

**A MODEL FOR AN INTEGRATED AND SECURE
PERSONAL IDENTIFICATION SYSTEM
(ISPIS)**

BY

JOEL KIMELI CHERUS

GDI/M/1113/09/11

A Thesis Submitted to the Institute of Postgraduate Studies and Research in Partial Fulfilment of
the Requirements for the Doctor of Philosophy (PhD) Degree in Information Technology of
Kabarak University.

KABARAK UNIVERSITY

October, 2014

DECLARATION AND RECOMMENDATION

Declaration

I hereby declare that this thesis is my own work and effort and that it has not been presented in any other university or college. Where other sources of information have been used, they have been acknowledged. The work was done under the guidance of Prof. Jason Githeko, Dr. Joseph Siror and Dr. Kageni Njagi.

Signed.....Date.....

Joel Kimeli Cherus

REG. NO: GDI/M/1113/09/11

Recommendation

The thesis entitled “*A model for an Integrated and Secure Personal Identification System*” written by **Joel Kimeli Cherus** is presented to the Institute of Postgraduate Studies and Research of Kabarak University. We have received the thesis and recommend it for acceptance in partial fulfilment of the requirement for the degree of Doctor of Philosophy (PhD) in Information Technology.

Signed.....Date.....

Prof. Jason Githeko, Thesis Supervisor
Department of Computer Science
Egerton University

Signed.....Date.....

Dr. Joseph Siror, Thesis Supervisor
Directorate of Science, Technology, Innovation and Communication
National Economic and Social Council, Kenya

Signed.....Date.....

Dr. Kageni Njagi, Thesis Supervisor
Institute of Postgraduate Studies and Research
Kabarak University

COPYRIGHT

Copyright © 2014, Joel Kimeli Cherus.
All rights reserved.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission.

ACKNOWLEDGEMENTS

Completion of this doctoral research would not have been possible without the support I got from several people. I would like to express my sincere gratitude to all of them. First of all, I am extremely grateful to my thesis supervisors, Prof. Jason Githeko, Associate Professor of Innovation and Internet Technologies at the Department of Computer Science, Egerton University, Dr. Joseph Siror, Director of Science, Technology, Innovation and Communication at the National Economic and Social Council, and Dr. Kageni Njagi, Director of Postgraduate Studies and Research at Kabarak University. I received their valuable guidance, scholarly inputs and consistent encouragement throughout my research work.

Much thanks to the staff of the School of Science, Engineering and Technology for being kind enough with their help at various phases of my research, and I do hereby acknowledge all of them. I specifically thank Prof. Jackson Kitetu, the school's dean, for accepting me as his student and according me all the support I needed. Dr. Christopher Mkirema Maghanga, the Head of Mathematics and Computing Sciences department, for not only providing me with all the necessary administrative support, but also an opportunity to teach at the university.

My data collection exercise was ridden with fewer obstacles because of the presence of a few individuals; Ken Angir, Integrated Population Registration Services (IPRS) department, Anderson Chebii, National Registration Bureau (NRB), Alex Njihia, Civil Registration Department (CRD), Dume Wanda, Department of Immigration and Inspector Wesley Lekariap, Banking Fraud Investigation Department (BFID). They assisted me a lot during my visit to their respective departments. I appreciate the generosity of Peter Kamothe on prototype development tools, Edwin Kimathi for his insightful ideas, and my employer, The Government of Kenya, for lessening my financial burden.

I am very much indebted to my family, my wife Joyce, daughters Hilda and Harriet and son Brian, who supported me in every possible way they could to see me through. I owe it all to Almighty God for granting me the wisdom, health and strength to undertake this research to its completion.

DEDICATION

This thesis is dedicated to my wife Joyce, daughters Hilda and Harriet and son Brian for being patient and understanding during my lonely struggles preparing it, and to my parents, for instilling in us the importance of hard work and education.

ABSTRACT

Personal Identification Systems are implemented to assist in identifying, authenticating and authorizing the right persons to the right entitlements. Criminals have however discovered ways of by-passing them in order to perpetrate identity fraud. As a result, the problem of identity fraud has become one of the fastest growing crimes in the world today, and a key facilitator of terrorism, money laundering and trafficking (of people, drugs, weapons and illicit material). In this study, an innovative model of a personal identification system that incorporates state of the art technologies is proposed to combat identity fraud. The system encompasses a secure integration of new and existing identification systems to provide for a real-time identity validation and verification. It can be accessed through ubiquitous devices such as smartphones and therefore can be used in a wide range of scenarios where identity checks are routinely done. Additionally, it is easy to use and free of typing-errors since users are presented with limited manual intervention. Its security architecture ensures confidentiality, integrity, availability and privacy of identity data. This design was informed by a review of literature on similar systems and the results of a survey that established the methods used by criminals to perpetrate identity fraud and the challenges facing Kenya's primary registration and identification systems. A prototype of the system was constructed and evaluated using a set of identity fraud scenarios developed from the survey results. The outcome of the evaluation demonstrated that the model is able to withstand many types of identity fraud. It is therefore recommended that countries that experience incidences of identity-related crimes such as Kenya should consider implementing the model as an alternative tool for curbing identity fraud. Future work may focus on refining the model and scaling it to a global level.

Keywords: Identity Fraud, Model, Personal Identification System

TABLE OF CONTENTS

LIST OF TABLES	x
LIST OF FIGURES	xi
OPERATIONAL DEFINITION OF TERMS	xiii
LIST OF ABBREVIATIONS AND ACRONYMS	xv
CHAPTER 1: INTRODUCTION.....	1
1.1 Background	1
1.2 Problem Statement	2
1.3 Research Objectives	3
1.4 Research Questions	3
1.5 Significance of the Study	3
1.6 Assumptions and Limitations	3
1.7 Research Contributions	4
CHAPTER 2 :LITERATURE REVIEW	5
2.1 Introduction	5
2.2 Concept of Identity and Identification	5
2.3 Identification system	6
2.4 Identification Systems in Kenya	11
2.5 Identity Fraud	24
2.6 Models of Identity Management Systems	26
2.7 Summary and Conclusion	28
2.8 Conceptual Framework	28

