Strathmore UNIVERSITY

SU+ @ Strathmore University Library

Electronic Theses and Dissertations

2021

A Prototype to identify fraudulent sim card registration using Public Key infrastructure verification approach.

Wanja, Gate Maureen
School of Computing and Engineering Sciences
Strathmore University

Recommended Citation

Wanja, G. M. (2021). *A Prototype to identify fraudulent sim card registration using Public Key infrastructure verification approach* [Thesis, Strathmore University]. http://hdl.handle.net/11071/12915

Follow this and additional works at: http://hdl.handle.net/11071/12915

This work is availed for free and open access by Strathmore University Library.
It has been accepted for digital distribution by an authorized administrator of SU+ @Strathmore University.
For more information, please contact library@strathmore.edu

A Prototype to Identify Fraudulent Sim Card Registration Using Public Key Infrastructure Verification Approach

Gate Maureen Wanja

A Thesis Submitted to the School of Computing and Engineering in Partial Fulfilment for the Award of the Degree in Master of Science in Information System Security.

November 2021

Declaration

I declare that this work has not been submitted previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the thesis itself.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University.

Gate Maureen Wanja

M.Gate

19th Nov 2021.

Approval

The thesis of Gate Maureen Wanja was reviewed and approved by the following:

Dr. Vincent Omwenga

Research Director,

School of Computing and Engineering Sciences,

Strathmore university

Dr. Julius Buritime

Dean, School of Computing and Engineering Sciences

Strathmore university

Dr. Bernard Shibwabo,

Director of Graduate Studies,

Strathmore University

Abstract

Identifying a legitimate subscriber is important for the Mobile Network Operators during the SIM card registration and verification process. Over the years, the use of Mobile devices has grown steadily, increasing the numbers of subscribers to the different MNOS significantly. The MNOs are the owners of the SIM cards which they issue to their subscribers. The SIM card stores critical information belonging to the user, and information such as the IMSI number is unique to identifying the module. Different governments have approached the issue of SIM card registration differently. In some countries, SIM card registration is mandatory, and there is a requirement to provide identification during the registration process, while this is not a requirement for other countries. The Mobile Network Operators must have the Know Your Customer policies to validate the users as they activate the SIM modules. The research objective was to design, develop and test a prototype used by the mobile network operators and the users for self-registration of SIM cards. This objective was achieved by creating a verification platform for the users to activate their SIM modules after purchasing them from MNOs. Activating the SIM would be done after a user has been issued with a signed public key by a certificate Authority. The prototype used the functionalities of the PKI that ensured the integrity and authentication of the legitimate users. Unit and usability tests were conducted to validate if the prototype achieved its main objective. Different users involved in the data collection phase gave their recommendations, which formed the requirements for developing the prototype and furthering this research work. Each of the specific objectives was also discussed to show how each was achieved.

Table of Content

Declaration ii

Approval iii

Abstract iv

Table of Content v

Table of Figures ix

List of Tables x

List of Abbreviations/Acronyms xi

Definition of Terms xii

Acknowledgment xiii

Chapter One: Introduction 1

1.1. Background to the study 1

1.1.2. Fraudulent Simcard Registration 2

1.1.3. Public-key Infrastructure 3

1.2. Problem Statement 4

1.3. Objective 4

1.3.1. General Objective 4

1.3.2. Specific Objectives 5

1.4. Research Questions 5

1.5. Justification 5

1.6. Scope and limitation 5

Chapter 2: Literature Review 6

2.1. Introduction 6

2.2. SIM card structure overview 6

2.3. SIM card registration 7
2.4. Fraudulent SIM card registration cases 8
2.5.Approaches of identifying SIM card Owners 10
2.5.1. SIM card identity validation approaches 10
2.6. Methods of implementing Owner identity. 10
2.6.1. Coupling a SIM Module to a wireless Communicating device 10
2.6.2. Electronic Know Your Customer (eKYC) 11
2.6.3. Use of radio communication network to detect a fraudulent subscriber module 11
2.7. Public Key Infrastructure 12
2.7.1. PKI authentication on the internet 15
The SSL handshake 15
2.8 Public Key Algorithms 15
2.8.1 RSA Algorithm 15
2.8.2. Elliptic Curve Digital Signature Algorithm 16
ECDSA Signing Algorithm 17
Chapter 3: Research Methodology 18
3.1 Introduction 18
3.2 Research Approach for Objectives 1 and 2 18
3.3. Research Approach for Objectives 3 and 4 18
3.3.1. Requirements gathering and planning. 19
3.3.2 Design 19
Location and Target Population 20
Sampling Techniques and sample size 20
Data Collection 20
Data Analysis 20
3.2.2.2.System Design 21

3.2.2. System Development....21
3.2.3. Testing and Deployment....21
3.4. Validation....22
3.5. Research quality aspects....22
3.6. Ethical Considerations and Approval....22
Chapter 4: System Design and Architecture....23
4.1. Introduction....23
4.2 System analysis....23
4.2.1. Requirements gathering....23
4.2.2. Research Findings....23
4.3. System Requirements....24
4.3.1. Functional Requirements....24
4.3.2. Non-Functional Requirements....25
4.4. System architecture....25
4.4.1 Key Management....26
4.5. System diagrams....27
4.5.1.Use case Modelling....27
4.5.2. The System sequence diagram....28
4.5.3. Entity-relationship Diagram....29
4.5.4. Wireframe diagrams....29
Chapter 5:System Implementation and Testing....31
5.1 Introduction....31
5.2 System Implementation....31
5.2.1 Development Environment....31
5.2.2. Hardware requirements....31
5.2.3 System Functionality....31

5.3 Prototype testing 36
5.3.1. Unit testing 36
5.3.2 Integration testing 37
5.4 System Validation 37
Chapter 6 :Discussion 38
6.1 Introduction 38
6.2.Analysis of SIM card registration in Kenya. 38
6.3.Review of the approaches used to identify the legitimate SIM card owner during SIM card registration. 38
6.4.Designing, developing, and testing of the prototype 39
Chapter 7: Conclusion and Recommendation 40
7.1 conclusion 40
7.2 Recommendations 40
7.3 Future works 40
References 41
Appendices 46
Appendix 1: Survey questions 46
Appendix 2: Turn It In Report 48
Appendix 3: Ethical review Certificate 49

Table of Figures

Figure 2. 1 Asymmetric Encryption 13

Figure 2. 2 Public Key Infrastructure 13

Figure 3. 1 Agile Lifecycle 15

Figure 4. 1 Research Findings Pie Chart. 20

Figure 4. 2 System Architecture 22

Figure 4. 3 System Administrator Use Case 23

Figure 4. 4 The System Sequence Diagram 25

Figure 4. 5 Database Schema 26

Figure 4. 6 System Administrator Login/Logout 26

Figure 4. 7 User validation on NIIMS 27

Figure 4. 8 User registration process 27

Figure 5. 1 Login form 29

Figure 5. 2 User Registration 29

Figure 5. 3 PKI SIM Card Generation 30

Figure 5. 4 SIM Verification 30

VT OMNES VNVM SINT

List of Tables

Table 2. 1 Identification and validation registry in Kenya 8

Table 2. 2 Basic PKI Components 12

Table 4. 1 System Administrator Use Case 23

Table 4. 2 Verification Use Case 24

Table 5. 1 Unit Testing Steps 31

List of Abbreviations/Acronyms

CA - Communications Authority

CPU - Central Processing Unit

CRD - Civil Registration Department

DIS - Department of Immigration Services

EPROM - Erasable Programmable Read-Only Memory

GSMA - Global System for Mobile Communications

ID - Identity

IC - Integrated Circuit

IMSI - International Mobile Subscriber Identity

IPRS - Integrated Population Registration System

MNC - Mobile Network Code

MNO - Mobile Network Operator

MSIN - Mobile Station Identification Number

NIIMS - National Integrated Information Management System

NRB - National Registration Bureau OPM

OPM - Office of the Prime Minister

PISCES - Personal Identification Secure Comparison and Evaluation System

PKI - Public Key Infrastructure

RAM - Random Access Memory

ROM - Read-Only Memory

SIM - Subscriber Identity Module

TMSI - Temporary Mobile Subscriber Identity

UCC - Uganda Communications Commission

UMTS - Universal Mobile Telecommunications

Definition of Terms

Certificate Authority – The entity in a Public Key infrastructure that is responsible for issuing certificates and ensuring compliance with a PKI policy.

Digital Signature – The result of a cryptographic transformation of data that when implemented provides a mechanism for verifying origin authentication, data integrity, and non-repudiation.

Elliptic Curve Cryptography – is a public key encryption technique that uses the elliptic curve mathematical entity.

Hash Function – A one-way function that maps a bit string of arbitrary length to a fixed-length bit string.

Key Pair – A public Key and its corresponding private key.

Message digest – The result of applying a hash function to a message.

Public Key Infrastructure – A framework that is established to issue, maintain and revoke public key certificates.

Private Key – a cryptographic key that is used with an asymmetric cryptographic algorithm and the owner does not make it public.

Public key Certificate – A set of data that uniquely identifies a key pair and an owner that is authorized to use the key pair.

Public Key – A cryptographic key that is used with an asymmetric cryptographic algorithm and is associated with a private key

x.509 Certificate – is a digital certificate that is used to manage identity and security in internet communications and computer networking.

Acknowledgment

First, I would like to express my gratitude to God, for His strength and grace throughout this journey.

Secondly, to my supervisors Dr. Vincent Omwenga and Dr. Joe Sevilla, and the Strathmore university colleagues for their consistent guidance and input to this work.

Special acknowledgment to my dear parents, Japhet Gate and Evangeline Gate, and Siblings; Lydiah, Ken, Morris, Yvonne, and Collins for your unending encouragement that constantly pushed me forward to finish strong.

Chapter One: Introduction

1.1. Background to the study

Globally, according to GSMA, there exist five billion unique mobile subscribers, and the growth per year has been estimated to be 3.72%. At the end of 2019, 477 million people in Sub-Saharan Africa subscribed to mobile services, with this number accounting for 45% of the population. This growth rate, especially in Africa, has improved methods of sharing information and also the methods for conducting business (Baker, 2012). In Kenya, Mobile use penetration has grown by 11% from 2014, at 16%, to the year 2019, which was at 27% (GSMA, 2020). 76% worldwide subscriptions and 95% across Africa are based on prepaid SIM cards, and 92% of all prepaid SIM cards are active (GSMA, 2018).

For a mobile phone to connect, it requires a SIM card. A Subscriber Identity Module (SIM) is a computer chip used in mobile phones containing memory for storing data, a processor, and applications that allow users to interact with the SIM. Memory is used to store phone numbers, messages, and emails (Silvester, 2015). Initially, when a Mobile phone is used for the first time, it sends an International Mobile Subscriber Identity (IMSI) present in the SIM card to the network. The network then looks it up in a database to ensure the card is registered. If the IMSI is recognized, the network creates another number called a Temporary Mobile Subscriber Identity (TMSI), which is encrypted and sent back to the phone. The phone identifies itself in all subsequent calls by broadcasting the TMSI (Electrochemist, 2010).

Mobile Network Operators are tasked with registering SIM cards before they are issued to subscribers in countries where Sim card registration is a necessity. Registration of SIM cards is the process of recording and verifying mobile phone numbers and personal information of a subscriber by a communication service provider(Oyediran et al., 2019). Beyond the ability to communicate, a mobile subscription can enable access to many life-enhancing services such mHealth, Medication, and in Kenya financial services such as Mpesa(GSMA, 2018).

Different governments that implement sim card registration policies differ due to specific concerns the government tries to address. The recently mandatory SIM card registration existing in most governments has increased concerns on national security(Oyediran et al., 2019). Mandatory SIM card registration eradicates the potential for anonymity of communications, enables location-tracking, and simplifies communications surveillance and interception(GSMA, 2018).

According to GSMA 2018, Governments take different approaches to mandatory SIM registration and are grouped the approaches into three categories:

• Capture and Store: Operators capture personal information upon purchasing a prepaid SIM card and keep the records, sharing information with government agencies on demand. 81% of countries with mandatory SIM registration laws use this approach.

• Capture and Share: Operators capture personal information and proactively share it with government agencies or regulators. 6% of countries with mandatory SIM registration laws use this approach.

• Capture, Validate and store: Operators capture personal information and validate it against a central government database. 12% of countries with mandatory SIM registration laws use this approach, including Kenya.

Before storing their customer's identification credentials, MNOs are required to validate the document presented or the customer's biometric details, which is usually done by querying a central government database. The validation process leads to either a successful or rejected registration. In Kenya, the telecommunication companies are tasked by the Communication Authority(CA) to capture, validate and store(Legal notice, 2015).

1.1.2. Fraudulent Simcard Registration

The increased penetration of Mobile Subscribers has also brought the increased challenges of fraudulent use Of SIM Cards. With the current registration schemes carried out by MNOs and the rise of activities such as SIM cards, Hawking has created loopholes in the registration process contributing to this problem. Crimes such as Identity theft, SMS Scams, and SIM swap are on the rise (Farooq Rind, 2019), with many subscribers falling as victims. Many governments are experiencing these challenges at different levels; for example, the Taiwan government has equated the Potential loss due to the problem to be up to several million US Dollars per year(YiBing Lin 2012). Safaricom, Airtel, and Telkom Kenya are the main MNOs operating in the country. Their agents have turned to SIM card Hawking to grow their subscribers and, in turn, fuelled the fraudulent registrations that aid criminal activity(Mutualiei, 2019). The CA also has banned SIM card hawking which is referred to as selling Simcard by unlicensed agents. The authority has also placed sanctions such. Subscribers found guilty of these crimes risk six months imprisonment or a fine of Ksh100,000.

