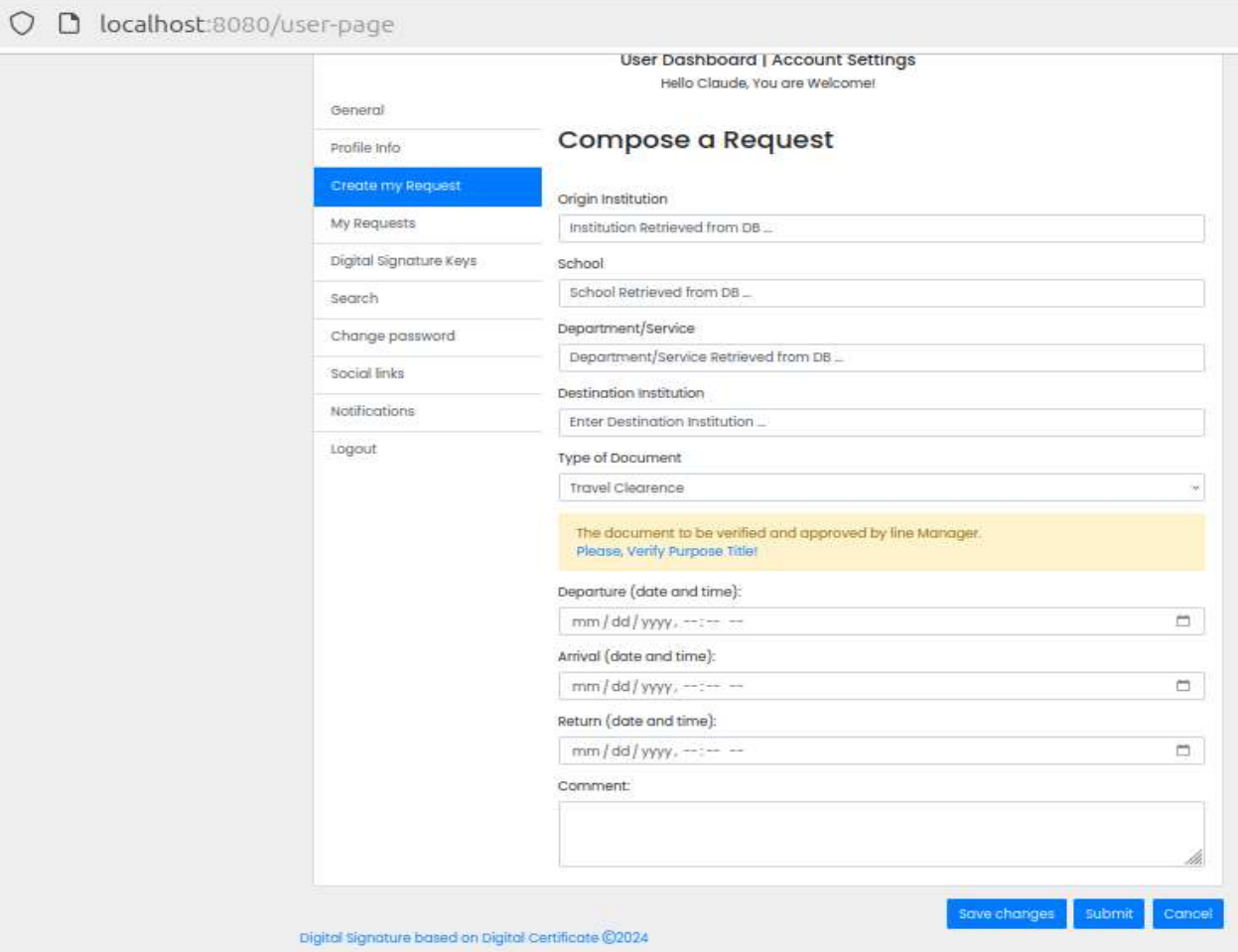


Figure 19: user profile account with different features

Users have the right to update their profiles, check account information, create and requests, Generate and save a PKI, verify a signature, search for information and documents, change password, configure social media and notifications. They have no right to sign documents.

Create a request

To send a request, a form is fulfilled and a file format is selected to serve as model to be signed upon approval. Related operation such as PostRequest provides a form by which to get records such as names of applicants and more other input details (see Figure 15) are fetched and recorded to the Database [72].



Source: system screenshot

Figure 20: Form to Request signed Document or permission

At Signatory side, GetApplicantList operation provides information like list of applicants to process application requests. Behind the presentation (information presented to the interface in front of user) there listeners on the buttons such that when a user make selection, a script syntax is executed to retrieved the data form the backend to the frontend interface [24].