CHAPTER 3 :RESEARCH METHODOLOGY	30
3.1 Introduction.....	30
3.2 Research Design.....	30
3.3 Target Population.....	32
3.4 Sampling Procedure	33
3.5 Research Instruments	34
3.6 Data Collection Procedures.....	35
3.7 Data Analysis	35
3.8 Developing and Constructing the Model	36
3.9 Verifying and Validating the Model	36
3.10 Ethical consideration and Limitations	37
CHAPTER 4 :RESULTS PRESENTATION AND DISCUSSION.....	38
4.1 Introduction.....	38
4.2 Survey	38
4.3 Model Development.....	60
4.4 Model Construction	101
4.5 Model Verification.....	107
4.6 Model Validation	112
CHAPTER 5 :SUMMARY, CONCLUSIONS AND RECOMMENDATIONS	121
5.1 Introduction.....	121
5.2 Summary of Findings.....	121
5.3 Conclusion	122

5.4	Recommendations.....	123
5.5	Suggestions for Further Research	124
	REFERENCES	126
	LETTER OF INTRODUCTION	135
	APPENDIX B:	136
	LETTER OF RESEARCH AUTHORIZATION.....	136
	APPENDIX C:	137
	QUESTIONNAIRE FOR IDENTITY FRAUD SURVEY	137
	APPENDIX D:.....	140
	INTERVIEW SCHEDULE FOR ID SYSTEM SURVEY.....	140
	APPENDIX E:	143
	SAMPLE SOURCE CODE FOR THE PROTOTYPE	143

LIST OF TABLES

Table 2. 1: Distinct Birth/Death Registration Procedures	15
Table 2. 2: Similar Birth/Death Registration Procedures	16
Table 3. 1: Target Population for the Survey.....	32
Table 3. 2: Selected Participants for Identity Fraud Survey	34
Table 4. 1: Methods of Identity Fraud.	48
Table 4. 2: Background of CRD System	50
Table 4. 3: CRD Registration Process	50
Table 4. 4: CRD Data Transmission Process.....	51
Table 4. 5: CRD Data Processing Process	51
Table 4. 6: CRD Data Storage Process	52
Table 4. 7: CRD Verification and Validation Process.....	52
Table 4. 8: CRD Technology	52
Table 4. 9: CRD System Architecture	53
Table 4. 10: CRD System Security	53
Table 4. 11: Background of KENRIS System	54
Table 4. 12: KENRIS Registration Process	55
Table 4. 13: KENRIS Data Transmission Process.....	55
Table 4. 14: KENRIS Data Processing Process.....	56
Table 4. 15: KENRIS Data Storage Process	56
Table 4. 16: KENRIS Verification and Validation process.....	57
Table 4. 17: KENRIS Technology.....	57
Table 4. 18: KENRIS System Architecture	57
Table 4. 19: KENRIS System Security.....	58
Table 4. 20: Examples of Modern Data Capture Devices	95
Table 4. 21: RightViews Table Data.....	103
Table 4. 22: Birth Details Data	113
Table 4. 23: Death Details Data.....	113
Table 4. 24: National ID Data.....	113

LIST OF FIGURES

Figure 2. 1: Basic Architecture of a Smart Card.....	10
Figure 2. 2: Development of the National Identity Card	13
Figure 2. 3: Birth/Death Registration Process	14
Figure 2. 4: Sample Certificate of Birth.....	17
Figure 2. 5: Civil Registration System Architecture.....	19
Figure 2. 6: Sample National Identity Card.....	21
Figure 2. 7: Sample Alien Identity Card.....	22
Figure 2. 8: Sample Refugee Identity Card	23
Figure 2. 9: National Identity Card System High Level Architecture	23
Figure 2. 10: Conceptual Framework	29
Figure 3. 1: Research Design	31
Figure 4. 1: Card Skimming.....	39
Figure 4. 2: System Model Views.....	60
Figure 4. 3: Model Development Process.....	62
Figure 4. 4: Requirements Model	63
Figure 4. 5: Functional Requirements.....	64
Figure 4. 6: Non-Functional Requirements	65
Figure 4. 7: Use Case Model.....	66
Figure 4. 8: Use Cases	67
Figure 4. 9: Interaction Overview Diagram for Login Use Case.....	69
Figure 4. 10: Login Sequence Diagram	70
Figure 4. 11: Interaction Overview Diagram for Identify a Person Use Case	72
Figure 4. 12: Validate Identity Sequence Diagram.....	73
Figure 4. 13: Verify Identity Sequence Diagram.....	75
Figure 4. 14: Class Model.....	76
Figure 4. 15: Data Model	80
Figure 4. 16: Component Model.....	81
Figure 4. 17: Federation Manager.....	82
Figure 4. 18: Deployment Model.....	85
Figure 4. 19: Architecture of NFC-Enabled Phone	87
Figure 4. 20: Biometric Verification and Identification	88
Figure 4. 21: IdP System workflow	90
Figure 4. 22: Picture of Return Screen.....	91
Figure 4. 23: Fingerprint Enrolment	91
Figure 4. 24: Human Iris.....	92

Figure 4. 25: Iris Acquisition System	92
Figure 4. 26: Face Acquisition.....	93
Figure 4. 27: Correct Photo Capture Position.....	94
Figure 4. 28: Database Integration.....	96
Figure 4. 29: ISPIS Security Model.....	97
Figure 4. 30: ISPIS Prototype Architecture	102
Figure 4. 31: Login Form.....	104
Figure 4. 32: User Access Rights Assignment Form.....	105
Figure 4. 33: University Profile	106
Figure 4. 34: Night Club Profile	106
Figure 4. 35: Functional Requirement to Use Case Realisation	109
Figure 4. 36: Use Case to Class Realisation	110
Figure 4. 37: Class to Component Realisation.....	111
Figure 4. 38: Identity Search by a Bank Employee	114
Figure 4. 39: Identity Search by Immigration Officer	115
Figure 4. 40: Identity Search by Hospital Employee.....	116
Figure 4. 41: Identity Search by a National Registration Bureau Employee.....	117
Figure 4. 42: Identity Search by Hospital Employee.....	118
Figure 4. 43: Identity Search by Immigration Officer	119

OPERATIONAL DEFINITION OF TERMS

Actor: Is a user of the system; user can mean a human user, a machine, or even another system or subsystem in the model.