Technology has been used to support the identification of fraud during Simcard Registration that has been used is. The implementation of radio communication to detect the presence of fraudulent subscriber modules(Santoro & Claps, 2012).In Kenya, Safaricom has implemented SMS notifications whenever a subscriber's national Identity numbers are used to register a SIMcard Line without their consent(Gadgets Africa, 2020). Another method where technology has been used is implementing an algorithm developed and used for encrypting data stored in or exchanged by the SIMs and the network to curb further cloning, which in turn jeopardizes the secrecy of such data (Santoro & Claps, 2012).

Other Scholars have proposed the adoption of technology in combating the fight against fraudulent SIM card registration. Some of the previous research work includes; the use of radio communication network for detecting the presence of Subscriber identity modules in a network for cellular communications (Santoro & Claps, 2012), and the use of algorithms that encrypt data stored in the SIM modules, and this is to curb SIM cloning (Larsen, 2011).

1.1.3. Public-key Infrastructure

Public Key Infrastructure refers to a system of policies, procedures, people, hardware, software, and services that support the use of public-key cryptography to obtain secure communication from one party to another. PKI was developed to support asymmetric cryptography where the message is usually encrypted by the sender using the public key of the receiver of the message is the only one who can decrypt the message using their corresponding. This type of cryptography solved the key management problem by sharing the signed key in a public file with the sender's name and public key(Albarqi, 2015). The PKI has previously supported pretty good privacy (PGP), an encryption system used to send encrypted emails and to encrypt sensitive files(Updated, 2019). The internet X.509 public key infrastructure(PKIX) is also a well-known infrastructure used to bind the identity of the key holder to the holder's public key.

The public key infrastructure has been used in different use cases recently to assist in the authentication of communication and achieve nonrepudiation, which means we can verify beyond doubt that an individual performed a particular task. Its ability to provide authentication can then be utilized by the MNOs as a method of identifying prepaid customers during SIM card Registration. The signed public-key certificate issued by a certificate authority would be presented to the MNO by a prepaid customer

1.2. Problem Statement

According to the communication Authority, in the effort to identify the fraudulent SIM registration due to its security concerns, it has directed the MNOs to ensure validation of user credentials is done properly on the Integrated Population Registration System (IPRS). This directive was issued to assist the MNOs to avoid inconsistencies and fake subscriber identity.

The current way of identifying fraud in SIM Card registration is that most governments, especially those in the developing world that require mandatory SIM registration, have weak National Identity schemes (Donovan & Martin, 2014). World Bank has estimated 1.1bn people across the globe lack official documentation. Most of them are in developing countries across Africa and Asia, where proof-of-identity is required during SIM card registration. In Kenya, proof of identity has been through submitting your National ID during SIM card Registration. This is then validated on the IPRS, which was intended to serve as the single source of truth (Atellah, 2019). However, the IPRS is limited in capacity. It only contains consolidated data from primary population registration agencies, these being the Civil Registration Department (CRD), National Registration Bureau (NRB), and Department of Immigration Services (DIS), which are established by different legal regimes. The challenges with the Kenyan verification approach are that there are existing gaps that create loopholes for criminals to create fake National Identity cards and use them during SIM card registration without the Knowledge of the MNOs. This research will focus on implementing Public Key Infrastructure as a method to identify fraudulent SIM card registration. PKI will provide a method to identify a legitimate prepaid customer for the MNO during the SIM card registration process and give a method to later verify the valid user.

1.3. Objective

1.3.1. General Objective

The purpose of this study is to provide the Mobile Network Operators (MNOs) with a way to curb fraudulent SIM card Registration by using a prototype that implements the PKI verification approach.

1.3.2. Specific Objectives

i. To analyse SIM card registration in Kenya.
ii. To review approaches used to identify the legitimate SIM card owner during SIM card registration.
iii. To design, develop and test a prototype to identify fraudulent SIM card registration using PKI algorithm-based technique.
iv. To validate the performance of the developed prototype in identifying fraudulent SIM card registration cases

1.4. Research Questions

i. How is SIM card registration carried out in Kenya?
ii. What approaches are used to identify the legitimate SIM card owner during SIM card registration?
iii. What techniques can be used to design and develop a prototype to identify fraudulent SIM card registration using the PKI algorithm-based technique?
iv. Is the PKI approach an effective technique to curb fraudulent SIM card registration?

1.5. Justification

This research is useful because it provides a method to validate the identity of a user intending to register for a SIM card. Identifying prepaid customers is important to the Mobile Network Operators since it facilitates the Know Your Customer policy, thus enforcing transparency and accountability on its subscribers. Solving the problem of fraudulent registration of SIM cards will be important to the subscribers who may be the victims of mobile-related crime.

1.6. Scope and limitation

The focus of this research will be on developing a framework to identify fraudulent SIM card registration. This research will not cover the larger verification and validation of identity schemes, including the civil registration and Nation Registration Bureau. This research is geographically limited to SIM card registration in Kenya. The tool will work as a web-based application to be used by the telecommunication companies during the registration process of the SIM card.

Chapter 2: Literature Review

2.1. Introduction

This chapter begins with an overview of how the SIM card works; it shows its structure and its unique features used by MNOs for user registration; it then analyses the current cases of fraud during SIM registration and how these fraud cases have affected the users. The review further seeks to check previous work done in curbing SIM card fraud, how the different countries have deployed these solutions, and to what extent the solutions have been able to resolve the challenge of fraud during SIM registration.

2.2. SIM card structure overview

The subscriber in Second-generation, Global System for Mobile Communications (GSM) and third-generation Universal Mobile Telecommunications System (UMTS) networks are usually identified by an International Subscriber Identity (IMSI). The IMSI comprises a three-digit Mobile Network Code (MNC), which determines the GSM network within a particular country, and a Mobile Station Identification Number(MSIN)of up to ten digits. The MSIN identifies the subscriber within a network, while the MNC and MSIN identify the subscriber within a country(Santoro & Claps, 2012).

The subscriber identity module is a smart card that stores the subscriber identification codes such as the IMSI. According to Sheng (2007), This smart card has a microprocessor, and it contains the following modules: a Control Processing Unit (CPU), Program memory(ROM)working memory (RAM), Data memory (EPROM or E2PROM), and a serial communications Module. All the five modules are bundled together in an Integrated Circuit(IC) to avoid illegal access and ensure the card's security. There are two different forms of SIM cards with the same functions: one is the full-Size SIM Card either the IC cards of ISO 7816 and size 25mm by 15mm and the Embedded SIM card, which is a Semipermanent packed to the cards in the mobile station equipment(Sheng, 2007). In all the two cards, they have installed waterproof, wear-resistant, anti-static contact with high accuracy and reliability characteristics.

Initially, the SIM was part of a European telecommunications standard that separated the mobile phones from the connected network by moving all the necessary security and identification data onto a chip embedded into a removable piece of plastic (prokaza, 2018). With the recent evolution of GSM technology, the SIM currently also stores a password that acts as a key to decrypt data. In the design of a SIM, it contains subscriber-related information,

including its identity, authentication key, and encryption key(Yi-Bing Lin et al., 2002). The SIM has limited memory, so it only stores information needed to connect to a mobile phone network. It sores the IMSI, whose function is to communicate the subscriber's call to a caller rather than someone else(prokaza, 2018). Before the innovation of cloud backup was made accessible to a mobile user, the SIM was also used to store contact names and their telephone numbers.

In its structure, the SIM card has features that are meant to retain its authenticity and security. One SIM is intended for one subscriber, although a particular subscriber can hold different SIM cards. The registration Process by the MNOs who are mandated to ensure this should be equivalently secure to cover any loopholes for fraudsters registration.

2.3. SIM card registration

According to (GSMA, 2018) Globally and in Africa, most Mobile subscriptions are usually based on prepaid SIM cards, and 92% of all prepaid SIMs are active in countries where SIM registration is Mandatory. Governments currently require mobile Network Operators to capture store and validate customers' identification credentials before registering their SIM Card in these countries. Other governments are now also requiring MNOs to Implement biometric authentication before writing a customer's SIM Card.

Currently, there is no requirement by either the federal or state level to register end-users of prepaid SIM cards in the USA. However, Senate Bill 3427 proposes using social security numbers, credit/debit card numbers, or driver's license numbers as a way for the seller to verify the customer's identification information. The Information to be retained by a wireless carrier include technical Information to identify the mobile device or the IMSI to identify a SIM card.

In Kenya, SIM card Registration has been tasked by the communication Authority to the MNOs.The majority, Safaricom Airtel and Telkom require capturing the owner's identification details before issuing a SIM Card. The regulation for SIM card registration by the Communications Authority of Kenya (2019) states that upon identifying documents, the telecommunications operators and licensed agents shall validate the said document as shown in Table 2.1.

Table 2.1. Identification and validation registry in Kenya (Emrys Schoemaker et al., 2019)

Type of identification	**Validation Registry**
National IDs	Integrated Population Registration System (IPRS)
Kenyan Passport	Personal Identification Secure Comparison and Evaluation System (PISCES). The telecommunication operator shall maintain a copy of the ID.
Other Passports	Integrated population Registration System (IPRS) and /or Personal Identification Secure Comparison and Evaluation System (PISCES). The telecommunication operator shall maintain a copy of the ID.
Alien	Integrated Population Registration System (IPRS). The telecommunication operator shall maintain a copy of the ID
Military IDs	The telecommunications operator shall maintain a copy of this ID

The Communications Authority requires an annual report from the telecommunication operators that includes the list of all SIM cards issued to their agents and the number sold by each during the telecommunications operations, the number of verification requests against IPRS and PISCES, and the mechanisms put in place to ensure customer information and personal data is secured.

2.4. Fraudulent SIM card registration cases

According to CNA (2020), recently, there has been a rise in fraud relating to prepaid SIM cards in Singapore. One of the cases involves eight individuals engaged in fraudulently registering prepaid SIM Cards using the particulars of unsuspecting customers or foreigners who have not entered Singapore. From the Singapore police force statements, the culprits had abused the computer systems holding registration information for prepaid SIM cards. They would then pre-register SIM cards using particulars of others and sell them to any other subscriber who wished to remain anonymous. This SIM card fraud case has led to the rise of other crimes such as unlicensed moneylending and scams. The culprits also took advantage of the anonymity provided by the Sim cards to continue contacting the victims untraceable and to also evade possible detection amongst themselves. Singapore is one of the countries in Asia that requires

proof of Identity during registration. The National Registration Regulations stipulate the sanctions in place intended to curb fraudulent SIM card registration and usage. For this case, the culprits risk a jail sentence for up to three years or a fine of up to ten thousand US dollars(*CNA*, 2020).

In Uganda, the Daily Monitor reported a SIM card syndicate charging fifty thousand Ugandan shillings to get a functional SIM card duly registered with mobile money services using a forged identity card in thirty minutes upon payment. The syndicate included telecom agents and security guards who operate the MTN and airtel SIM card registration centers. During the processing of the SIM card, they require a photo, ask for the customer's name and date of birth. They then use a fake name and a fake date of birth to create a refugee identity card. With a fake identification, the process of registering a SIM is initiated. The clients choose their wished telephone number from the printed list, and in thirty minutes, they have a newly registered fake SIM card. The Uganda Communications Commission (UCC) states that one can only acquire a new SIM upon presentation of a valid ID from the National Identification and Registration Authority, a foreigner can only acquire a SIM card Upon presentation of a valid passport, and a refugee needs an identity card or any other authorization letter from the Office of the Prime Minister (OPM) (Ngwomoya, 2019).In such a scenario, the fraudulent registration of SIM cards is treated as a threat to the country's national security. The anonymity presented using forged documents made it difficult for any criminal to be traced, even using the telecoms database.

Kenya has already surpassed the 100 percent mark of mobile penetration, and according to the Communications Authority, this has been marked by the fact that most users own more than one SIM card either from the same or different service providers. The rise of penetration rates has also increased the number of fraudulent registration cases and rampant SMS scams. In one case, a doctor recently sued one of the telecoms for over three hundred thousand Kenya Shillings SIM card fraud. In this case, the fraudsters used the Doctor's details to register new SIM cards, and later the criminals used the acquired fake SIM cards to sell their land to an unsuspecting buyer without his knowledge. The fraudsters initiated a sale transaction involving his land, and the piece was sold for 300,000 Kenyan shilling's. Buyers then paid for the ground using a Mobile money service and later approached the Doctor to transfer the land documents, which the Doctor was unaware of. The investigators then revealed that two SIM cards had been registered using the Doctor's credentials, and the fraudsters masqueraded as the Landowners (Joseph Penda, 2020).

There is a challenge to verify or identify the legitimate subscriber during the SIM registration process in all the above cases. The difficulty levels rise even higher when the fraudsters liaise with government officials, who make prosecuting the criminals harder. The issues have also revealed that the telecoms database could be holding wrong information regarding their customers due to the inability to have a process that prevents unlawful registrations of SIM cards.

2.5.Approaches of identifying SIM card Owners

2.5.1. SIM card identity validation approaches

Different governments implement different policies to foster Know Your Customer policies for the MNOs.The categories are capture and store, capture and share, capture, and validate(GSMA, 2018). For those MNOs in the regions where their governments require capture and validation, they are required to validate their customer's identification credentials against a central government database, usually maintained by a government regulator(Waddington & Wilson, 2019). Eleven countries requiring capture and validation require MNOs to use biometric-authentication processes when registering their prepaid SIM customers(GSMA, 2018).GSMA has indicated that the capture and validate method gives the highest assurance that the registered individual is who they claim to be.