PKI Generator and verification option

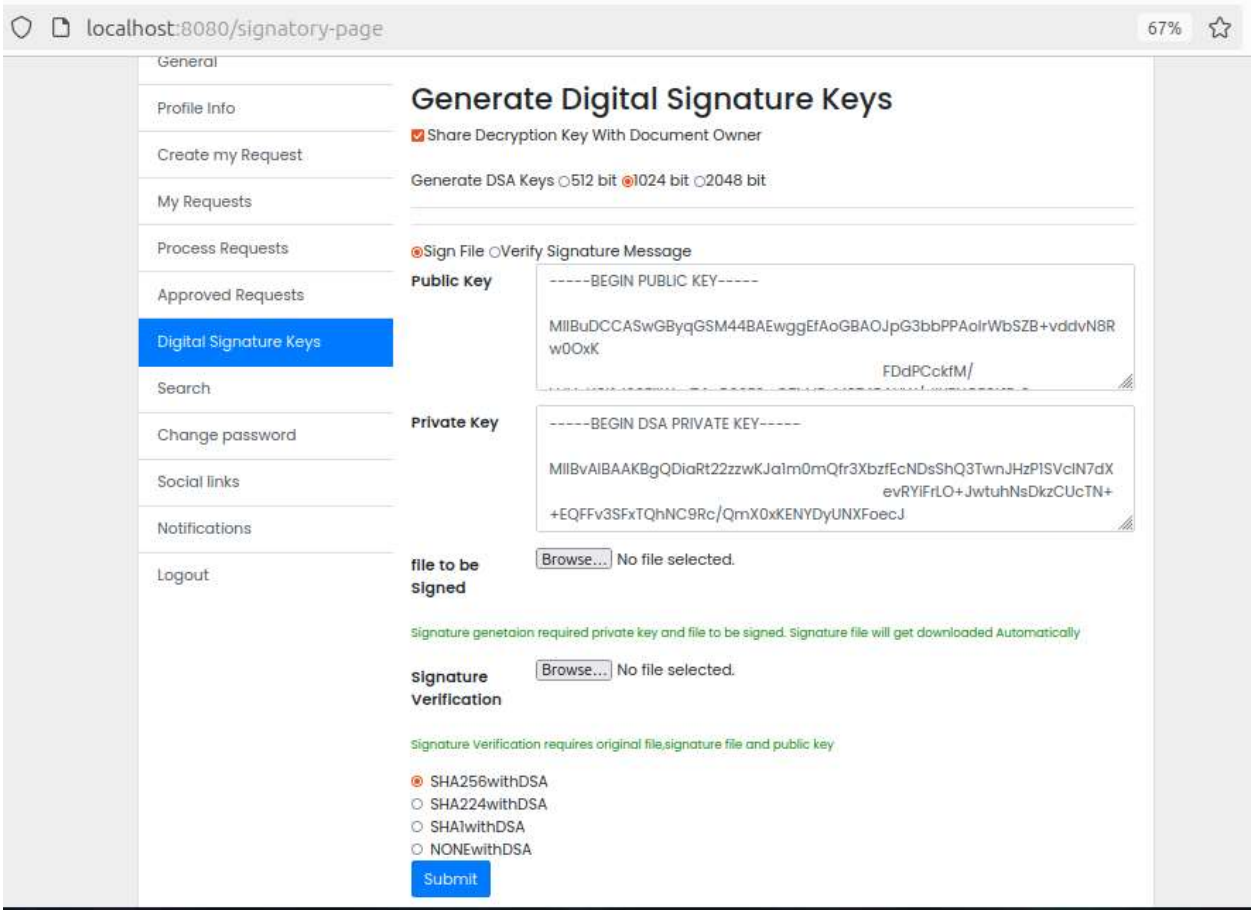


Figure 21: PKI Generator option

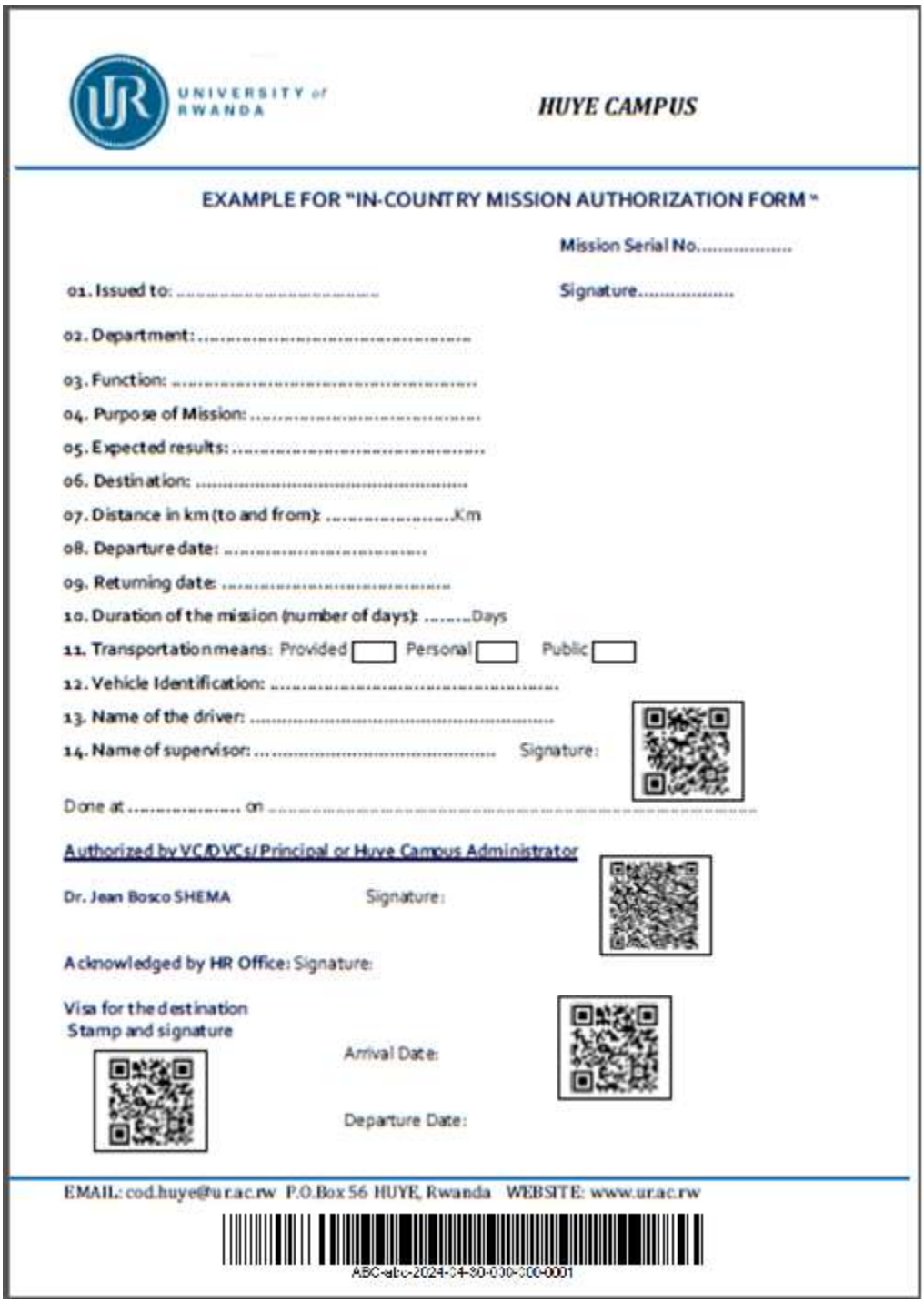
5.4.2. Operation Verification

In the above section was mentioned the verification function provided in the operation page to retrieval supported files and even for select list of user requests. In the same way, this method can be used to verify operation at level of primitive inputs types; just to refer basic data type in programming like integer, Boolean, composite (varBinary(max)) for image, etc [73]. In such case parameter (a letter) and value (number) can be user to verify the correctness of data. The system provides a way of comparing two documents online. Online tool to compare two documents from any device, with a modern browser like Chrome, Opera and Firefox. You must agree with terms of service and privacy policy by clicking to compare now.

Source: QR scan screenshot

Figure 22: QR Scanner interface

Signed document



UNIVERSITY of RWANDA

HUYE CAMPUS

EXAMPLE FOR "IN-COUNTRY MISSION AUTHORIZATION FORM "

Mission Serial No.....

01. Issued to: ..... Signature.....

02. Department: .....

03. Function: .....

04. Purpose of Mission: .....

05. Expected results: .....

06. Destination: .....

07. Distance in km (to and from): .....Km

08. Departure date: .....

09. Returning date: .....

10. Duration of the mission (number of days): .....Days

11. Transportation means: Provided ☐ Personal ☐ Public ☐

12. Vehicle Identification: .....

13. Name of the driver: .....