Biometric: Technologies that measure and analyse human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements

Biometric template: Representations of a fingerprint or other biometric using a series of numbers and letters.

Breeder Document: A document, genuine or fraudulent, that can serve as a basis to obtain other identification documents or benefits fraudulently.

Civil Data: These are text-based data about an individual such as name, identification number, gender, age etc.

Digital Signature: A mathematical scheme for demonstrating the authenticity of a digital message or document.

Enrolment Process: The registration of a person's identity through creation of a biographical footprint and recording of biometric data

Identity Card: A card bearing identifying data about the individual whose name appears thereon.

Identity Fraud: The deliberate use of identity deception details and/or stolen identity in the commission of crime.

Identity-related crime: All punishable activities that have identity as a target or a principal tool

Identity Theft: The theft or assumption of a pre-existing identity, with or without consent, and, whether, in the case of an individual, the person is alive or dead

Kipande: A copper chained metal container that was used to keep identity registration papers and worn around the neck by Kenyan male adults during the colonial period.

M-PESA (M for mobile, PESA is Swahili for money): Is a mobile-phone based money transfer and micro financing service used by Safaricom.

National Identification System: A mechanism used by governments to prove their residents' identities.

Personal Identification System: A mechanism used to prove the identity of a person.

Personally Identifiable Information: Information that can be used to uniquely identify or locate a person.

Safaricom: Is a leading mobile network operator in Kenya.

Smart Card: A plastic card with a built-in microprocessor, used typically for electronic processes such as financial transactions and personal identification.

State of the Art: The incorporation of new ideas and the most up to date knowledge in order to make advancements in the already existing knowledge.

Use Case: Represents a discrete unit of interaction between a user (human or machine) and the system.

User-centric: A structured way of allowing users to conceptualize, enumerate and control their relationships with other parties, including the flow of information.

LIST OF ABBREVIATIONS AND ACRONYMS

ACS	Access Control System
AFIS	Automated Fingerprint Identification System
API	Application Programming Interface
CA	Certification Authority
CRD	Civil Registration Department
DDL	Data Definition Language
DNA	Deoxyribonucleic Acid
DRA	Department of Refugee Affairs
EMV	Europe, MasterCard and Visa
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HCI	Host Controller Interface [Also “Human-Computer Interaction”]
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IIS	Internet Information Services
IPRS	Integrated Population Registration Services
ISO	International Organization for Standardization
ISPIS	Integrated and Secure Personal Identification System
IdP	Identity Provider
KENRIS	Kenya National Registration and Identification System
MIRP	Ministry of State for Immigration and Registration of Persons
NFC	Near Field Communication

NFC CLF	NFC Contactless Front End
NFC-WI	NFC Wired Interface
NRB	National Registration Bureau
PC	Personal Computer
PI	Personal Identifier
PIN	Personal Identification Number
PL	Missive
PKI	Public Key Infrastructure
OCL	Object Constraint Language
RFID	Radio Frequency Identification
SACCO	Savings and Credit Cooperative Society
SD	Secure Digital
SDLC	Software Development Life Cycle
SE	Secure Element
SIM	Subscriber Identity Module
SP	Service Provider
SQL	Structured Query Language
SSL	Secure Socket Layer
SWP	Single Wire Protocol
TAN	Tax Deduction Account Number
UICC	Universal Integrated Circuit Card
UML	Unified Modelling Language
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

1.1 Background

Contemporary forms of crimes are becoming increasingly sophisticated. Some of these crimes facilitate the commissioning of other crimes. Identity fraud is one such crime that facilitates terrorism, money laundering and trafficking of people, drugs, weapons and illicit material. Investigation into the September 11, 2001 terrorist attack in the United States of America revealed that the perpetrators used fraudulent identification documents to board the ill-fated planes (Willox & Regan, 2002). Several banks in East Africa have in the recent past lost substantial amounts of their customers' cash through identity fraud (Mumo, 2012). Law enforcement agencies have not been spared either by this new wave of crime. In January 2013, a man was arrested in Kenya for having successfully imposed himself as an assistant commissioner of the Kenyan police for more than five years (Gitonga, 2013). These examples show that today's criminals are able to fake their identities in order to perpetrate crimes without being detected.

There are systems however which have been developed to assist in identifying people. These systems have been in existence for a long time. In France, Napoleon introduced an identification system that was meant to control wages by stopping workers from moving around to find well-paying jobs (Douglas, 2011). The Nazi German's people's registration system (*Volkskartei*) was established to allow for the supervision of the entire workforce (Aly & Roth, 2004). The Chinese established an identity workbook that was meant to prevent workers from changing jobs without permission and moving from one place to the other (Shaw, 1996). The Kenya's identification system was introduced by the colonial government in 1915 when the Native Registration Ordinance was passed. The system forced male adults to carry registration certificates that were meant to assist the colonial authorities in supervising and controlling their movement and recruitment into colonial labour (Zezeza, 1992).

Personal identification systems today are determinants of entitlement to certain services, rights and obligations. They are used by financial institutions, immigration departments, security agencies, health institutions, academic institutions, among others, to fulfil these entitlements. This has in turn motivated criminals into innovating ways of compromising them in order to illegitimately enjoy the entitlements. A compromised identification system

results in identity fraud, a crime that is continuously rising and impacting negatively on the economic, political and social stability of many countries globally.

Kenya has several disparate systems that store identification information regarding citizens and all legal resident foreigners. The primary agencies running these systems include those in charge of such functions as birth and death registration, adoptions, identification and registration of citizens, registration of tax payers, licensing and registration of drivers, issuance of passports, regulation of foreign nationals, bankruptcy, health insurance, social security, divorces, health information, criminal records, refugees, education, labour, land registration, SIM registration and others. Currently, the above systems operate independent of each other (“Silo Model”). The lack of interoperability among them makes it hard for one agency to verify the authenticity of identity information from the other agencies.

1.2 Problem Statement

The world today is increasingly becoming insecure as a result of continued rise in criminal activities such as terrorism, money laundering, drug trafficking, illegal immigration and arms trafficking. Countries like Kenya have been forced to increase their budgets on security in an effort to eradicate the crimes. Weak identification systems have however allowed criminals to perpetrate the crimes without being detected. Effective personal identification systems are supposed to (1) identify, (2) authenticate and (3) authorize the right person to the right entitlements so as to prevent identity misuse.