Validation methods require the presence of the subscriber during the registration process. This can be done through a collection of biometrics, that is, fingerprints, or a capturing a photo for facial recognition. It could also be done by querying an existing government database with the subscriber's original details to ensure they are who they say they are. However, the success of these validation schemes is highly dependent on the extensiveness of the national identity schemes.

SIM card on its own has the IMSI, which is a unique code to identify the module. The IMSI is made up of a three-digit Mobile Network Code(MNC), which determines the GSM network within a particular country, and a Mobile Station Identification Number(MSIN)of up to ten digits. The MSIN identifies the subscriber within a network, while the MNC and MSIN identify the subscriber within a country(Santoro & Claps, 2012).

2.6. Methods of implementing Owner identity.

2.6.1. Coupling a SIM Module to a wireless Communicating device

This method adopts a phone profile in a wireless device to a subscriber identity module. According to Burgan & Basharat, (2008) involves the following steps:

Extract the subscriber identity information from a SIM card when it is coupled to the wireless communication device. The next step involves associating at least a portion of the subscriber identity information from the SIM card with at least a predetermined profile stored on the wireless communication device and enabling access to the predetermined profile only when the portion of the Subscriber identity information is associated with the predetermined profile stored on the wireless communication device.

2.6.2. Electronic Know Your Customer (eKYC)

Singtel, a telecommunication company based in Singapore, has recently launched a digital self-registration service known as the electronic Know Your Customer(eKYC) that will enable prepaid customers to purchase a SIM card and do the registrations online (BIS, 2019).

eKYC involves using a systematic method to capture a person's biometric data for Customer Identification and Verification (CIV). The procedure starts with enrolment which involves in-person capture; this could be done through third parties that act as enrolment centers established for document authentication and capturing of biometric data. This data is then put together in a national registry where the telecommunication companies can query and be used to verify the identity of their customers, as in the case of Singapore(GSMA, 2016). When a user requests a new SIM card, the service provider uses a card reader authorized by a regulator or the ID agency to authenticate the information with the central database to fulfill CIV requirements. (Perlman & Gurung, 2019)

2.6.3. Use of radio communication network to detect a fraudulent subscriber module

This solution provides an automatic mechanism that can determine whether a legitimate and illegitimate Sim are used at the same time(Santoro & Claps, 2012). The implementation of this solution provides a method of detecting a fraudulent Sim regardless of the physical service location of the legitimate SIM and without making unnecessary network resources. Once the illegitimate SIM is detected it allows the network operator to intervene.

According to Santoro and Claps (2012), this deployment is done in the following steps: First, a service node, receiving a registration request by first user equipment compromising a SIM for defining the identity of a subscriber; initiating a checking to establish whether the subscriber is already registered with the same identifying at least one service node of over the network including the first service node. If the subscriber is already registered with the same identity in at least one service node over the network, retrieving status information on at least a second user equipment associated with the already registered subscription for checking whether the

second user equipment is not the first user equipment and then disabling any subscription of the subscriber associated with the identity if the second user Equipment results not to be the first user equipment.

2.7. Public Key Infrastructure

From the introduction on the background of the study, Public key infrastructure is the framework of encryption that protects communicating entities (Heinonen,2018). It is used to govern the issuance of digital certificates to protect sensitive data, provide unique digital identities for users, devices, and applications, and secure end-to-end communication(Sandberg & Rodberg-Larsen, 2006).PKI provides security through encryption, and this is achieved through the use of a public key which anyone can use to encrypt a message, and a secret/private key, which only one person should be able to use and decrypt the sent messages. People's devices and applications can use these keys. The common application for PKI is, for example, the use of SSL certificates on websites and the use of digital signatures. PKI model is used since it enforces integrity confidentiality authentication and non-repudiation. It can achieve this by combining both symmetric and asymmetric and hashing to ensure efficiency.

In symmetric cryptography, the same key is used for the encryption and decryption of messages. This structure is risky because if the distribution channel used to share the key gets compromised, the whole system for secure messages is broken(Heinonen et al., 2008). Asymmetric encryption solves the exchange problem in symmetric cryptography. A message goes through mathematical permutations to become encrypted but requires a private key to decrypt and a public key to encrypt.

Both symmetric and asymmetric are used together since asymmetric encryption is slower. Asymmetric encryption alone has the security risk of the man in the middle. PKI resolves the man's challenge in the middle by issuing and governing digital certificates that confirm and verify the identity of people, devices, and applications that own private keys and the individual public keys, which ensures confidentiality between the parties involved(Key factor, 2018). PKI provides that a certificate signed using an individual's private key, the corresponding public key pair can be used to; Authenticate that the individual presenting the signed certificate owns the corresponding private key and ensure integrity in that what is contained in the certificate has not been changed from its initial form("PKI and Digital Certificates for Government," 2018)

Authenticating, providing integrity, and encrypting a message that can only be decrypted with its associated private key allows the PKI infrastructure and digital certificates to verify individuals over a secure communication channel. The management of the digital certificates, which includes their issuance and revocation, is done by an entity known as the Certificate Authority.

Table 2. 2 Basic PKI Components (Al-Khouri, 2011)

Components	**Description**
Digital certificate	They act as the foundation of the Public Key Infrastructure, which includes electronic credentials consisting of public keys used for signing and encrypting data.
Certification Authorities (CA)	These are the trusted entities involved in managing the digital certificates, which include their issuance and revocation.
Certificate policy and practice statements	These are policies that outline the degree to which the digital certificates and certification authorities are to be trusted and the legal channels to be followed in case this trust is broken.
Certificate repositories	This is the location where the Certificates are stored and published.
Certificate revocation list	This is a list of certificates that have been revoked before their actual expiration date.

VT OMNES UNVM SINT

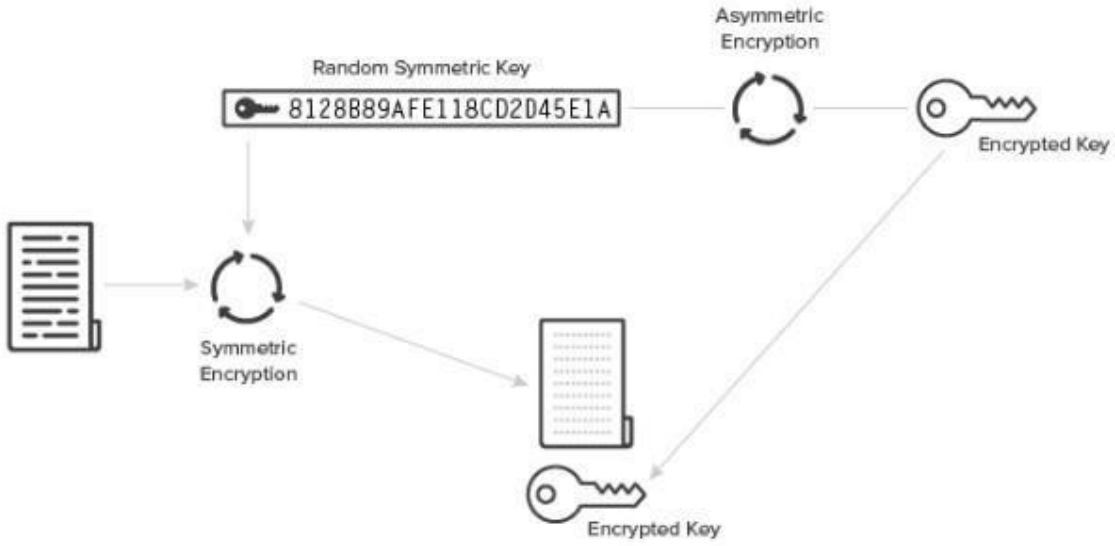

Figure 2.1. Asymmetric Encryption (Sandberg & Rodberg-Larsen, 2006)

PKI resolves the challenge of the man in the middle scenario in both Symmetric and asymmetric cryptography. It can do so by issuing digital certificates to confirm the identity of people, devices, or applications that own private and corresponding public keys(Heinonen et al., 2008).

Certificate authorities are responsible for creating digital certificates and own the policies for vetting recipients and issuing the certificates themselves.

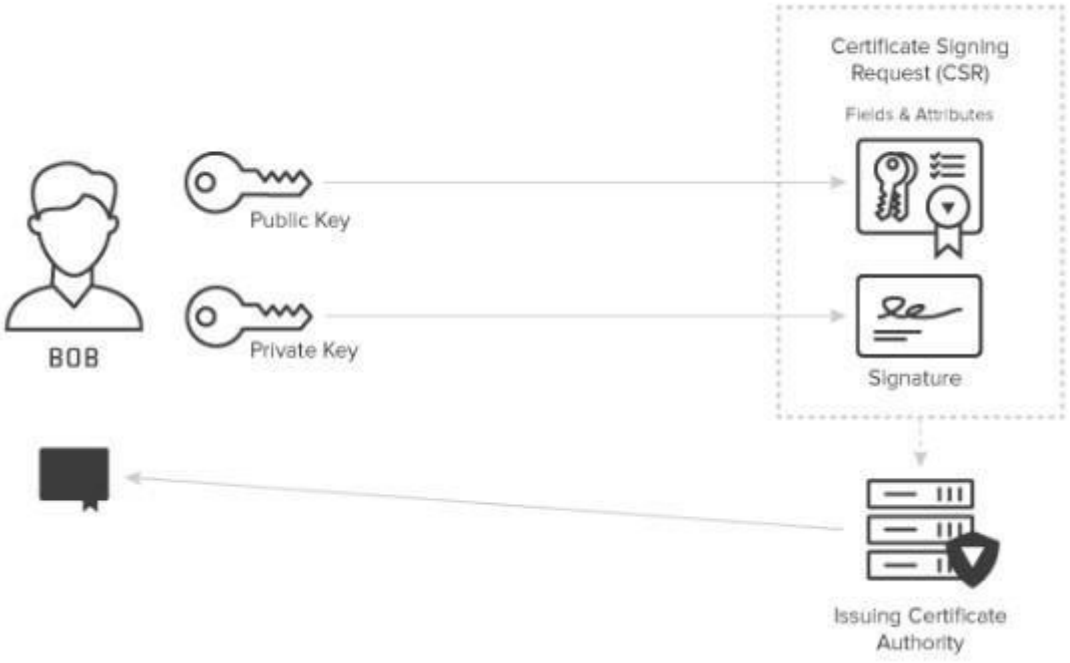

Figure 2. 2 Public Key Infrastructure (Sandberg & Rodberg-Larsen, 2006)

2.7.1. PKI authentication on the internet

For entities on the internet to communicate there need to exist trust and one of the way,s this is achieved is by having these entities verify their identity. For secure communication, for example between a web server and a web application, this is enabled by the secure sockets layer which is a security protocol that creates an encrypted link between a web server and a web browser(*DigiCert*, 2019).In SSL communications, the server's SSL certificate contains an asymmetric public and private key pair while a symmetric session key is used between the server and the private key during the SSL handshake.

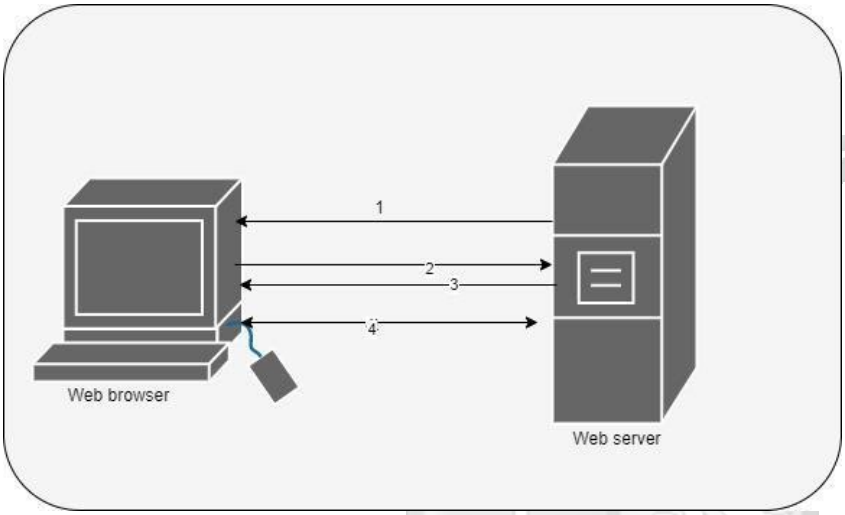

Figure 2. 3 The ssl handshake (Rodberg-Larsen, 2016)

The SSL handshake

Initially, the server sends a copy of its asymmetric public key, then the browser creates a symmetric session key and encrypts it with the server's asymmetric public key then sends it to the server. The server decrypts the encrypted session key using its asymmetric private key to get the symmetric session key. Finally, the server and browser now encrypt and decrypt all transmitted data with the symmetric session key(*DigiCert*, 2019).

2.8 Public Key Algorithms

2.8.1 RSA Algorithm

RSA is a public-key algorithm that is named after Ron Rivest, Adi Shamir, and Leonard Adleman the individuals who invented it. It works by ensuring that the key pairs are secured(Educative, 2020). One individual can send an encrypted message to another individual without any prior exchange of secret keys. The first one uses the second's public key to encrypt

the message and then decrypts using the private key which is only known to them.RSA can also be used to sign messages in digital signatures(Barker, 2016).

How RSA works(Barker, 2016).