14. Name of supervisor: ..... Signature:

Done at ..... on .....

Authorized by VC/DVCs/Principal or Huye Campus Administrator

Dr. Jean Bosco SHEMA Signature:

Acknowledged by HR Office: Signature:

Visa for the destination
Stamp and signature

Arrival Date:

Departure Date:

EMAIL: cod.huye@ur.ac.rw P.O.Box 56 HUYE, Rwanda WEBSITE: www.ur.ac.rw

ABC-abc-2024-04-30-000-000-0001

Figure 23: Signed document

5.5. JMeter, Testing and Evaluation

JMeter testing was used to verify the load and performance of internal feature the system, from Application class. In the presented Response Times Over Time figure 18 we set up a test plan with sample population of 50 users: an input from the method SignNewRequest, an expected, and a current result after execution. To show the of every parameter in the program, break points are defined [18].

JMeter elements such as Thread group were used to simulate real users. A sample population of 50 were used in this testing. Thread group: It is a set of threads and each thread represents one user behand the application under test.

Basically, each thread simulates a real user request to the server, and controlling a thread group allows you to set the number of threads for each group. For example, if we have set the number of threads to 200 and JMeter created and simulates 200 user requests to the server under test.

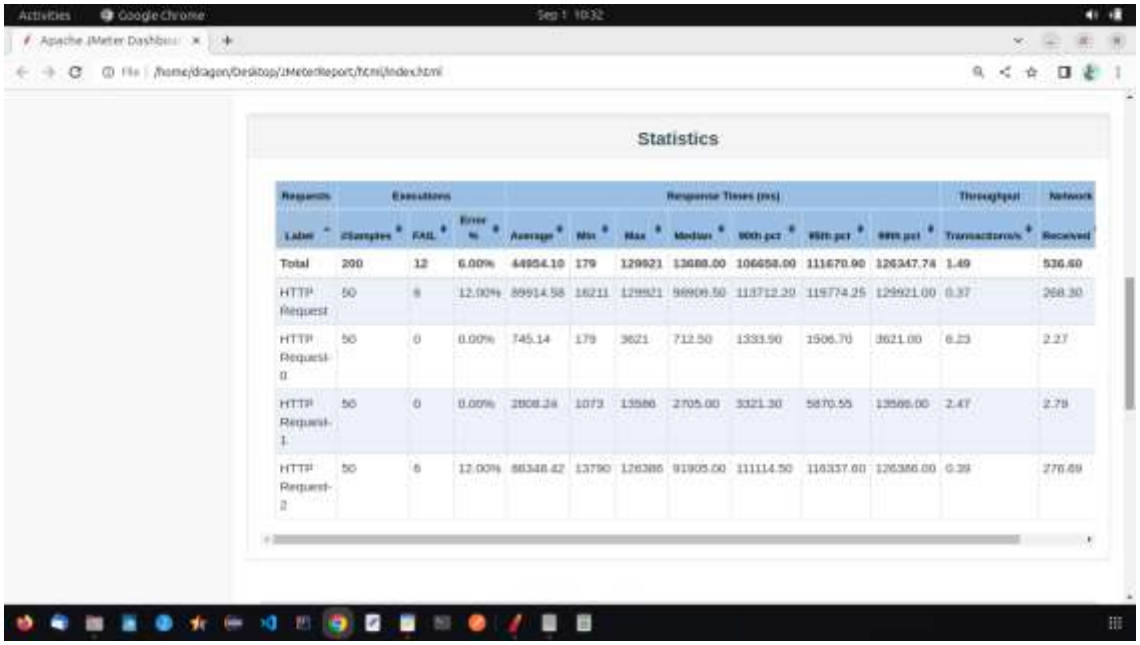


Figure 24: statistics table

A Statistics table providing in one table a summary of all metrics per transaction including 3 configurable percentiles.