Identity fraud is however growing exponentially the world over. In Kenya, a lot of money has been lost by financial institutions due to identity fraud. International terrorists have occasionally succeeded in by-passing identification systems and have ended up in destroying life and property. Many people have been conned using fake identification documents when buying property such as land and motor vehicles. This shows that the problem of identity fraud is huge and is affecting multiple sectors of the economy. Previous studies have attempted to suggest potential solutions to identity fraud from legal, educational and technological perspectives. However, there has been little focus on personal identification systems as tools for combating identity fraud.

The purpose of this study therefore was to develop a model of a personal identification system that is resilient, secure and capable of curbing identity fraud.

1.3 Research Objectives

The general objective of this study was to develop a model of an integrated and secure personal identification system that incorporates state of the art technologies in order to effectively combat identity fraud.

Specific Objectives

The specific objectives of this study were to:

1. Identify the methods used to perpetrate identity fraud.
2. Determine the challenges that make Kenya's personal identification system vulnerable to identity fraud.
3. Develop a model of a personal identification system that addresses these challenges.
4. Verify and validate the model.

1.4 Research Questions

The following research questions guided the study:

1. What methods are used to perpetrate identity fraud?
2. Why is Kenya's personal identification system vulnerable to identity fraud?
3. What personal identification system design would mitigate the current and expected future weaknesses of the Kenyan personal identification system?
4. How will the proposed personal identification system design (model) satisfy the requirements of its users and fulfil its intended purpose?

1.5 Significance of the Study

The study contributed valuable knowledge to the field of personal identification systems. Governments can adopt the proposed design to enhance their personal identification systems as tools for combating identity fraud, and thus improve global security and economic stability. The expected outcome of implementing this solution is a reduction in costs incurred by banks, security agencies, health institutions, revenue authorities, academic institutions and similar others in fighting identity-related crimes.

1.6 Assumptions and Limitations

It is assumed that the respondents gave honest and expert opinions during the survey. There was however a few limitations encountered during the study.

- i). The kind of responses received from the survey suggested that most people were not familiar with the way identity fraud is carried out. Further, some of the participants

interviewed were unwilling to discuss the topic openly because of its sensitivity. Therefore, it may not have been possible to identify all the methods used by criminals to perpetrate identity fraud.

- ii). The model was tested through a prototype as opposed to a real world system. The prototype may not have incorporated all the expected features of the proposed ISPIS. Therefore the prototype may not be implemented as a real world system but can only be used for testing purposes.

1.7 Research Contributions

This thesis has made a number of contributions to the research knowledge in the domain of personal identification systems:

1. *A new model of identity management system:* Though the ISPIS model was guided by identity federation during its development, it ended up as a hybrid of ‘Federated Identity System model’ and ‘Centralized Identity System model’. This new model called ‘**CHERUS ISPIS model**’ adds to the existing models of identity management systems.
2. *A tool for combating identity fraud:* Secure integration of personal identification systems has been demonstrated as an alternative tool for combating identity related crimes.
3. *Tackling privacy:* It has been shown that personal identification systems can be designed to allow users have different roles and access rights. This is likely to raise their level of adoption in countries that have traditionally been affected by issues of data privacy.
4. *Source of literature:* This thesis provides a rich source of literature to identity fraud and identification systems research community.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The aim of this chapter is to provide an overview of literature on current development in the area of identity fraud and identification systems. It begins with an explanation of the concept of identity and identification (Section 2.2) and continues to review literature on the following topics: Identification System, touching on issues of adoption, privacy and technologies (Section 2.3): Personal Identification Systems in Kenya (Section 2.4): Identity Fraud, with specific emphasis on perpetration, detection and prevention methods (Section 2.5): and Models of Identity Management Systems: ‘Siloed’; Centralized; Federated; and User-Centric (Section 2.6). It then highlights existing gaps in literature (Section 2.7) and finally presents a conceptual framework for the study (Section 2.8).

2.2 Concept of Identity and Identification

2.2.1 Identity

The Oxford English Dictionary (Oxford University Press., 2014) defines identity as “the fact of being who or what a person or thing is”. In many countries, the law recognizes two categories of persons, i.e. a “natural person” and an “artificial or legal person”. The Kenyan law confers rights and imposes obligations to both the natural and artificial person (Hussain, 2002). A natural person is a human being that has the capacity for rights and duties while an artificial person is an entity such as a corporation (office or a group of persons) created by law to whom certain legal rights and duties may be attached. Artificial persons are real or imaginary beings to which personality is attributed by law or by way of fiction where it does not exist. In the digital world, a person is represented by a collection of data about him/her (Ying, Wu, & Barbará, 2010).

A person can have multiple identities (Such, Espinosa, Garcia-Fornes, & Botti, 2011), but only one unique person can assume a given identity. The need to identify an individual is at times unnecessary. For example, it is possible for one to conduct transactions with other people without necessarily being identified (such as when buying foodstuffs in a shop). However, the need for identity arises as soon as a person has a recurring interaction with another person. In some situations, assuming a given identity entitles one to benefit from

privileges (Kemp, 2010; Pan, Winchester, Land, & Watters, 2010). To benefit from a due privilege or right, a person often only needs to prove his/her membership of a group or that he/she satisfies some requirements. For instance, to buy alcohol, all that one needs to prove is that he/she meets the legal age requirements (S. Sproule & Archer, 2010). In the modern world, people have to deal more and more with those they haven't met, and sometimes will never meet in person (Sullivan, 2009). Being able to identify the other party with strong confidence has become a precondition to many interactions in today's society.

2.2.2 Identification

Identification is "the act [or process] of recognizing or establishing as being a particular person" (Clarke, 1994). In small enough communities, individuals can identify each other by their physical characteristics or by name, but in large communities, identification is complex and requires other means (Castro, 2011). Clarke suggested three basic means of identifying human beings. The first one is "knowledge-based" identification. This is where a person is recognized by demonstrating knowledge in information he/she is expected to know. Such information may include the person's surname or personal identification number. Second is "token-based" identification, whereby a person is recognized by being in possession of some item like the passport, identity card, or a driver's license. Third is "biometric" identification, which refers to a variety of identification techniques that are based on some physical characteristics like the description of appearance, social behaviour, finger prints, retinal scans and DNA patterns.