1. Generate two large random primes, *p* and, *q* of approximately equal size such that their product $n = pq$ is of the required bit length.
2. Compute $n = pq$ and $o = (p - 1)(q - 1)$.
3. Choose an integer e, $1 < e < o$, such that $gcd\ (e,o) = 1$.
4. Compute the secret exponent d, $1 < d < o$ such that $ed = 1\ mod\ o$
5. The public key is (n, e) and the private key is (d,p,q). Keep all the values d,p,q, and o secret.

n is known as the modulus.

e is known as the public exponent.

d is known as the secret exponent.

2.8.2. Elliptic Curve Digital Signature Algorithm

ECDSA is a Digital Signature Algorithm that uses the keys derived from Elliptic Curve Cryptography (ECC) (HYPR, 2021). ECDSA is popular because of its smaller key size and ability to maintain security. This trend continues to grow as the demand for devices to remain secure increases due to the size of the keys growing, drawing to the scarcity of mobile resources. ECDSA bases its approach to public-key cryptographic systems on how elliptic curves are structured algebraically over finite fields. Another advantage of using ECDSA it assists to maintain high levels of both performance and security. Due to its security and performance features, ECDSA is used in the implementation of digital signatures in cryptocurrencies such as bitcoin and Ethereum (AVI networks, 2019).

The ECDSA Key-pair consist of :

The private key (integer): *privKey*

Public Key (EC point): $pubKey = privKey * G$

The private key is generated as a random integer in the range [0…n-1]. The public key *pub key* is a point on the elliptic curve, calculated by the EC point multiplication: $pubkey = privKey * G$ which is the private key, multiplied by the generator point *G*.

The public key EC point {x,y} can be compressed to just one of the coordinates + 1 bit(svetlin Nakov, 2018).

ECDSA Signing Algorithm

The ECDSA signing algorithm takes as input a *msg* a private key *priv y* and produces as output a signature which consists of pair of integers pairs of integers {r,s}. The ECDSA signing algorithm works as follows:

1. Calculate the message hash, using a cryptographic hash function like SHA – 256: h = hash(*msg*)
2. Generate securely a random number k in the range [$1..n - 1$]
3. Calculate the random point $R = k * G$ and take its x – coordinate: $r = R.x$
4. Calculate the signature proof: $s = k^{-1} * (h + r * privKey) \ (mod\ n)$
5. Return the signature *{r,s}*.

VT OMNES VNVM SINT

Chapter 3: Research Methodology

3.1 Introduction

This chapter explains in detail how each of the research questions listed in chapter one was handled. The research methodology chapter shows how the proposed solution was designed, how the research planning was carried out, and how the development and testing were done. The methodology that was adopted for this research was the object-oriented analysis and design. This was preferred since it gave a technical approach for analysing and designing the prototype. It also allowed the researcher to use visual modeling throughout the software development process, which helped communicate the product design and ensured its quality.

3.2 Research Approach for Objectives 1 and 2

The first objective was to discuss how SIM card registration was carried out in the country by the different MNOs.The literature review analysed the procedures and steps involved in registering the prepaid customers to be issued with the SIM cards. From the results of these analyses, the review sought to show the gaps in the current methods of identifying fraud during SIM card registration since the method used for identifying the customer was inadequate. The querying of customer details that would be used for identification was done n the IPRS system, which was a combination of different government databases and lacked the aspect of primary data collection from the citizens. This covered the second objective, which was to review approaches used to identify the legitimate SIM card owner during SIM card registration.

3.3. Research Approach for Objectives 3 and 4

To achieve objectives three and four, a public key infrastructure prototype was modelled to achieve authentication of the customer who is registering for their SIM card at an MNO and bring about the security capabilities of the PKI, which are the integrity of the data and nonrepudiation. This process of modelling the prototype was achieved by implementing the agile software methodology process, which breaks down a given task into smaller iterations. This methodology was chosen since it allowed the process of prototyping. This methodology would allow the prototype to be built, test it, and reworked the model until the acceptable outcome was achieved.

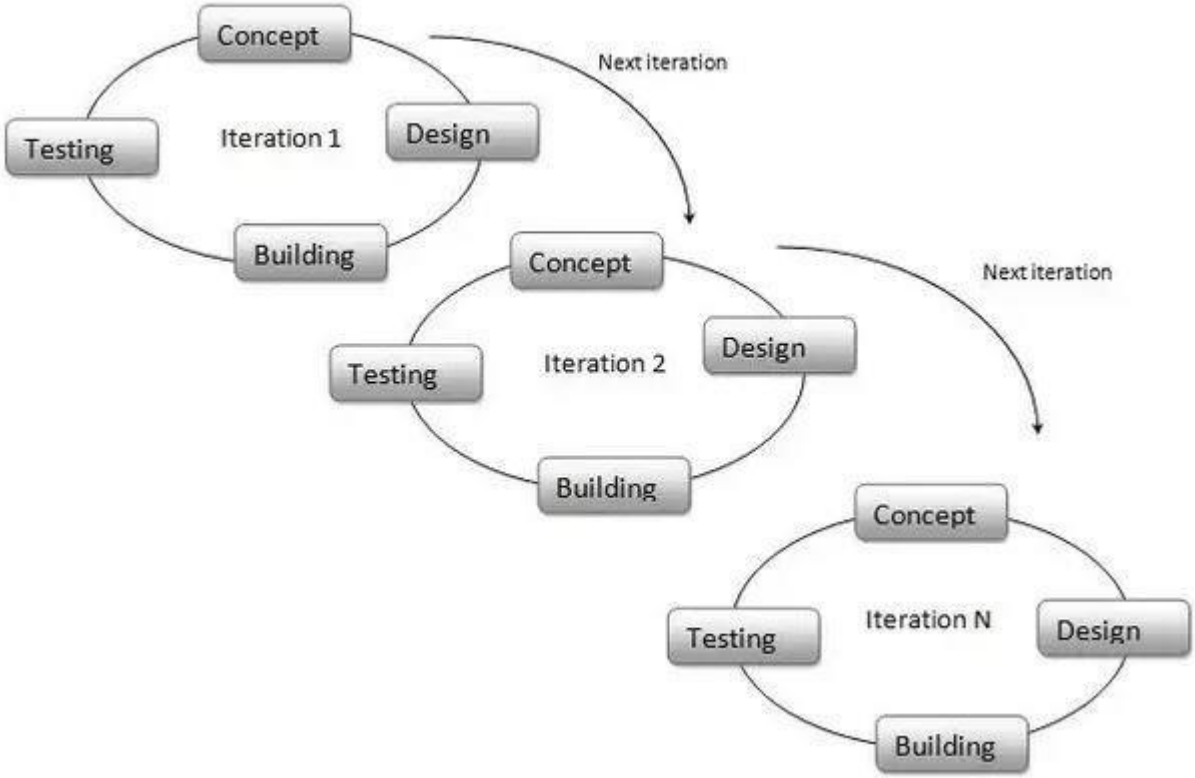

Figure 3. 1 Agile Lifecycle (Ihor Feoktistov, 2020)

3.3.1. Requirements gathering and planning.

The process of requirements gathering, and planning was the initial stage that assisted in building the concept of the model. The activities included in the planning stage involved concept ideation, which was the process of consultation from the subject expert. This was done to give the researcher an overview of what the development lifecycle would look like. The planning stage was divided into project initiation risk analysis and final reviews. From the planning stage, the requirements gathering process followed. They were gathered through document and Journal review and by analysing the gaps of the current system, which was covered in the literature review. The research also included conducting questionnaires to users to understand the challenges they face regarding fraud in SIM card registration. The outcome of this phase will be to define the technical approaches that would be followed to prototype the model successfully.

3.3.2 Design

3.3.2.1 Research Design

In this phase, the experimental research design was used because it allowed more than one independent variable to be applied to more than one dependent variable and thus showed the effect of these results(Mitchell, 2015). Different models had been developed before in the

prototype to curb fraud in the SIM card registration process. Checking the effect of how each stage of the prototype was applied against the ability to solve the problem allowed the design to be effective for this study.

Location and Target Population

The study was conducted from the Strathmore university premises, which was convenient since it is in the capital city of Nairobi, where most of the telecommunication companies had headquarter offices. This location was also unique since the city's population is quite dynamic and high, and it had the most increased cases of SIM card fraud compared to the rest of the cities in the country. The scope also of the research was limited to cases of fraud in Kenya. Thus, the location of this research offered a prime opportunity to reach the target population of prepaid customers.

Sampling Techniques and sample size

The sample size was collected through randomization of the collected samples to ensure equal chances of selection for every sample used in the study. The users from the telecommunication companies and the prepaid customers were part of the selected sample. The study then utilized the stratified sampling technique, which involved dividing the elements of the target population into subgroups. The estimated people who were part of the survey were sixty, obtained through referrals and online research panels.

Data Collection

Both primary and secondary data were collected for the study, and this process was done for three months. The primary data collection included both the quantitative and the qualitative research methods. The use of questionnaires was the major method employed in the primary data collection phase. The questions for the questionnaire are attached to the appendix, and this process was conducted through online platforms such as Google forms. The advantage of the online questionnaires is that they were efficient in reaching the required targets and consumed less time than physical contact with each customer. The secondary data sources included gathering from published journals, books, and websites through document review.

Data Analysis

This involved analysing data collected during the data collection phase. This was done using Microsoft office excel sheets. The results were tabulated using charts for interpretation of results. The steps involved in this phase included gathering data requirements, collecting data, analysis of data, interpretation, and visualization of data. The purpose was to find the meaning

of the data collected in the previous phase from the different customers and use these results to develop the research design. For example, the feedback from the customers regarding how effective other models used to curb fraud had worked would give guidance on what the PKI prototype needed to cover so that it can be an effective tool to solve the research problem.

3.2.2.2.System Design

The design phase involved interpreting the requirements that have been identified in the requirement analysis stage.

The tools that were used for the analysis of the data and process will include the following.

- Use Case diagrams – was used to show how the different users will interact with the prototype.
- Database schema – this was being used to show the relationships between the entities during database design and development.
- A sequence Diagram- was used to show the thlogicalic interaction between the objects in the platform in the order that they follow.

3.2.2. System Development

This phase involved converting the design into an actual prototype by writing code. The development process will be iterative to allow better performance of the detection model. The tools used were.

- Php and Bootstrap – they were used to develop the front end of the platform to allow efficient user interactivity for both the administrator at the MNO and the customer who would also be a user of the system
- Python was used to develop the elliptic curve algorithm that was able to generate the key pairs to be issued to the users

3.2.3. Testing and Deployment

After the development of the proposed model underwent different testing phases to ensure that the desired functionalities are in place. The proposed testing methods were :

- Unit testing involved testing individual modules of the proposed solution to confirm they are performing as they should.
- Integration testing was used to check if the different modules are working efficiently when combined to work together.

3.4. Validation

To ensure accuracy, reliability, and consistent performance of the proposed model, it was validated by performing the outlined functionality execution, and results of each iteration of the testing phase were reviewed and measured for accuracy and reliability. This was done to check if the system can perform identification of SIM cards as indicated in the research objectives. The outcome of the different solutions that were implemented earlier was also compared with the outcomes of the prototype that was model to check if the model was able to correctly identify a customer and in return curb fraud during registration of the customers.

3.5. Research quality aspects

In ensuring the quality of this study two factors which are reliability and validity were assessed. The validity included checking the accuracy of the proposed prototype in meeting the study objectives and he targeted functionality for the prototype while reliability ensured that the proposed methodology which was agile, that was used for the modelling of the public key infrastructure prototype had been applied appropriately.

3.6. Ethical Considerations and Approval

To meet the research standards there was a necessity to obtain ethical approval that would ensure that the research was done under all the required guidelines. This approval was a uired from the institution's Ethical Committee at Strathmore University which is mandated to ensure that quality research is carried out and particularly regarding the subject of fraudulent SIM card registration the data collection process from the prepaid customers was done ethically and give assurance that the research followed all the stipulated research guidelines. The ethical code oonconducts adhered to in this research and this was achieved through acquiring consent before conduction the online surveys.

Chapter 4: System Design and Architecture

4.1. Introduction

This chapter describes the designing process of the prototype that will be used to identify fraudulent SIM card registration. The process starts from system analysis and requirements gathering system architecture which has the UML diagrams.

4.2 System analysis

A survey was conducted to understand the current processes used in the identification and verification of SIM cards in Kenya. The survey questions were drawn from the research questions that were initially formulated to guide the research. The recommendations and the challenges drawn from the survey would help in designing the proposed prototype.

4.2.1. Requirements gathering

The methods used for requirements gathering were conducting a survey and document review for previous work done by other researchers. The survey was issued to users to understand how SIM card registration is currently carried out in Kenya, and the challenges the current SIM card registration has in identifying fraudsters. Document review was important in giving insights to the researcher regarding the different solutions that have been used to identify a legitimate SIM card user during registration. Document review also was used to show the techniques for designing a PKI-based algorithm that would be used to verify a legitimate SIM card user.

4.2.2. Research Findings

The study targeted SIM card owners, and out of the sample collected 11 % owned one SIM card,60 % owned two SIM cards, 27% three Sim cards, and 3 % owned four and More Sim cards.