Response times Percentiles Over Time which include successful responses only:

Figure 25: Response times Percentiles Over Time

It was found that the 50th percentile (median) of a response time is 500ms that means that 50% of my transactions are either as fast or faster than 500ms

Active Threads Over Time:

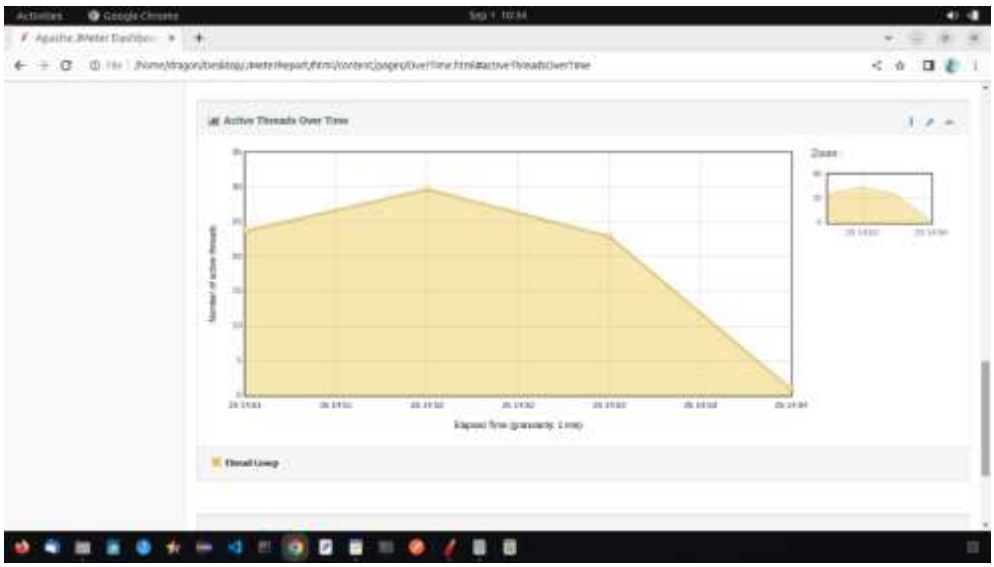


Figure 26: Active Threads Over Time

After 1minute, active requests tend to zero.

Response Time Overview which excludes Transaction Controller Sample Results:

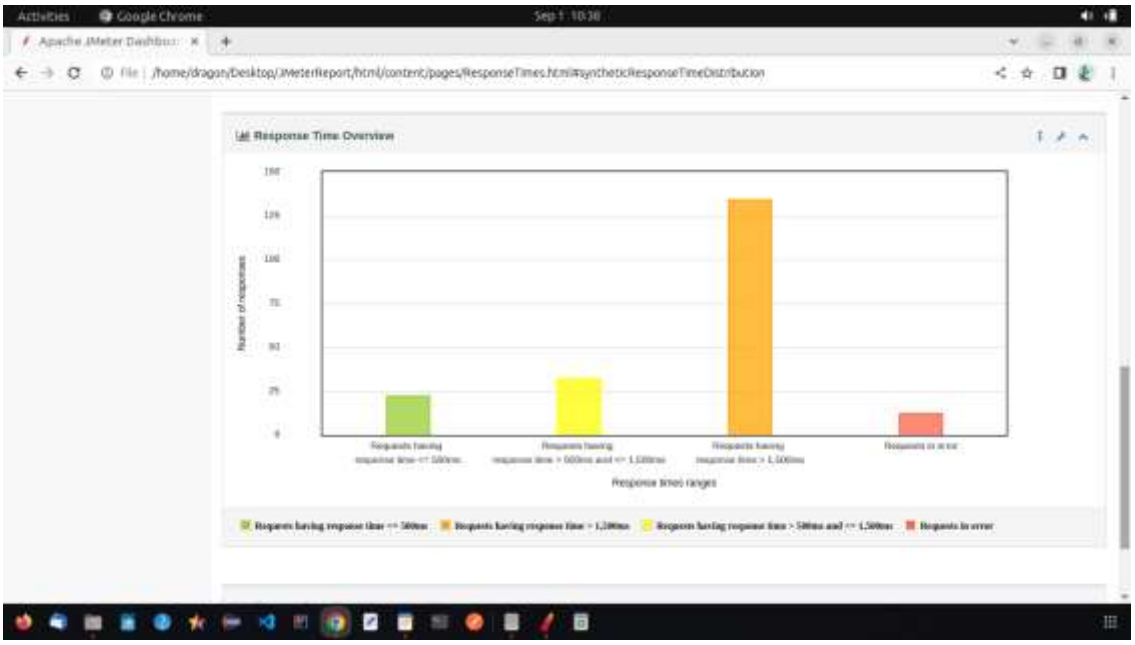


Figure 27: Response Time Overview which excludes Transaction Controller Sample Results for each category in milliseconds.

Overview between requests having response time which is less than 500ms, requests having response time which is greater than 500ms, requests having response time which is greater than 1,500ms and requests in error.

5.6.Database Modeling

Database Modeling also called Data Structuring represents the nature of data, and the business logic to control the data. It has the role to organize the database itself. In this way, the structures of data here above discussed, are explicitly determines by the data model. Data model helps to communicate between business people who require the computer system, and the technological people, who can fulfil their requirements.

The Digital Signature based on Digital Certificate facilitate the work of administrator to manage and assign different signatories to manage applicants' requests, sign and approve requested documents on demand.