In addition, a person may also be identified by his/her biographical information built up over time (Mills, 2007). This information is usually in form of birth registration details, education details, electoral register entries, employment history, registration of marriage, details of benefits claimed and taxes paid, insurance policies etc. The process of identification is designed to answer the question, "who are you?" (Smedinghoff, 2012).

2.3 Identification system

An identification system provides identification functionalities of registration, information storage and information revelation (Record, 2008). Such a system can be used alone or integrated with others to meet the needs of an identification scheme. Computerized identification systems are commonly referred to as 'electronic identification systems' (Castro, 2011). In this study, identification systems are referred to as "Personal Identification Systems" because the study is restricted to solutions for human identification.

2.3.1 Adoption of Identification Systems

Governments have implemented national identification systems to assist public agencies in identifying and verifying the identities of citizens who are being availed services or making public transactions (Encinas-Franco, 2005). In the recent past, China launched a plan to create machine-readable national identity cards for its citizens. India has created a unique identification number to be allocated to every citizen (Greenleaf, 2010). Mexico has rolled out a national identity smartcard for all its citizens. The card contains biometric data including a photograph, signature, fingerprints and iris scans. The U.S. government issued its citizens with electronic passports having embedded computer chip that contains personal information displayed on the data page of the passport, a digital photograph, and a digital signature. Kenya is also looking at improving its current identity card system by incorporating modern technologies. In the private sector, many companies are using identification systems to manage their employees and verify the identities of people they interact with. Some companies have issued photo identity cards to their employees for both identification and access to their premises. Similarly, academic institutions like colleges and universities issue their students with identity cards for the same purpose.

There are several studies that have been undertaken on the adoption of identification systems. Loo, Yeow, and Chong (2009) explored the extent of user acceptance of the national identity card and driving license applications that are embedded in the Malaysian multipurpose smartcard, and later investigated ergonomics issues affecting the citizens' intention to use the same card for homeland security purposes (Yeow, Yuen, & Loo, 2012). They discovered that Malaysians do not have high intentions to use the identification application mainly because of lack of understanding of its benefits, lack of facilitating conditions and lack of social support. Cofta (2008) conducted a similar study in the United Kingdom taking into consideration perceived value of privacy. They found that small alterations are required to make identification systems preserve privacy which will in turn improve their acceptance. Rissanen (2010) studied the diffusion of electronic identity card in Finland. They found that adoption of these cards for electronic transactions was quite low as compared to the existing Tax Deduction Account Number (TAN). Warren and Mavroudi (2011) conducted interviews on the perception of biometric identity cards that were meant to be used by foreign nationals in the United Kingdom and found that although the interviewees raised few objections, they were concerned about being unfairly targeted for additional

surveillance. Heichlinger and Gallego (2010) studied the roll out of electronic identity cards in Spain which were meant for physical and online authentication. They found out that the diffusion of electronic identity cards was fairly good but its use was low.

2.3.2 Security and Privacy Issues

Implementation of government identification systems has been slow in many countries because of privacy issues. Several studies have been carried out to unearth this challenge. De Hert (2008) studied the growing human rights recognition of the value of digital identity and its management. The study found that most constitutional courts agree that digital identities should be protected and secured. Borcea-Pfitzmann, Hansen, Liesebach, Pfitzmann, and Steinbrecher (2006) proposed a universally usable identity management meta-system that would enhance user privacy. They concluded that for privacy to be enhanced, identity management has to be user-controlled. Koops, Leenes, Meints, Van Der Meulen, and Jaquet-Chiffelle (2009) discussed privacy and data protection with regard to identity management systems. They concluded that systems should be designed in a way that allows privacy protection built as far as possible from the start. Kosta, Zibuschka, Scherner, and Dumortier (2008) examined an identity management system, PRIME toolbox, that has been built with privacy-enhancing technologies from a legal viewpoint. They found that such a system can assist individuals to secure themselves against technology violations and allow them to “enable upstream control of privacy rights as well as individual control”.

2.3.3 Modern Identification Technologies

Government and private sectors are pursuing the implementation of advance identification technologies such as biometrics, smart cards and digital signatures with a view to providing secure and accurate identity verification, enhancement of system security and protection of the integrity and confidentiality of information(Al-Khoury & Bal, 2007).

2.3.3.1 Biometrics

Biometric identification uses unique human characteristics such as fingerprints, iris patterns, face and hand geometry to ascertain and verify peoples' identity. This technique is more reliable in identity verification than token and knowledge-based methods (A. K. Jain, Hong, & Pankanti, 2000). When an individual is enrolled into a biometric system, his/her identifiers are captured and stored in a database. The system takes numerous

images/recordings of an individual's biological and non-biological data and subsequently consolidates them into one main image, known as the 'biometric sample'. It is from this sample that the unique features are captured and extracted and then converted to a 'biometric template', which, in turn, is used for purposes of verification and identification (Das, 2006). Each template is linked to a unique number generated during the enrolment process. The verification process aims to establish someone's claimed identity. The database containing the template of the person to be verified is searched on the basis of the unique number. Since the number is linked to the template, a one-to-one (1:1) relationship is said to exist. The identification process on the other hand looks to establish the identity of an unknown person. This means that the unique number is not known and therefore the entire database has to be searched. In such a scenario, a one-to-many (1:N) relationship is said to exist. A good example is an Automated Fingerprint Identification System (AFIS) which is used by law enforcement agencies to identify and track criminals.

Several studies have been undertaken on biometrics in relation to personal identification systems. Dettmer (2004) outlined the technology behind biometrics including face recognition, iris prints, and fingerprints and concluded that future identity cards will comprise biometric features to enhance security. A. K. J. F. N. Jain, K. (2010) proposed an automated fingerprint recognition system that would increase identification accuracy. Wayman (2008) discussed the difference between personal identity and digital identity with regard to biometric identity management. Peyravi (2010) designed a model of identity authentication using individual's biometric index, RFID and image processing.

2.3.3.2 Smart Cards

A Smart Card is defined by the Oxford English Dictionary (Oxford University Press., 2014) as "a plastic card with a built-in microprocessor, used typically for electronic processes such as financial transactions and personal identification". It was developed in 1973 by Roland Marino and introduced into the commercial market in 1981 when the French state telephone system adopted it as an integral part of its phone card network. Today, smart cards are increasingly popular in many industries such as telecommunications, banking, transportation, healthcare, insurance, and government identification systems.