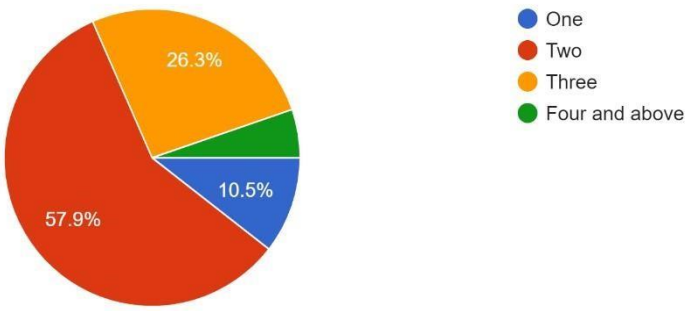

Figure 4. 1 Research Findings Pie Chart.

The majority of those that owned more than one SIM card was not all from the same telecommunication companies. Some of the Telecommunication companies from which most users had were: Safaricom, Airtel, and Telkom, which are the main MNOs in Kenya. Out of all the purchases done, 74% were made from a telecommunication Customer care desk. In comparison, the rest, 26%, were made from a SIM card Hawker who is an unauthorized seller according to the Communication's authority guidelines for SIM cards. Some of the concerns experienced by either having multiple SIM cards or having purchased the SIM card from an unauthorized seller were double allocation of numbers causing a lot of strange calls, having someone else's number registered with legitimate user details, or even having a loan issued to a different user using a legitimate person's details. In addition, some were concerned that through purchasing the SIM card from a SIM card, hawkers were giving out a lot of personally identifiable information like the details f their National Identity cards to an entity that was not guaranteeing any security for this information. Other concerns were getting a lot of spam messages and calls from con artists.

From the survey conducted, some of the recommendations to the problem were; providing a method to assure the customer's data privacy at the point of purchase and beyond, to have only verified outlets as the resellers of the SIM cards from the different MNOs, Encrypting the personal data to curb attacks such as the man in the middle attacks and also to ensure the confidentiality and integrity of the customer's data, including different methods of authentication such as Biometric registrations and issuance of smart cards with electronic chips.

4.3. System Requirements

This section shows the system view, describes what the system needs to do, and outlines operation limitations and assumptions for the prototype. These requirements are drawn from the review of previous studies used in solving the problem applied in different use cases and from the recommendations provided by the users through the survey conducted.

4.3.1. Functional Requirements

Functional requirements are used to define what a system can do by explaining the basic system behavior and its constraints .these features allow a system to function as it was intended, and if they are not met, the system will not work. The functional requirements for this prototype are as follows:

i. The prototype should allow the user to log in and log out of the platform at their convenience.

ii. The prototype should allow the user to view stored customer details for verification when needed. iii. The prototype should allow the process of verification of a user through querying the existing registry.

iv. The prototype should be able to generate keys and associate them with the individual users of the system.

v. The prototype sold be able to revoke or suspend compromised certificates for individual keys.

4.3.2. Non-Functional Requirements

Non-functional requirements are used to define the system behaviors, features, and characteristics that affect the system's usability. When the non-functional requirements are well defined, they bring about a good user experience through meeting the user expectations.

The non-functional requirements are as follows:

i. The prototype should be available to ensure verification and identification of the user is done.

ii. The prototype should be reliable and recoverable to ensure no user data is lost, and if it does, it could be recovered.

iii. The prototype should be easy to use by providing a uniform way to obtain and issue certificates. iv. The prototype should be able to respond to the verification queries in a fast and efficient way.

4.4. System architecture

The system architecture shows the overall outline of the proposed prototype. It is used to abstract the relationships, constraints, and boundaries between the different components of the prototype and provides a view of the physical deployment.

The prototype has a user(Prepaid customer) who sends a request first to the Certificate Authority (CA) to get issued with a signed public key certificate. The RA verifies the user's request for a digital certificate and tells the CA to issue the public key certificate if the users' credentials are valid.

The user can now purchase a SIM card from the telco company and use the e-hakisha application to activate the SIM card. The activation process is initiated by request from the prepaid customer to the telecommunication sharing the IMSI number of the SIM card and the customers. Signed Public keys. The telecommunication sends the user an encrypted response

which when they decrypt the message using their public key gets their key to activate the SIM card.

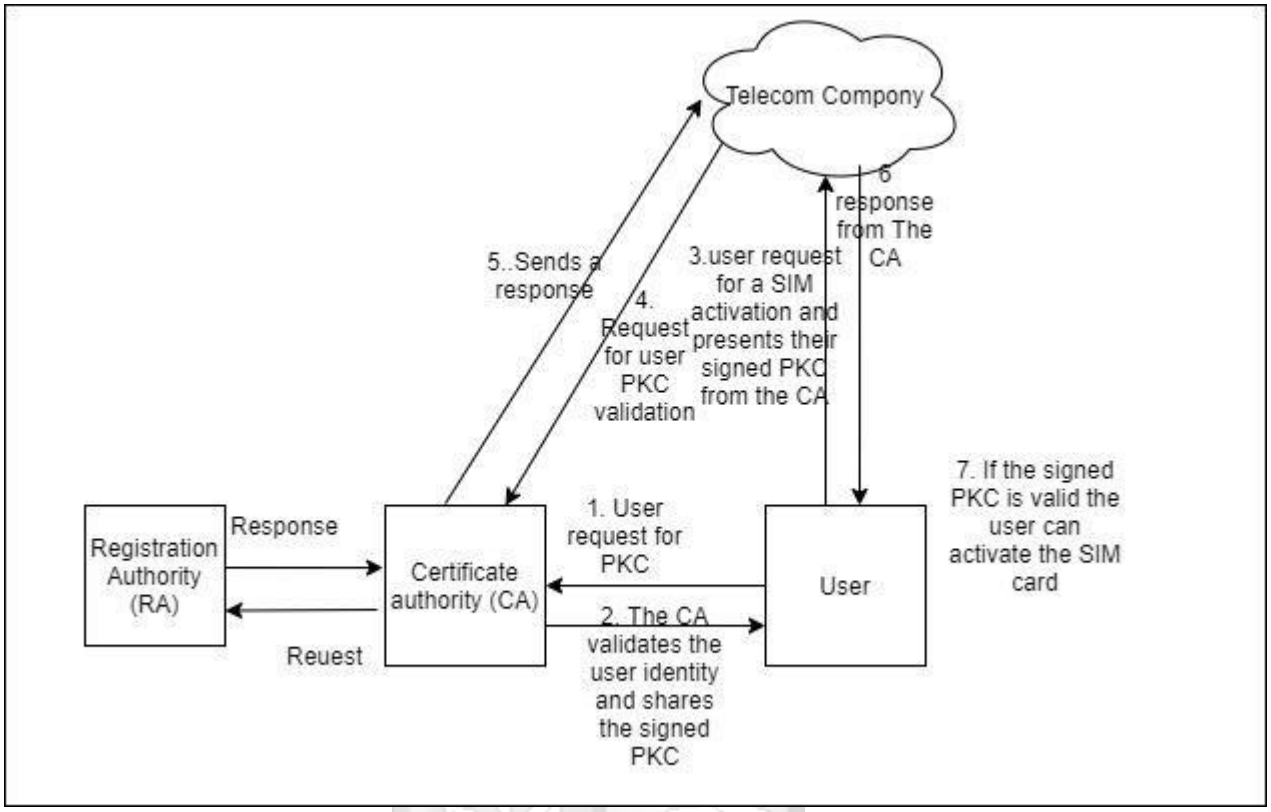

Figure 4. 2 e-hakikisha System Architecture

4.4.1 Key Management

Key Management refers to the process of standardizing the security of the cryptographic keys in an infrastructure setup. This is from the creation, exchange, storage, and deletion. Key Management is crucial since it forms the basis for data security where sensitive data is encrypted and decrypted via the encryption keys(Puneet, 2020). On the e-hakikisha application, both symmetric and asymmetric keys are used in the process of user authentication. Keys ensure the safe transmission of data from the user to the telecommunication company. The key generation algorithm for the e – hakisha is the ECDSA, a secure and high-performance algorithm. The distribution of keys is done through the use of signed public key certificates. Each certificate containing a public key and other information is created by a certificate authority and is given to the user with the matching private key(Delphia weaver, 2016). The registration authority on the e- hakikisha application acts as an interface between the user and the CA for PKC registration. The CA trusts the RA to verify the identity of the user and the certificate content. The signed public-key certificate issued to a prepaid customer has a date of issue, which is used to show the period within which the certificate will be valid. In the communication between the Telco and the prepaid customer, the customer conveys the signed their

key information by transmitting their signed certificate. The Telco can verify that the authority created the certificate.

4.5. System diagrams

4.5.1.Use case Modelling

Use cases are used to outline the primary actors and show the inputs and outputs from the system. These scenarios also explain how the system responds to requests from the primary actor and show what a successful transaction looks like.

Use case diagram

The main actor in this use case is the telecommunications company administrator, who can log in to the system and update the login credentials. The administrator can register a SIM card holder and generate a private-public key pair for the same.

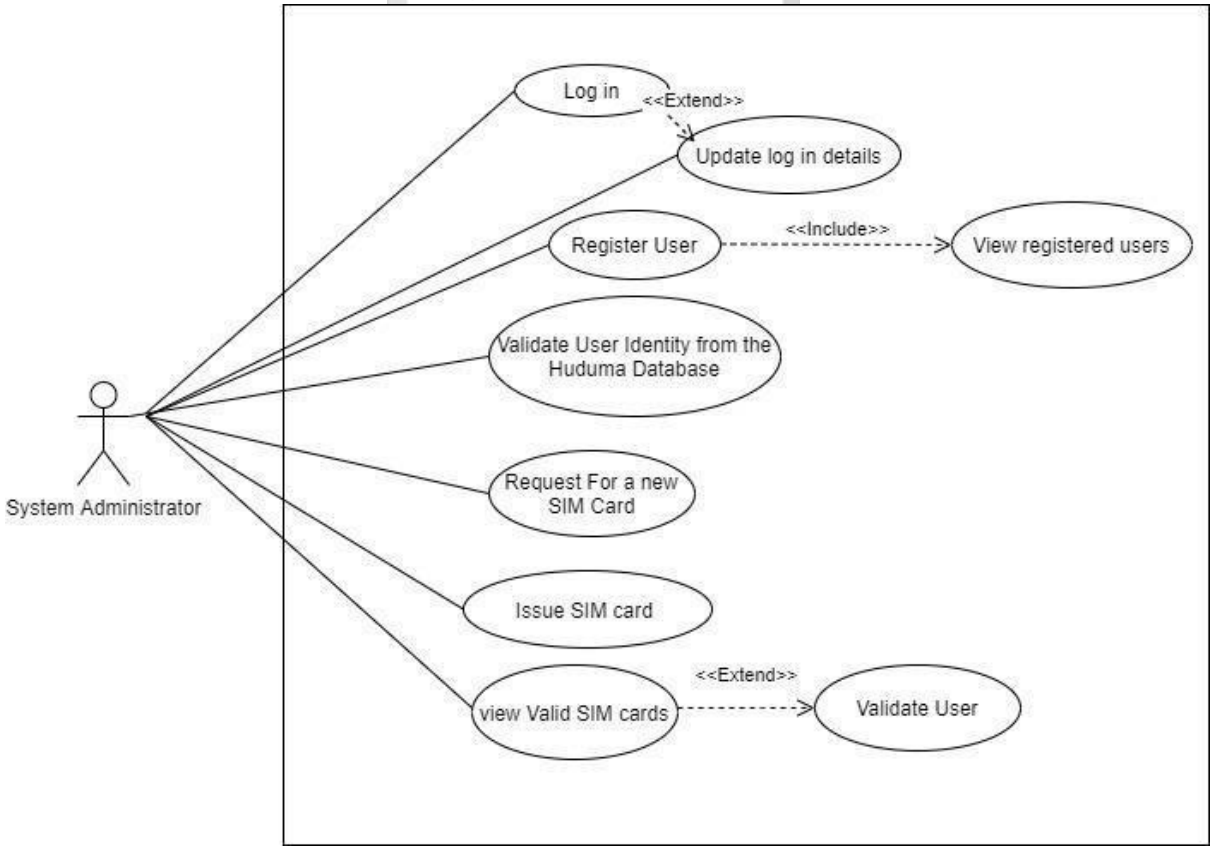

Figure 4. 3 e-hakikisha Use Case

Table 4. 1 e-hakikisha Use Case

Use case	**User registration**
Actor	System Administrator.
Purpose	To register new SIM car users to the telecommunications company database.
overview	This is the initial stage of identifying the legitimate users. after registration, the users are issued with a SIM card that is PKI enabled.
Cross Reference	Verification use case.
Pre-Conditions	The administrator must be logged in to the platform
Postconditions	A SIM card user is successfully registered to the system and issued with a PKI-based SIM card.

4.5.2. The System sequence diagram

The system sequence diagram shows the processes between all the system users or actors and the system itself. The main entities that interact with the system are the system administrator and the telecommunications clerk.