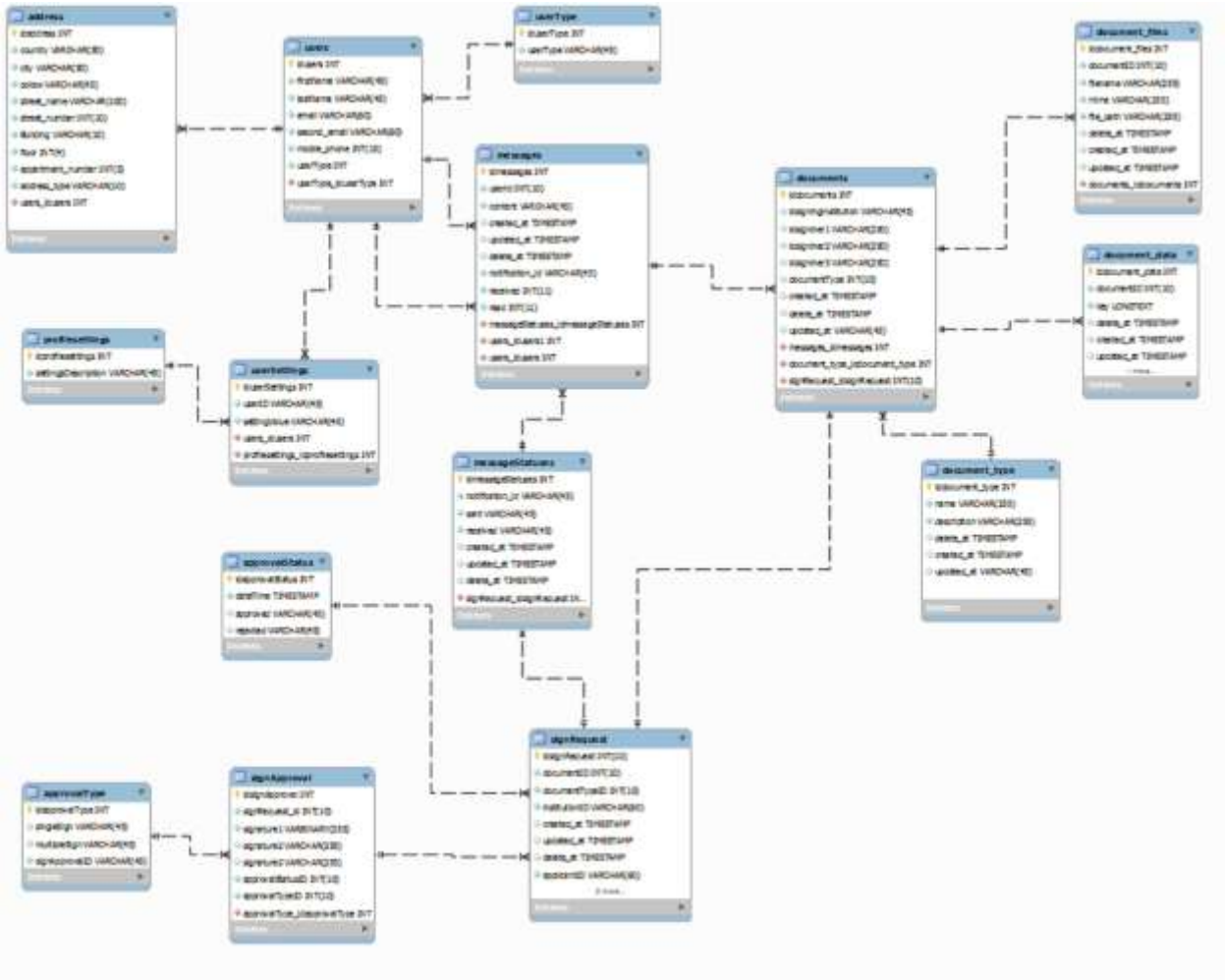


Figure 28: Database Modeling

Source: own design

5.7.Prototype Evaluation

The whole process from web service, the request formulated, the document to be signed, the QR, public keys, signers and information transmitted are assimilated and accessible in the form of linked data.

The applicant cannot accidentally send a request nor a sign can't sign through a simplified process. To be authorized each request is proven with a hash function and a QR code are generated after completing a form. The stepped can be completed only by an authorized user through an authentication mechanism. Thus, Digital Signature based on Digital Certificate is attributable as demonstrated during the JMeter testing.

At a certain extent, none trusted databases have the ability to store, use the data and verify the existing document. Thus, the sign document, the digital signature and associated certificate are portable.

The approval and sign can be revoked and revisable with certain number of conditions and a notification alert is sent across the system to all concerned actors, after what a new decision is communicated and a document is generated for that operation.

Anyone with the public key can generate a forgery document. Yet the are other means to publish and verify results: document number produced from the system, date and time must coincide with the recorded operation and communicated to all actors. If not, issue of forgery is detected and communicated across the system users.

None authentic documents are easily tracked and have no possible record in the main database. Digital signatures are legal signatures because they follow a chain of proof, we have proven the mean to test the validity. And when generated, concerned actors are all informed for any change. In this way, the Digital Signature based on Digital Certificate is Linkable, Attributable, Portable, Revisable, and Verifiable.

Chapter 6 Conclusion and Recommendation

1.1. Conclusion

This research was being conducted to provide requirement analysis of Digital Signature based on Digital Certificate. In a signing system, some messages are only received by authorized users in a form of encrypted formats. But other messages/documents contain parts of encrypted messages with a plain text revealed to public as proof of originality. The main target was to design a trustworthy model that allows users to securely exchange digitally stamped documents ensuring the none repudiation, validity and verification, performance and sympathy in one system. The above mission was accomplished through the sub-objectives that have a specific question to be solved.

Sub-objective1: Understand the existing workflow, identifying the gap for improving the Digital Signature based on Digital Certificate and propose solutions to overcome the existing problems.