The chip in the card may contain a microprocessor (usually 8 bit) and memory (RAM, ROM and EEPROM) that makes it a small on board computer itself or it may contain only memory depending on the task it has to perform. The RAM is used as a temporary buffer

during program execution. ROM stores operating system and standard routines such as encryption algorithms and communication protocols. EEPROM store application programs written in assembly language of the embedded microprocessor. Data stored in EEPROM can be changed by the microprocessor using an on-chip charge pump, eliminating the need for a separate external power supply for programming. The I/O port is primarily used for communication and authentication. Smart cards store access codes, passwords, public and private keys used in encryption and authentication (Noore, 2000). The basic architecture of a smart card is presented in *Figure 2.1*.

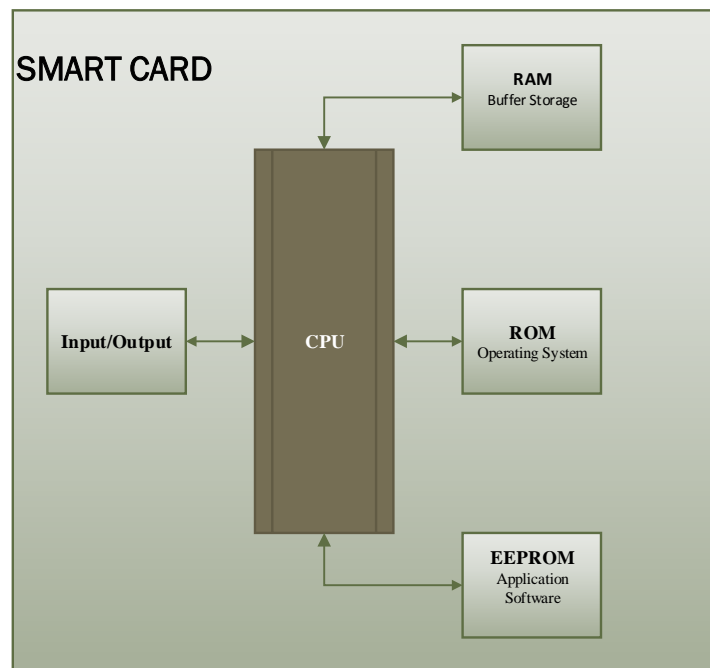


Figure 2. 1: Basic Architecture of a Smart Card

There are three types of smart cards: contact, contactless and combi cards. Contact card is the most widely used. It has to be inserted into a card reader for it to be read. Electrical contacts located on the outside of the card connect to a card reader when the card is inserted. Contactless card require only close proximity to the reader for it to be read. These cards communicate with readers via radio waves. Combi card on the other hand has a single chip that allows connection to the card reader through both contact and contactless interfaces. Their use targets such markets as banking, transport, Government and other areas where larger memory, higher security and multiple interfaces are needed.

Research in the application of smart cards in human identification is attracting a lot of interest. Kardas and Tunali (2006) developed a smart card based healthcare information for

personal identification and transfer of health data. The system uses encryption keys and digital signature keys stored on smart cards for secure and authenticated data communication between clients and database servers over distributed object protocol. Sauveron (2009) explored the evolution of smart cards and proposed open multi-application cards for the future. Hsu, Yeh, Chen, Liu, and Liu (2011) designed an online smart card-based system to address the problem of duplicate medications for outpatients visiting multiple hospitals.

2.3.3.3 Digital Signatures

Handwritten Signatures have traditionally been used in sensitive operations like banking transactions, purchase processes or contract agreements to tie down the involved parties respecting the commitments made and thus avoiding a further repudiation of the responsibilities taken (Hernandez-Ardieta, Gonzalez-Tablas, de Fuentes, & Ramos, 2013). With the shift to digital transactions, the handwritten signatures have been replaced with digital ones. Digital signature technology is one of the most secure identification methods which is created through the use of the public and private encryption process (Lincoln, 2004), commonly known as public key infrastructure (PKI). The signing party employs a key pair, wherein the sender affixes the signature using their private key and the recipient checks the signature with the public key. A digital signature is part of a message that indicates the correct source and signifies that such message has not been altered in transit. PKI requires the use of a trusted third party, namely a certification authority (CA) in order to verify that a particular person owns a specific key. Therefore PKI requires the CA to play an important role in establishing a confidential and reliable environment for digital signatures to exist. In this environment, strangers can enter into transactions with each other because each party can rely on the CA to verify identities and signatures. Rössler (2008) describe in detail how identities can be managed by electronic means and how foreign electronic identities can be incorporated into a national electronic identity framework (PKI) in order to access e-Government services.

2.4 Identification Systems in Kenya

Kenya has two primary registration and identification systems namely: The Civil Registration System and The National Registration and Identification System. The Civil Registration System was introduced by the British colonial government in 1904. It was initially meant to record the births and deaths of only Europeans and Americans, but was later

extended to Asians, and finally to Africans on attainment of independence in 1963 (Ministry of Information and Registration of Persons, 2013b). The main purpose of these recordings was to assist the government in managing health conditions and distribution of inheritance. It was mandatory that births and deaths were to be reported to a central registration office. Later on, every individual was obliged to register the events either in their places of occurrence or place of residence. Any midwife, traditional birth attendant, or physician present at the birth delivery point or place of occurrence was required by law to report the event to the local registration office. Where no such agents were present, the mother reported the event to the local chief who was then to communicate the same to the local registration office (Munene, 1994). Today, registration is done for all births and deaths that occur within the country and abroad. For each successful birth or death registration, a corresponding birth or death certificate is issued. A birth certificate is an internationally recognized and accepted instrument of identity that can be presented to any authority as evidence of facts of birth such as date of birth, place of birth, parentage and nationality. On the other hand, a death certificate is the official legal record of death. It includes information about the person who died and about their cause of death. This certificate can be used to claim life insurance benefits, pensions and to settle estate ownerships.