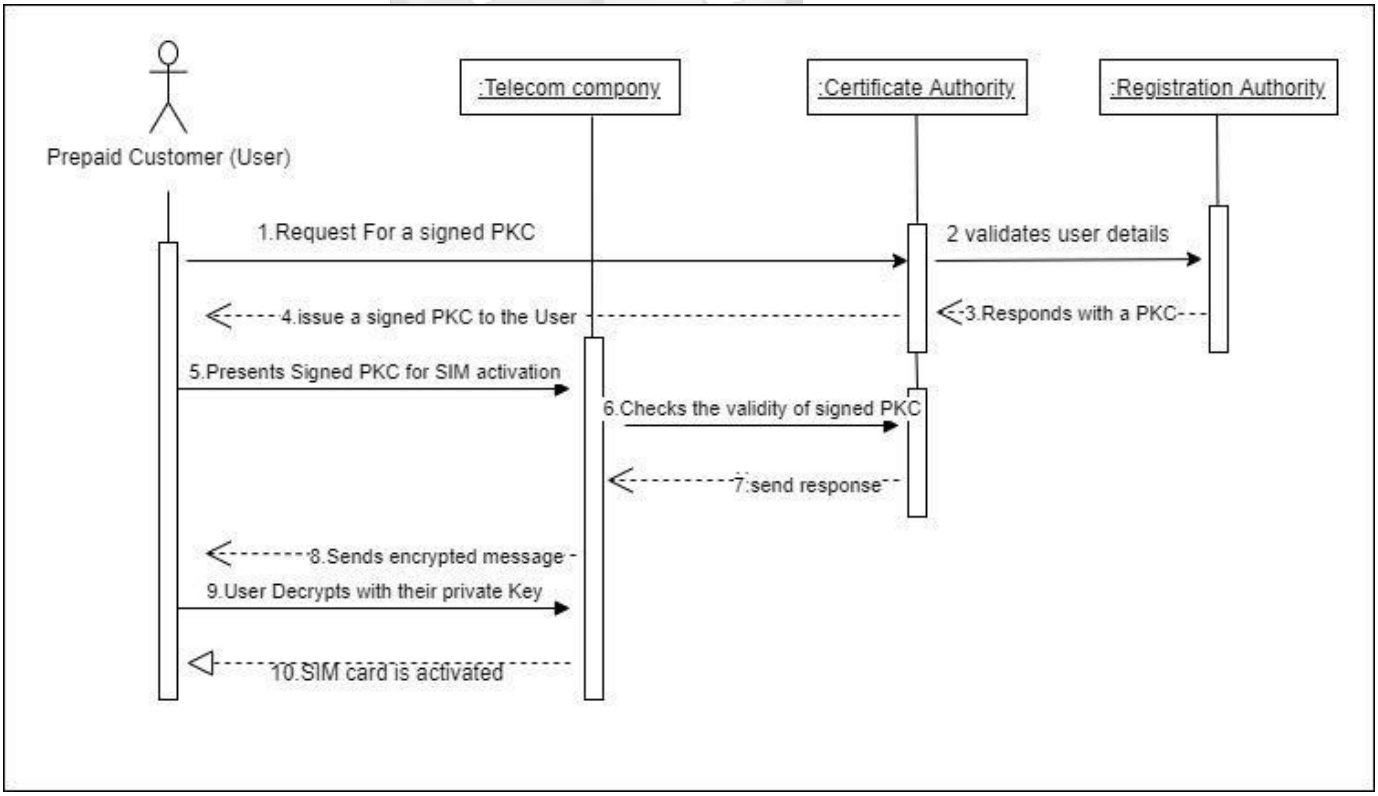

Figure 4. 4 The System Sequence Diagram

4.5.3. Entity-relationship Diagram

It refers to the skeleton structure that is used to represent the logical view of the entire database. It is used to define the organization of data and show the association of the relationships among the different entities.

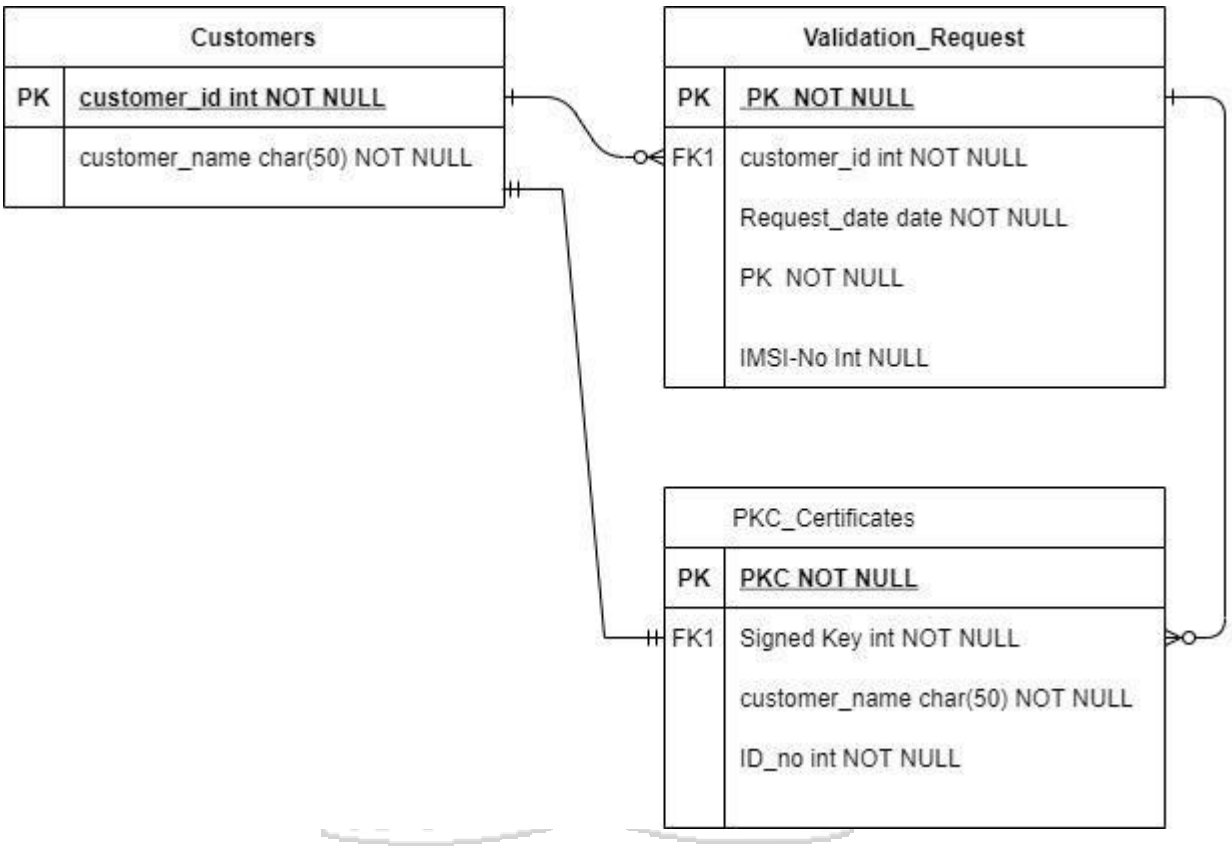

Figure 4. 5 Entity relationship diagram

4.5.4. WWireframediagrams

Wireframerame is used in the design process to show the architectural blueprint. It works as a reference point for showing the functional specifications of the prototype.

System Administrator Login/Logout Interface

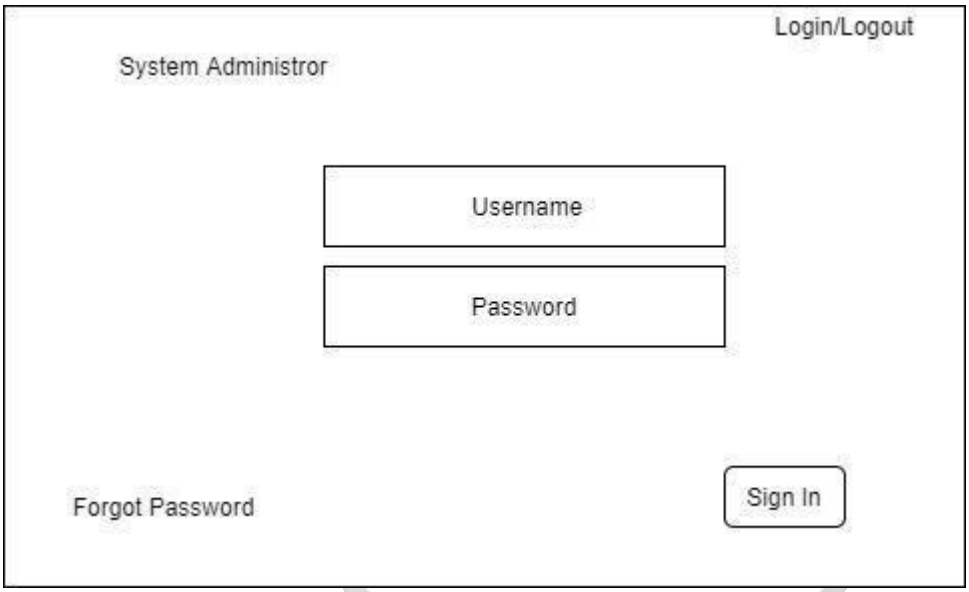

Figure 4. 6 System Administrator Login/Logout

User National ID validation Interface

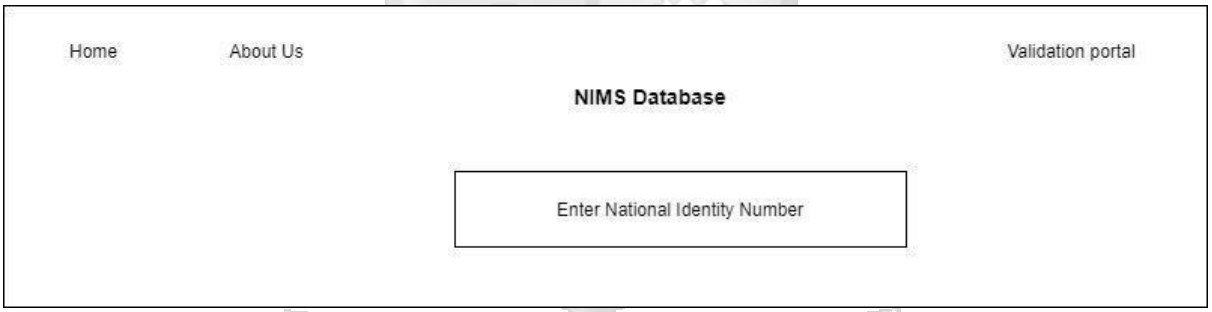

Figure 4. 7 User validation on NIIMS

User Registration Interface

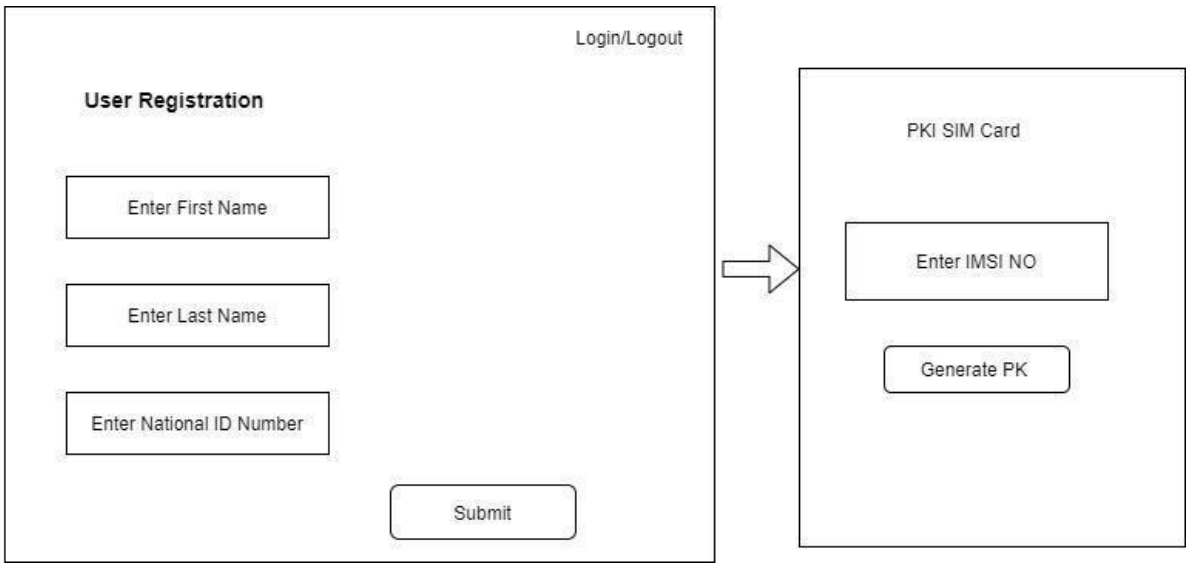

Figure 4. 8 User registration process

Chapter 5:System Implementation and Testing

5.1 Introduction

From the designs created in the previous chapter, the system design was developed, and the prototype was tested to check whether the system is usable and if the functionalities are met. This chapter seeks to discuss the process of system implementation and the tools used.

5.2 System Implementation

5.2.1 Development Environment

The e-hakikisha verification prototype was developed using the Python programming language on the backend and PHP Laravel on the user interfaces. The prototype was expected to have many SIM card verification requests, which necessitated robustness. Python Language allowed the implementation of the ECDSA algorithm to generate public keys, private keys, and digital signatures. The database used was MySQL to store the requests of SIM activation from the user to the telecommunication company. The application also modelled let's encrypt as its Certificate Authority used to the user's public key certificates.

5.2.2. Hardware requirements

The minimum system requirements of the SIM card verification prototype were.

1. Laptop computer with Windows 10 operating system
2. The computers' processor speed was 3.4 GHz, a minimum RAM of 4GB, and A minimum hard disk space of 60GB.

5.2.3 System Functionality

This section looks at the functionalities of the critical interfaces of the prototype.

The administrator Login

The prototype was designed to have an easy-to-use login interface. Upon filing the user details, the system would internally verify the credentials and determine the access level the user has.