The first sub-objective was accomplished via data collection and collaboration with peers, to get clear understanding of the situation. The addressed question was: "*Do the proposed solutions measure up to the identify gap and problematic?*" Most interviewed participants helped to dash a light on the existing system and enabling us to accumulate crucial information. The improvement was made from user requirements and system requirements; proposing a new workflow model. By these, we get to know what are the users' wants and how the system can efficiently and effectively address them.

Sub-objective2: Define the required systems and inter-connection to facilitate flexible deliverance and facilitate management of services.

The purpose of this sub-objective was to review the existing models and technologies behind the current documents' signing systems, with the aim to improve and automate the services. The address question was: "*Do defined functional and non-functional requirements matching the users' needs?*". Interviews, systematic analysis, experience and observation from the peer collaborators were keys to accomplish this sub-objective. The challenge of long waiting for a line

manager's signature, the risk to your document lost or damaged, the obligation to hand it from one place to another seeking for validation, the challenge to get the processing status while waiting for response. To solve this issue, the system nullified the use of printable documents, by exchanging privately digitally documents from the applicants to the signatories; and from signatories to owner requesting any documents. Notifications messages are exchanged to improve communication end help to get the processing status in real-time.

Sub-objective3: Design the Digital Signature based on Digital Certificate system with specified requirements.

The sub-objective was addressed from the security requirements, data privacy and need to comply to the latest needs in cryptography encryption. The research question to be addressed was: "*Can the provided prototype of digital signature be attributed, verifiable, linkable, reversible, revocable, potable and computable?*" The first challenging obstacle was documents' server and how to make it accessible to public allowing only certified systems to access it on time and in times. To address this issue, a self-signed certificates were generated and all involved signing institutional interface should be hosted locally in the same data center or shared server as the documents sever.

The second was the documents to be signed themselves. Parts of the documents (not the whole document must be encrypted = semi encrypted documents). By this only fully authorized users can read the whole documents, as some hidden important messages are encrypted using QR code, HASH encryption and PKI certificates.

Sub-objective4: Validate that changes the new work process for signing with digital signature and certificate

The validation analysis was conducted to check whether the presented workflow satisfy the elaborated requirements and if identified challenges were all removed. The research question to be addressed was: "*Is the system load, performance and security up to the normal?*" The system for Digital Signature based on Digital Certificates, solved the long waiting time, helping the applicants to composed a request for documents, signatory to approve and sign, push notification, transmit the documents to the responsible people, signing and encrypting parties of documents, using the latest encryption methods in cryptography and programming.

1.2.Recommendations

Sensitization is one of the recommendations to be addressed in the future. In Data Privacy, exposing a handwriting signature on lists, signed documents, and everywhere, … is also a data leak. The signer anonymity is also recommended and systems have full ability to control the process enabling users the ability to verify and validate or revise the process in case of emergency need. To understand these, people must be trained, educated on the matter of standards and data privacy.

In the coming days, semi-encrypted messages and documents will provide a new mean to share information and protect data. Systems like Hospital Management Systems, Students Management System, governments and their institutions, will see the new emerging partially encrypted documents as a necessity in their working environment.

The last recommendation would be simply to stay up to date. Technologies get old, security deplete very quickly and attackers are constantly innovating new bad scenarios. To harden the encryption as much as possible, but also implement the most secure encryption algorithm can help secure many systems in the current world.

List of References

[1] N. S. Ramadani, V. Misimi, E. Ramadani, and F. Idrizi, “The Role and the Impact of Digital Certificate and Digital Signature in Improving Security During Data Transmission,” vol. 2, no. 1, pp. 116–120, 2017.

[2] “PUBLIC-KEY CRYPTOGRAPHY SECURITY-BASED ANALYSIS OF THE UNDERLYING INTRACTABLE PROBLEMS by HUSAIN H . AL KHULAIF BS ., Colorado State University , 2011 A thesis submitted to the Faculty of the Graduate School of the University of Colorado in partial fulfil,” 2013.

[3] D. Sharma, “A Review of QR code Structure for Encryption and Decryption Process,” *Int. J. Innov. Sci. Res. Technol.*, vol. 2, no. 2, pp. 13–18, 2017, [Online]. Available: www.ijisrt.com

[4] D. S. S. Core and D. S. S. Demonstrations, “Digital Signature Service Table of Contents,” pp. 1–289.

[5] E. W. Patton *et al.*, “SemantEco: A semantically powered modular architecture for integrating distributed environmental and ecological data,” *Futur. Gener. Comput. Syst.*, vol. 36, pp. 430–440, 2014, doi: 10.1016/j.future.2013.09.017.

[6] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, “Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal,” *J. Cybersecurity Priv.*, vol. 1, no. 2, pp. 219–238, 2021, doi: 10.3390/jcp1020012.

[7] I.G.U.Dilmini Rathnayaka, “A Review of Software Development Methodologies in Software Engineering,” no. 4, pp. 1844–1853, 2020.

[8] N. S. Egoshin, A. A. Konev, and A. A. Shelupanov, “A model of threats to the confidentiality of information processed in cyberspace based on the information flows model,” *Symmetry (Basel).*, vol. 12, no. 11, pp. 1–18, 2020, doi: 10.3390/sym12111840.

[9] I. Standard, “INTERNATIONAL STANDARD ISO / IEC techniques — Digital signatures,” vol. 2006, 2006.

[10] V. Singh and S. K. Pandey, “Revisiting Cloud Security Threats: Repudiation Attack,” *Int. J. Recent Technol. Eng.*, vol. 8, no. 5, pp. 1790–1798, 2020, doi: 10.35940/ijrte.e6377.018520.

[11] O. Sacco, J. G. Breslin, and S. Decker, “Fine-grained trust assertions for privacy management in the social semantic web,” *Proc. - 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2013*, pp. 218–225, 2013, doi: 10.1109/TrustCom.2013.30.