The National Registration and Identification System on the other hand came into being immediately the British colonial government passed the Native Registration Ordinance in 1915. The Ordinance made it compulsory for all male natives of sixteen (16) years and above to wear on their necks, a metal container that was referred to as ‘Kipande’ (Florence et al., 2007). This copper plated metal contained the holder’s registration certificate which had his particulars including fingerprint impressions. This certificate was meant to assist the colonial authorities in supervising and controlling the movement and recruitment of male indigenous Africans into colonial labour. The ‘Kipande’ was later changed into an identity card in form of a booklet that contained particulars of its holder such as name, date of birth, place of birth, colour of eyes, fingerprint impressions etc. The booklet was later replaced with a paper-based identity card that was referred to as “1st Generation Identity Card”. Today, “2nd Generation Identity Card” is being issued to Kenyans who have attained the age of eighteen (18) years. Possession of a national identity card allows an individual to vote, purchase property or even obtain employment, among other entitlements. *Figure 2.2* shows the development of the Kenyan national identity card.

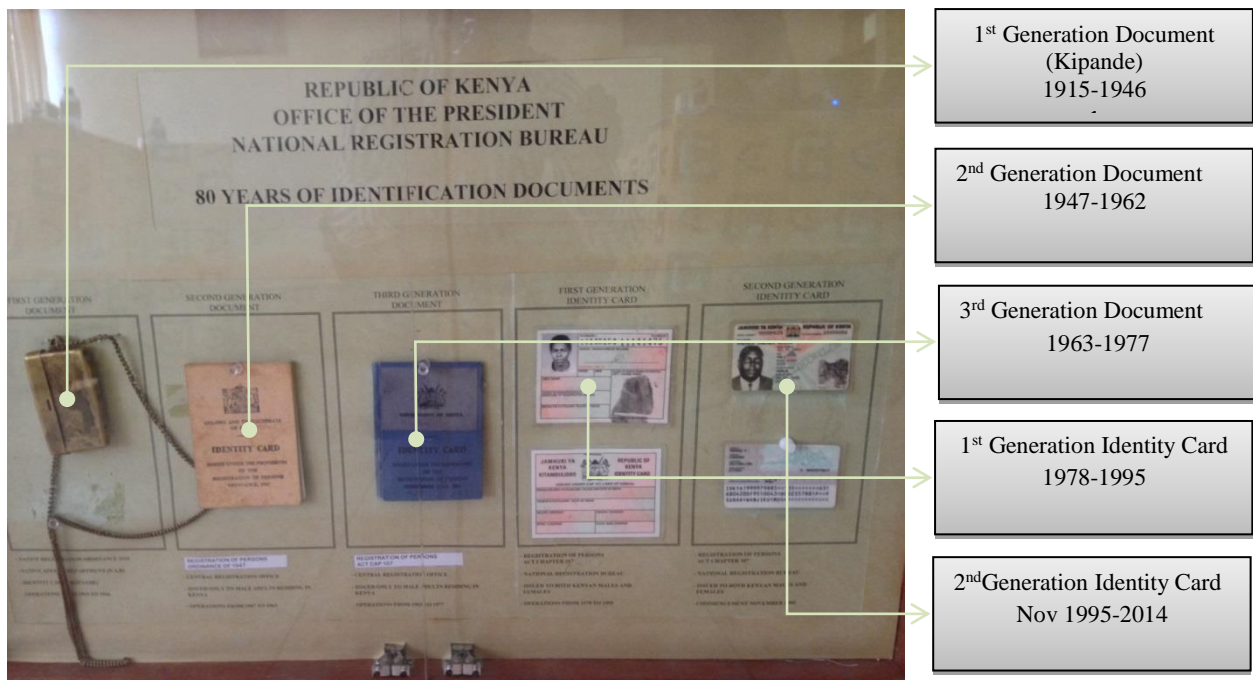


Figure 2. 2: Development of the National Identity Card

2.4.1 Civil Registration System

The Civil Registration System in Kenya is managed by the department of Civil Registration. The department is responsible for the registration of births and deaths occurring in Kenya and of Kenyan citizens occurring abroad. Birth and death data is recorded in a civil register. This register is used to generate birth and death certificates which serve as legal documents that protect civil rights of individuals. It also provides a source of data for the compilation of vital statistics.

2.4.1.1 The registration Process

The process of birth and death registration is currently semi-automated, with a large chunk of work being done manually. The registration of births and deaths follow similar procedures. However, there is a clear distinction between the procedure for registering a birth or a death which occurs at home and that which occurs in health institutions. *Figure 2.3* below illustrates this process.