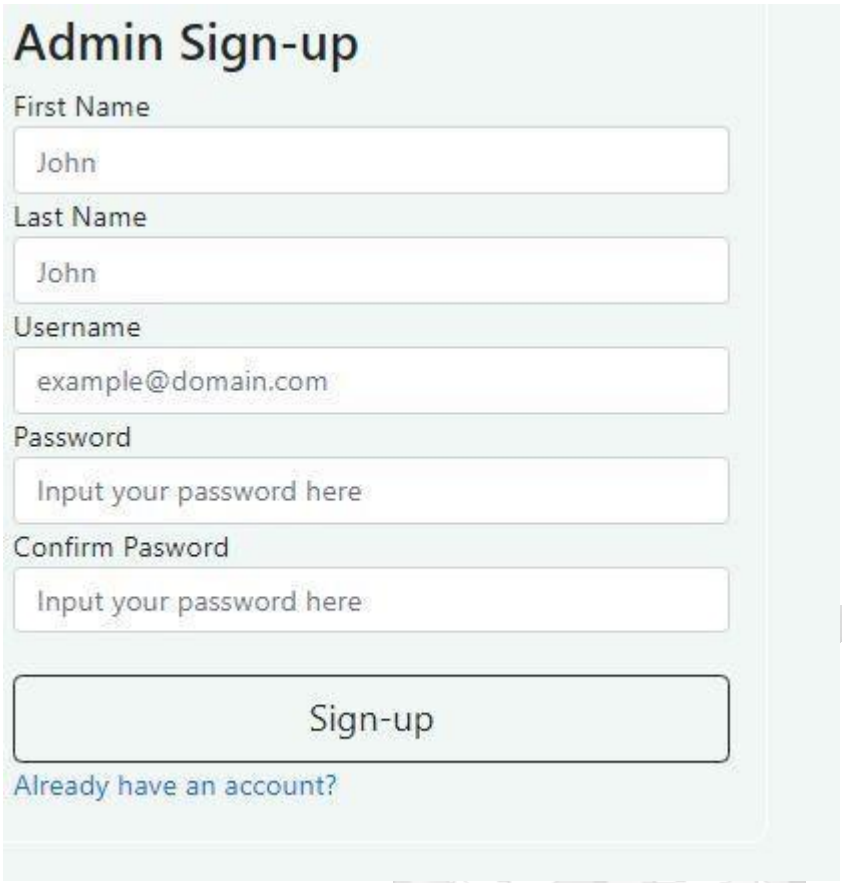

Figure 5. 1 Registration form

VT OMNES VNVM SINT

Figure 5. 2 Login form

User Registration Portal

In this portal, the system administrator after a successful login will enter the user details for the registration of a new SIM card.

VT OMNES VNVM SINT

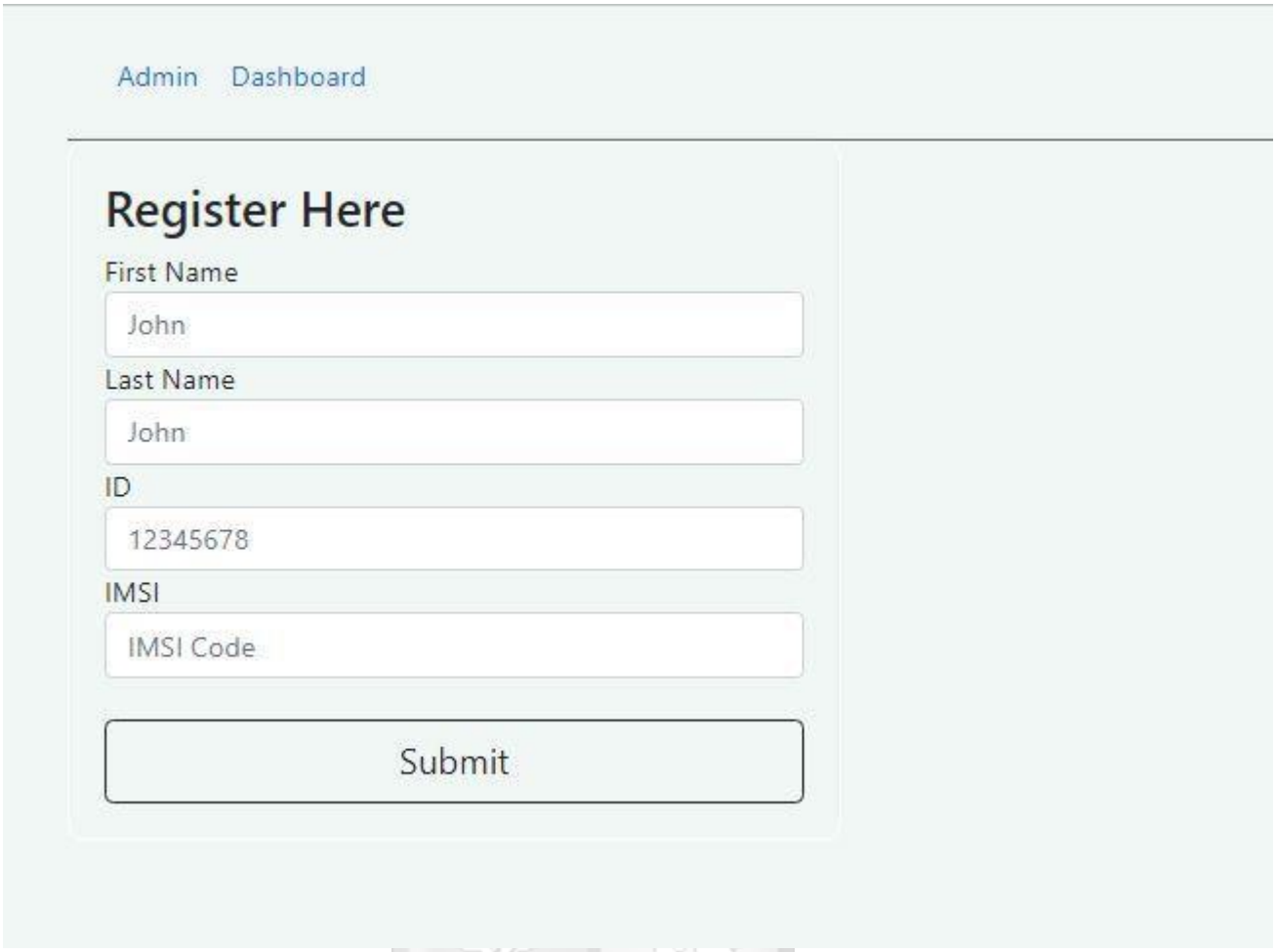

Figure 5. 3 User Registration

Validation of user Identity

Figure 5. 4 User Validation

Generation of PKI SIM card Number

After successful registration of a new user, the system administrator then requests a SIM Card number. This SIM card is a combination of both the National Identity numbered the SIM card's IMSI

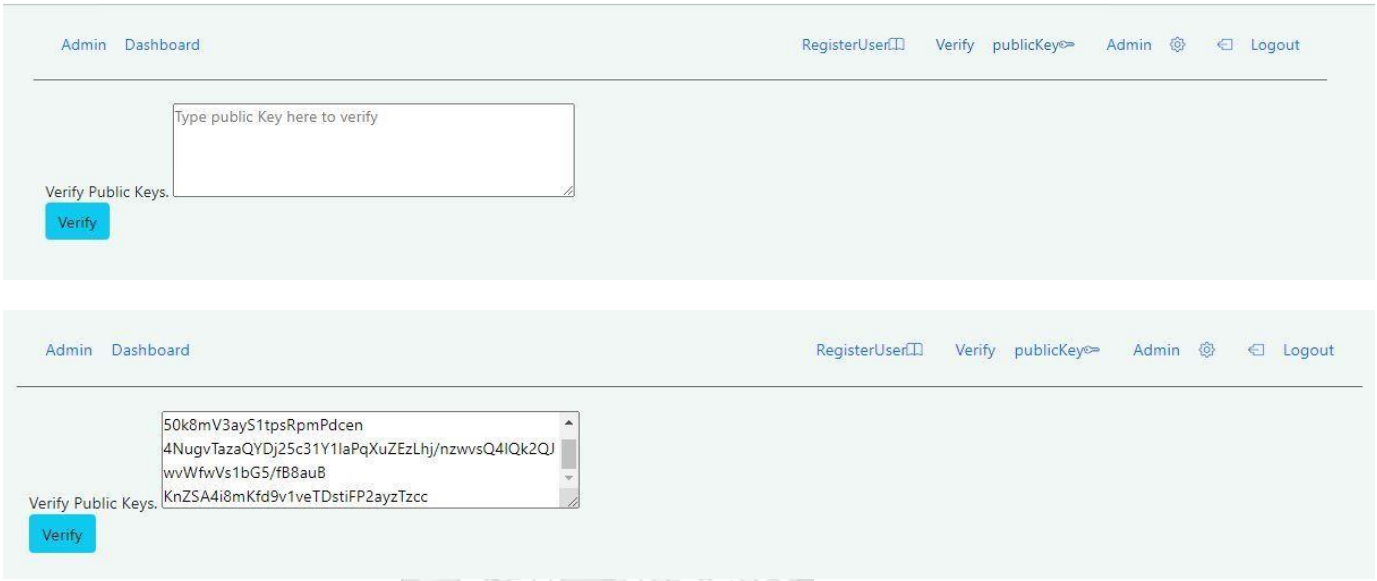

Figure 5. 6 PKI SIM Card Generation

Validation of the SIMcard

This process will be done when a telecommunication company needs to verify that the issued SIMcard or the SIMcard presented by the user is valid. This will be done by sending a query and getting a response as either valid or invalid.

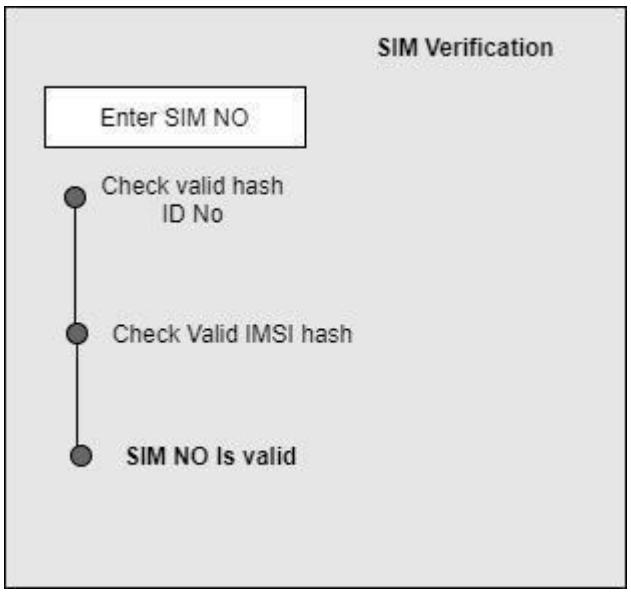

Figure 5. 4 SIM Verification

5.3. Prototype testing

The section describes the functionality tests that were performed to verify if the system met its objectives

5.3.1. Unit testing

Unit testing was performed on each module to ensure that it was developed correctly. In addition, test cases were created to test different modules to check whether they met the user requirements and performed as expected.

Table 5. 1 Unit Testing Steps

Segment	**Test description**	**Results**
Account Registration	Users are required to create an account by providing and confirming their credentials (username and password)	Test passed
Account Login and Logout	Users are required login and log out of the system using their credentials	Test passed
Key generation	Both symmetric and asymmetric keys used for encryption and decryption are generated	Test Passed
Signing certificates	The public key certificate is generated and signed by the CA	Test Passed

5.3.2 Integration testing

Once each module had successfully gone through unit testing, the modules were combined to test how they would work together and deliver on their functionalities. In addition, their efficiency, and their ability to securely exchange data were tested to ensure the prototype performance was as designed. Finally, once the integration testing was successful, the prototype was introduced to respondents for usability testing.

5.4 System Validation

This section seeks to check the alignment of the system to the real business environment where it was deployed. For the SIM card, verification prototype user acceptance testing was done by conducting a survey.

Users were given access to the prototype and were required to answer a questionnaire that would test how usable the prototype was. The questioned checked the user proficiency level against the prototype's ease of use levels.

Below were the recommendations made by the respondents.

1. Improve the verification module to automate the entry of the private key to the system.
2. To have the system deployed on a mobile application for ease of use by MNO's authorized retailers.

VT OMNES VNVM SINT

Chapter 6:Discussion

6.1 Introduction

This chapter discusses the outcomes of the study by analysing each specific objective and how it was realized through the research. It also seeks to show how the research findings contributed to achieving the set objectives.

6.2.Analysis of SIM card registration in Kenya.

This was done through the literature review chapter by discussing in-depth the process of SIM card registration in Kenya. From the review, the telecommunication companies in Kenya who are majorly Safaricom Airtel and Telkom registered their users by using their national identity card as the verification document. After the verification process, the customers are then issued with a SIM card from their respective telecommunication company.

There was a survey conducted during the requirements gathering stage to assess how the current process of registration affected the user. The challenge they faced with the current registration process was the use of their credentials, which is the national Identity card for illegitimate registration. The illegitimate user would then use the falsely registered SIM card for fraudulent purposes and the telecommunication company would not have a way to verify the legitimate user.

The fraudulent SIM card registration often happened when the registration was done without correct verification of the National identity card(GSMA, 2016). Fraud also would occur if the methods in place for identification of the customers by the MNOs are not done effectively(Communications Authority of Kenya, 2019).

6.3.Review of the approaches used to identify the legitimate SIM card owner during SIM card registration.