[12] J. P. McCusker, T. Lebo, A. Graves, D. Difranzo, P. Pinheiro, and D. L. McGuinness, “Functional requirements for information resource provenance on the web,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7525 LNCS, no. May 2016, pp. 52–66, 2012, doi: 10.1007/978-3-642-34222-6_5.

[13] A. Kasten and A. Scherp, “Towards a configurable framework for iterative signing of distributed graph data,” *CEUR Workshop Proc.*, vol. 1121, 2014.

[14] M. K. Prathiba and L. Basavaraj, “Online Handwritten Signature Verification System Based OnBayes’ Theorem,” no. September, pp. 1025–1030, 2017, doi: 10.21647/icctest/2017/49104.

[15] J. M. Tirado, O. Serban, Q. Guo, and E. Yoneki, “Web Data Knowledge Extraction,” no. 881, 2016, [Online]. Available: http://arxiv.org/abs/1603.07534

[16] T. Kuhn and M. Dumontier, “Trusty URIs: Verifiable, immutable, and permanent digital artifacts for linked data,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8465 LNCS, pp. 395–410, 2014, doi: 10.1007/978-3-319-07443-6_27.

[17] J. Davis and K. Daniels, *Effective DevOps*. 2016. [Online]. Available: https://www.amazon.com/-/es/Jennifer-Davis/dp/1491926309

[18] D. Zima, “Modern Methods of Software Development,” *Task Q.*, vol. 19, no. 4, pp. 481–493, 2015.

[19] A. Mateen, M. Azeem, and M. Shafiq, “AZ Model for Software Development,” *Int. J. Comput. Appl.*, vol. 151, no. 6, pp. 33–36, 2016, doi: 10.5120/ijca2016911701.

[20] N. Mohammed, A. Munassar, and A. Govardhan, “A Comparison Between Five Models Of Software Engineering,” *Int. J. Comput. Sci. Issues*, vol. 7, no. 5, pp. 94–101, 2010.

[21] L. Notes, “Lecture Notes for Data Structures and Algorithms,” no. March, 2019.

[22] C. S. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, *Introduction to Algrithms, 3rd Edition (The MIT Press)*. 2009.

[23] M. W. Harkins, *Managing Risk and Information Security*. 2016. doi: 10.1007/978-1-4842-1455-8.

[24] D. J. Eck and W. S. Colleges, “Introduction to Programming Using Java,” *Environments*, vol. 2006, no. December 2006, 2010.

[25] S. Krishnamurthi and K. Fisler, “Programming Paradigms and Beyond,” *Cambridge Handb. Comput. Educ. Res.*, pp. 377–413, 2019, doi: 10.1017/9781108654555.014.

[26] E. Deelman *et al.*, “Pegasus: A framework for mapping complex scientific workflows onto distributed systems,” *Sci. Program.*, vol. 13, no. 3, pp. 219–237, 2005, doi: 10.1155/2005/128026.

[27] C. S. Wasson, *System analysis, design, and development: Concepts, principles, and practices*. 2006. doi: 10.1002/0471728241.

[28] J. Grady, *Design modeling and simulation*. 2010. doi: 10.1201/9781439819623-c17.

[29] J. Niederst *et al.*, *Learning Web Design, Fourth Edition*. 2012. [Online]. Available: http://www.winnystudio.com/kmcweb/lectures/LearningWebDesig4thEdition_01.pdf

[30] J. Pieprzyk, H. Wang, and C. Xing, “Multiple-Time Signature Schemes,” pp. 88–100, 2004.

[31] S. Gaw and E. W. Felten, “Password management strategies for online accounts,” *ACM Int. Conf. Proceeding Ser.*, vol. 149, pp. 44–55, 2006, doi: 10.1145/1143120.1143127.

[32] D. Heng and Y. W. Tok, “Fintech: Financial Inclusion or Exclusion?,” *IMF Work. Pap.*, vol. 2022, no. 080, p. 1, 2022, doi: 10.5089/9798400208645.001.

[33] O. of justice programs US Department of justice, “The Fingerprint Sourcebook: U.S.

Department of Justice," *U.S. Dep. Justice*, p. 422, 2012.

[34] C. Tech, P. Grubbs, P. Rösler, and F. A. U. Erlangen-nürnberg, "Interoperability in End-to-End Encrypted Messaging Julia Len," 2024.

[35] F. Martin, "SSL Certificates HOWTO," *Linux Doc. Proj.*, p. 29, 2002.

[36] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X. 509 public key infrastructure certificate and CRL profile," *Internet Soc.*, vol. 54, no. RFC 3280, pp. 1–129, 2002, [Online]. Available: http://www.ietf.org/rfc/rfc3280.txt

[37] L. E. Lwakatare, *DevOps adoption and implementation in software development practice : concept, practices, benefits and challenges*. 2017.

[38] ISO, "INTERNATIONAL STANDARD ISO / IEC / IEEE Systems and software engineering — iTeh STANDARD PREVIEW iTeh STANDARD PREVIEW," vol. 2015, 2015.

[39] R. S, "System Analysis and Design," *J. Inf. Technol. Softw. Eng.*, vol. 02, no. 05, pp. 1–12, 2012, doi: 10.4172/2165-7866.s8-e001.

[40] S. White and D. Miers, *BPMN Modeling and Reference Guide: Understanding and Using BPMN*. 2008.

[41] "WorkflowManagementJablonskiBussler.pdf."

[42] M. Devillers, "Business Process Modeling as a means to bridge The Business-IT Divide," vol. Master's T, no. 156, p. 66, 2011.

[43] W. Van Der Aalst and K. M. van Hee, "Workflow Management: Models, Methods, and Systems (Google eBook)," vol. 52, no. 2001, p. 368, 2004, [Online]. Available: http://books.google.com/books?id=O1xW1_Za-I0C&pgis=1

[44] S. Islam, "Software Development Risk Management Model- a goal-driven approach Shareeful Islam," *Softw. Syst. Eng. Inst. Comput. Sci. Tech. Univ. Munich*, 2011.

[45] I. Sommerville, *Software Engineering (9th ed.; Boston, Ed.). Massachusetts: Pearson*

Education. 2011.

[46] J. S. Valacich and J. F. George, *Modern Systems Analysis and Design Ninth Edition*. 2021.

[47] J. E. Gary B.Shelly dan Harry J.Rosenblatt ; Ormrod, "Systems Analysis and Design Ninth Edition," *Pract. Res. - Plan. Des.*, p. 67, 2010.

[48] R. Kumar and A. Perti, "Security issues with self-signed SSL certificates," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 7, pp. 149–153, 2019.

[49] J. Katz, *Cryptography*. 2004. doi: 10.1201/9781420057133.

[50] H. Naseer, M. N. Mumtaz Bhutta, and M. A. Alojail, "A Key Transport Protocol for Advance Metering Infrastructure (AMI) Based on Public Key Cryptography," *1st Annu. Int. Conf. Cyber Warf. Secur. ICCWS 2020 - Proc.*, 2020, doi: 10.1109/ICCWS48432.2020.9292385.

[51] J. Clark and P. C. Van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements," *Proc. - IEEE Symp. Secur. Priv.*, pp. 511–525, 2013, doi: 10.1109/SP.2013.41.

[52] M. Souppaya, W. Haag, P. Turner, and W. C. Barker, "Securing web transactions," 2018, [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/tls-serv-cert-mgt-nist-sp1800-16b-draft.pdf

[53] W. Schroeder, "Certified Pre-Owned Abusing Active Directory Certificate Services".

[54] D. Adrian *et al.*, "Imperfect forward secrecy: How diffie-Hellman fails in practice," *Commun. ACM*, vol. 62, no. 1, pp. 106–114, 2019, doi: 10.1145/3292035.

[55] L. Tan, X. Shang, L. Zou, H. Yang, Y. Wen, and Z. Liu, "Multi-party co-signature scheme based on SM2," *PLoS One*, vol. 18, no. 2 February, pp. 1–24, 2023, doi: 10.1371/journal.pone.0268245.

[56] D. L. Mcguinness, D. Adviser, J. Hendler, P. Fox, and M. Dumontier, "WEBSIG : A DIGITAL SIGNATURE FRAMEWORK FOR," vol. 2015, no. July, 2015.

[57] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, “Design and Implementation of Rivest Shamir Adleman’s (RSA) Cryptography Algorithm in Text File Data Security,” *J. Phys. Conf. Ser.*, vol. 1641, no. 1, 2020, doi: 10.1088/1742-6596/1641/1/012042.

[58] N. I. Chesnokov, D. A. Korochentsev, L. V. Cherckesova, O. A. Safaryan, V. E. Chumakov, and I. A. Pilipenko, “Software Development of Electronic Digital Signature Generation at Institution Electronic Document Circulation,” *2020 IEEE East-West Des. Test Symp. EWDTS 2020 - Proc.*, 2020, doi: 10.1109/EWDTS50664.2020.9224967.

[59] W. Jansen, “NIST Internal Report - 7564 Directions in Security Metrics Research,” *Nist*, p. 26, 2009, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.158.3401

[60] N. P. Hegde and V. V. D. Shastrimath, “Digital Signature Algorithm: A Hybrid Approach,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 3, pp. 656–660, 2023, doi: 10.14569/IJACSA.2023.0140376.

[61] Patel, “Elliptic Curve Digital Signature Algorithm,” pp. 9–25, 2019.

[62] E. Transactions and D. Agency, “Establishing a Certification Authority (CA)”.

[63] U. Dod, P. Key, R. G. Installroot, U. G. Contact, and D. O. D. P. K. E. Team, “InstallRoot 5 . 6 User Guide,” no. October, 2023.

[64] Rr. priyadharshini, “A Comparative Study on the Performance and the Security of RSA and ECC Algorithm,” *Spec. Issue Publ. Int. Jnl. Adv. Netw. Appl.*, no. March, pp. 168–171, 2015, [Online]. Available: https://www.researchgate.net/publication/344788441

[65] S. Levy, “Performance and Security of ECDSA,” pp. 1–4, 2015, [Online]. Available: http://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Levy.pdf

[66] H. Kufner and M. Vogt, “Betreuung Von Drogenabhangigen in Bauerlichen Familien,” *Sucht*, vol. 41, no. 2, pp. 98–99, 1995.

[67] I. Noorwali, “Scholarship @ Western A Requirements Measurement Program for Systems

Engineering Projects : Metrics , Indicators , Models , and Tools for Internal Stakeholders," 2020.

[68] G. Muller, "System Architecting," p. 234, 2018.

[69] "December 21, 2023 Securing the Public Key Infrastructure Workshop Report," pp. 1–20, 2023.

[70] H. Elbehiery, "Enhancement of QR code Student's Attendance Management System using GPS," *IOSR J. Comput. Eng.*, vol. 21, no. 4, pp. 18–30, 2019, doi: 10.9790/0661-2104011830.

[71] S. L. Nita and M. I. Mihailescu, "Java Cryptography Architecture," *Cryptogr. Cryptanalysis Java*, pp. 29–46, 2022, doi: 10.1007/978-1-4842-8105-5_4.

[72] S. Mason, *Electronic Signatures in Law*. 2016. doi: 10.14296/1116.9781911507017.

[73] L. Lemay and C. L. Perkins, *Teach Yourself Java in 21 Days*. 2010. [Online]. Available: yotube.com