As discussed in the Literature review, different use cases have been developed to identify a legitimate SIM card user. One of the use cases involves coupling a SIM module to a wireless communicating device. Extracting the subscriber identity information from a SIM card then it is coupled to the wireless communication device. The next step involves associating at least a portion of the subscriber identity information from the SIM card with at least a predetermined profile stored on the wireless communication device and enabling access to the predetermined profile only when the portion of the Subscriber identity information is associated with the predetermined profile stored on the wireless communication device.

From the research findings, the researcher sought to find out how PKI was implemented and if it was an applicable use case in identifying a SIM card. PKI has been implemented in an identity management system where the users were issued with a digital identity card that carried their private key which could then be used for verification of the user.

6.4.Designing, develop, and testing of the prototype

From the document review, a prototype of the PKI-based SIM card was designed. The prototype had a user portal that the prepaid customers would use to request a signed public key certificate from a verified Certificate Authority. The CA after receiving validation from the RA would then issue the signed public key to uniquely identify the customer. The customer uses this signed certificate to request SIM activation from the telecommunication company. The telecommunications company then checks from the CA if the presented PKC is valid. If the certificate is valid, it means the customer has been authenticated and the process of activating the SIM card can be done by the telco through the exchange of keys and messages.

This was implemented using the python programming language which used the elliptic curve algorithm to generate the key pairs and a signature. Currently, the prototype works as a web client to be used by the telecommunications companies who have their system administrator with the rights to issue and verify a SIM card user.

VT OMNES VNVM SINT

Chapter 7: Conclusion and Recommendation

7.1 conclusion

Fraudulent Sim card registration is a problem for both the user who might be the victims after their details are used by the illegitimate users and a problem for the telecommunications companies as they implement the Know Your Customer policies. The current method of validating a SIM card use is limited to using the national identity card number and biometrics which are the face image. This is a challenge because the national Identity card is not fully comprehensive and there are still existing SIM card Hawkers who sell the SIM cards to users without any validation.

This research focused on studying this problem to develop a prototype that would be used to verify fraudulent SIM card registration. The prototype uses the security features and the concepts of a public key infrastructure model to ensure that data for the user is confidential and has integrity. The strengths of the PKI make it suitable to solve the problem of fraudulent SIM card usage. The analysis of the data collected revealed that the developed prototype answered most of the research questions and the specific objectives of the study were met.

7.2 Recommendations

Below are the recommendations made to improve the study:

i. The user could also be issued with a digital certificate which can be verified by a Certificate Authority that will then provide an added security layer.

ii. To use different encryption techniques for example the Elliptic curve cryptography which reduces the processing overhead.

7.3 Future works

From this study the researcher has captured gaps that are in the SIM card registration process, however, the proposed prototype has areas for further research works to be conducted. This prototype could also work for the larger national identification System where the users are issued with a digital national Identity card that has PKI capabilities.

References

Al-Khouri, A. (2011). PKI in Government Identity Management Systems. *Computing Research Repository - CORR, 3*. https://doi.org/10.5121/ijnsa.2011.3306

AVI networks. (2019). *What is Elliptic Curve Cryptography? Definition & FAQs*. Avi Networks. https://www-stage.avinetworks.com/glossary/elliptic-curve-cryptography/

Barker, E. (2016). *Recommendation for Key Management Part 1: General* (NIST SP 800-57pt1r4; p. NIST SP 800-57pt1r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r4

BIS. (2019, November). *Digital ID and e-KYC*. https://www.mas.gov.sg/development/fintech/technologies---digital-id-and-e-kyc

Educative. (2020). *What is the RSA algorithm?* Educative: Interactive Courses for Software Developers. https://www.educative.io/edpresso/what-is-the-rsa-algorithm

Emrys Schoemaker, Tom Kirk, & Isaac Rutenberg. (2019). Kenya's Digital Ecosystem. *Caribou Digital*.

HYPR. (2021). *Elliptic Curve Digital Signature Algorithm (ECDSA) | Security Encyclopedia*. HYPR. https://www.hypr.com/elliptic-curve-digital-signature-algorithm/

svetlin Nakov. (2018). *ECDSA: Elliptic Curve Signatures*. https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages

Albarqi, A., Alzaid, E., Alghamdi, F., Asiri, S., & Kar, J. (2015). Public Key Infrastructure: A Survey. *Journal of Information Security, 06*, 31–37. https://doi.org/10.4236/jis.2015.61004

All about SSL Cryptography | DigiCert.com. (n.d.). Retrieved October 26, 2021, from https://www.digicert.com/faq/ssl-cryptography.htm

Communications Authority of Kenya. (2019). *Registration of SIM cards*.

GSMA. (2016). *Mandatory registration of prepaid SIM cards*.

Mitchell, O. (2015). Experimental Research Design. In W. G. Jennings (Ed.), *The Encyclopedia of Crime and Punishment* (pp. 1–6). John Wiley & Sons, Inc.

https://doi.org/10.1002/9781118519639.wbecpx113

Perlman, L., & Gurung, N. (2019). *Focus Note: The Use of eKYC for Customer Identity and Verification and AML* (SSRN Scholarly Paper ID 3370665). Social Science Research Network. https://doi.org/10.2139/ssrn.3370665

Self-register your Prepaid SIM Card with Singtel's new EKYC SIM. (2019, August 8). *NPN - New Retail New Experience*. https://www.npn.sg/self-register-your-prepaid-sim-card-with-singtels-new-ekycsim/

Updated, J. P. (2019, December 20). *What is PGP Encryption and How Does It Work? | Varonis*. Inside Out Security. https://www.varonis.com/blog/pgp-encryption/

What are SSL, TL, S, and HTTPS? | DigiCert. (n.d.). Retrieved October 26, 2021, from https://www.websecurity.digicert.com/security-topics/what-is-ssl-tls-https

8 arrested over fraudulent registering of prepaid SIM cards after islandwide raids on mobile phone shops. (2020). CNA. https://www.channelnewsasia.com/news/singapore/8arrested-fraud-prepaid-sim-cardsmobile-phone-spf-13025504

Al-Khouri, A. (2011). PKI in Government Identity Management Systems. *Computing Research Repository - CORR*, *3*. https://doi.org/10.5121/ijnsa.2011.3306

Atallah, J. (2019, June 14). *JULIET ATELLAH - Toa Kitambulisho! Evolution of Registration of Persons in Kenya | The Elephant*. https://www.theelephant.info/datastories/2019/06/14/toa-kitambulisho-evolution-ofregistration-of-persons-in-kenya/

Baker, M. (2012). *How mobile puts the business at the tip of Africa's fingers*. t http://www.bbc.co.uk/news/business-18643549

Boateng, O. N. (2018). *SIM Registration—Fraud Prevention Mechanism in Mobile Communication Space in Ghana—Institute of ICT Professionals, Ghana*.

https://iipgh.org/sim-registration-fraud-prevention-mechanism-mobilecommunicationspace-ghana/

Burgan, J. M., & Besharat, M. (2008). *Method and system for associating a user profile to a sim card* (United States Patent No. US20080081609A1).

https://patents.google.com/patent/US20080081609A1/en

Communications Authority of Kenya. (2019). *Registration of SIM cards*.

Donovan, K., & Martin, J. A. (2014). *The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change.*

http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820 Farooq, S. (2019). *Mitigating common fraud risks*.

GSMA. (n.d.). Retrieved December 1, 2020, from https://www.gsma.com/ GSMA. (2018). *Access to Mobile Services and proof-of-identity*. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/02/AccesstoMobile-Services-and-Proof-of-Identity.pdf

GSMA. (2020). *Mobile internet Connectivity 2020*. https://www.gsma.com/r/wpcontent/uploads/2020/09/Mobile-Internet-ConnectivitySSA-Fact-Sheet.pdf

Heinonen, P., Webster, M. A., & Lindstrom, J. (2008). *Method and system for a secure PKI (Public Key Infrastructure) key registration process on the mobile environment* (United States Patent No. US20080130879A1).

https://patents.google.com/patent/US20080130879A1/en

Ihor Feoktistov. (2020, January 9). *Agile Software Development Lifecycle Phases Explained*. https://relevant.software/blog/agile-software-development-lifecycle-phases-explained/

Keyfactor. (n.d.). *What is PKI? A Public Key Infrastructure Definitive Guide - Keyfactor*.

Retrieved December 3, 2020, from https://info.keyfactor.com/what-is-pki

Larsen, R. E., Hazen, P. K., Guliani, S. K., Hasbun, R. N., Talreja, S. S., Ong, C., Brown, C. W., & Kendall, T. L. (2001). *Method and apparatus for preventing the fraudulent use of a cellular telephone* (United States Patent No. US6223290B1).

https://patents.google.com/patent/US6223290B1/en

Legal notice, 163. (2015). *Kenya Kenya Information and Communications Act*. Government press.

Mobile Phone Communication. How does it work? (2010, March 2). *ElectroSchematics.Com*. https://www.electroschematics.com/mobile-phone-how-it-works/

Mobile Subscribers Providing False Information in SIM Card Registration Risk Six Months In Jail. (2018, June 4). *Communications Authority of Kenya*. https://ca.go.ke/mobilesubscribers-providing-false-information-in-sim-cardregistration-risk-six-months-injail/

Mutua, J. (2019, November 28). *Kenya: New Rules to End SIM Card Hawking, Fraud*.

AllAfrica.Com. https://allafrica.com/stories/201911280788.html

Ngwomoya, A. (2019). *Scam rocks SIM card registration*. Daily Monitor. https://www.monitor.co.ug/uganda/news/national/scam-rocks-sim-cardregistration1852002

Oyediran, O., Omoshule, A., Misra, S., Maskeliūnas, R., & Damaševičius, R. (2019). The attitude of mobile telecommunication subscribers towards sim card registration in Lagos State, Southwestern Nigeria. *International Journal of System Assurance Engineering and Management*, *10*(4), 783–791. https://doi.org/10.1007/s1319801900809-6

PKI and Digital Certificates for Government. (n.d.). *SSL.Com*. Retrieved May 4, 2021, from https://www.ssl.com/article/pki-and-digital-certificates-for-government/

prokaza, J. (2018, April). *How does a SIM card work?* BT.Com. http://home.bt.com/techgadgets/phones-tablets/how-does-a-smartphone-sim-cardwork-the-technologybehind-sim-cards-explained-11363967555573

Safaricom Will Alert When Your ID Number is Used To Register A SIM Card. (2020, May 15). *Gadgets Africa*. https://gadgets-africa.com/2020/05/15/safaricom-alert-youidnumber-fraud-sim-card/

Sandberg, L., & Rodberg-Larsen, K. (2006). *Method for enabling PKI functions in a smart card* (United States Patent No. US7024226B2). https://patents.google.com/patent/US7024226B2/en

Santoro, P., & Claps, M. (2012). *Method and radio communication network for detecting the presence of fraudulent subscriber identity modules* (United States Patent No. US8090347B2). https://patents.google.com/patent/US8090347/en Sheng, H. (2007). *SIM card Security*. Chair for communicating Security. https://www.emsec.ruhr-uni-bochum.de/media/crypto/attachments/files/2011/04/sim_card_security.pdf

Silvester, K. (2005). *User authentication using a mobile phone SIM card* (United States Patent No. US20050221853A1). https://patents.google.com/patent/US20050221853A1/en

Waddington, R., & Wilson, M. (2019). *Understanding Capture and Validate KYC process*. GSMA.

Yi-Bing Lin, Ming-Feng Chen, & Rao, H. C.-. (2002). Potential fraudulent usage in mobile telecommunications networks. *IEEE Transactions on Mobile Computing*, *1*(2), 123– 131. https://doi.org/10.1109/TMC.2002.1038348

Appendices

Appendix 1: Survey questions

The following feedback will be used to gather insights that will be solely used for research work.

1. Are you a SIM Card Owner *

Mark only one oval.

- Yes
- No

2. If yes, How many? *

Mark only one oval.

- One
- Two
- Three
- Four and above

3. If you have more than one are they all from the same Telecommunication Company? If no please list the different Companies

_____

4. Where was the place of purchase? *

Check all that apply.

- [ ] Telecommunication's Customer care desk
- [ ] SIM Card Hawker

Other: [ ] _____

5. If other please fill below

_____

6. Have you experienced any security concern that is associated with your SIM card purchase and/or registration. If yes please explain *

_____

_____

_____

_____

_____

7. Please provide any suggestions or comments you would like us to consider with regards to fraudulent SIM registration in Kenya

_____

Appendix 2: Turn It In Report

Curiginal

Document Information

Analyzed document	Thesis.docx (D109941165)
Submitted	6/30/2021 11:26:00 AM
Submitted by	
Submitter email	Maureen.Gate@strathmore.edu
Similarity	11%
Analysis address	library.strath@analysis.urkund.com

Appendix 3: Ethical review Certificate

Strathmore UNIVERSITY

11th November 2021

Ms Gate Maureen,
maureen.gate@strathmore.edu

Dear Ms Gate,

RE: A prototype to verify Fraudukent SIMcard registration using public key infrastructure verification approach

This is to inform you that SU-IERC has reviewed and **approved** your above **SU-master's** research proposal. Your application reference number is **SU-IERC1094/21.** The approval period is **11th November 2021 to 10th November 2022.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-IERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-IERC within 48 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-IERC within 48 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to SU-IERC.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

for: Prof Fred Were,
Chairperson; SU-IERC

STRATHMORE UNIVERSITY INSTITUTIONAL ETHICS REVIEW COMMITTEE (SU-IERC)
11 Nov 2021
TEL: +254 (0)703034000
P.O BOX 59857-00200
NAIROBI-KENYA

VT OMNES VNVM SINT