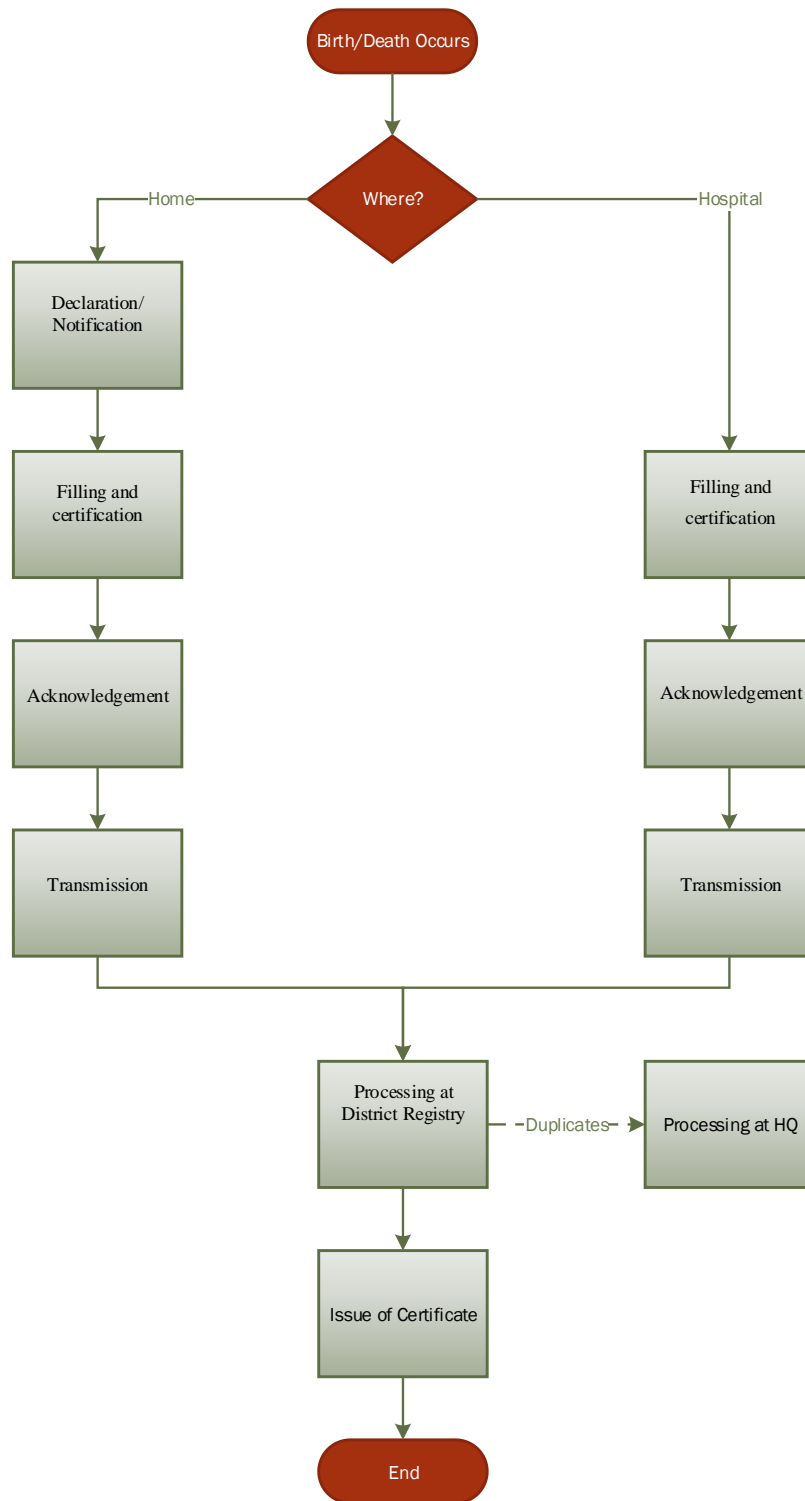


Figure 2. 3: Birth/Death Registration Process

The above procedures are described in *Table 2.1* and *Table 2.2* below.

Table 2. 1: Distinct Birth/Death Registration Procedures

Procedure	Birth/Death Occurring at Home	Birth/Death Occurring in Health Institution
<i>1. Declaration/ Notification</i>	The parents of the new born or the relatives of the deceased report the event immediately to the assistant chief who has been appointed as a part-time Registration Assistant (RA) of the sub-location of occurrence.	There is no declaration or notification for registration because the midwife or the nurse who fills the registration form is a witness in the occurrence of the event. Moreover, immediately the event occurs, the registration form is completed in the presence of the mother of the baby or the relative of the deceased.
<i>2. Filling and Certification</i>	When the RA receives the report on the occurrence of an event, he/she fills in duplicate the registration form beginning with the Register of Birth/Death. The RA then enters the name of the informant in the form and asks the latter to sign. He finally countersigns as the RA of the sub-location where the event occurred	In compliance with Health Institution procedures and practices, the function of filling of the registration forms is delegated to the midwife, nurse and doctor. These persons play the role of informant and partly that of the RA in the filling of the form. In the case of the death register however, only the doctor is authorized to fill and certify the cause of death.
<i>3. Acknowledgement</i>	Acknowledgement of Birth Notification (ABN) or the Permit for Burial (PB) is filled by copying some of the particulars entered on the register of birth. The ABN or the PB is then issued to the parent of the child or relative of the deceased or any other informant who took the report to the RA.	After the forms have been filled and signed by the midwife or the nurse and doctor, the rest of the steps are the responsibility of health institution's RA. These steps involve visiting all wards to collect all booklets of registration forms: comparing the number of filled forms with the number of births and deaths entered in the Health Institution birth and death record books: ensuring that all entries in the birth and death registers are correct: certifying the correctness of the information entered in the form by signing the space reserved for the RA: and filling and signing the counterfoils relating to the ABN and PB. Finally, the RA tears off and hands over, to the mother of baby or the relative of deceased, the ABN or PB respectively, and returns the booklets to the various wards.
<i>4. Transmission of forms to the District Registrar</i>	At the end of each month, the RA counts each category of forms (both original and duplicate) which he/she has filled for the events reported during the month. He/she then enters their numbers in a transmittal form and keeps them in an envelope awaiting the Assistant District Registrar (ADR) to come and take them to the DR.	On prescribed dates, the RA of the Health Institution transmits directly the completed forms to the DR under cover of a transmittal form which also acts as a statistical return to the DR.

Table 2. 2: Similar Birth/Death Registration Procedures

Procedure	Birth/Death Occurring at Home or Health Institution
5. <i>Follow-up of errors</i>	<p>On receiving the forms, the ADR checks whether the forms agree with the number entered in the transmittal form. He/she then checks if there are any inconsistencies in the forms or clerical errors. Some of these errors can be rectified with the RA immediately while those that require further consultations are sorted out later. The ADR prepares a statistical return which is a consolidated summary of all the transmittal forms from the sub-locations to accompany the registration forms to the DR.</p>
6. <i>Processing at the District Registry</i>	<p>The actual processing of the registers of birth and death at the district registry consists of several steps, which are essentially the same regardless of the origin of the forms. There is however minor differences with regard to the detail in some of the steps. Generally, the registry clerk counts the forms to ascertain that the number of the forms agrees with the corresponding number entered by the respective RA/ADRs in the consolidated return. If there is agreement in the numbers, the clerk acknowledges receipt otherwise he/she states any discrepancy. The registry clerk then verifies the contents of each form to make sure that there are no missing entries or illegible words, illogical/inconsistent information. If the RA, in the opinion of the clerk, can obtain the missing information or correct the inconsistent information, the clerk fills the appropriate query form to elicit the information attaching a tag on the register while he waits for the RA's reply.</p> <p>After the errors have been corrected, the clerk then enters the name of the district (using a rubber stamp), assigns a running registration number (using a hand numbering machine), enters the date of registration (using a date stamp) and enters the name of the DR (using a rubber stamp) into the form. The DR then appends his/her signature to the register. Following the DRs signature, the registry clerk separates the original documents from the duplicates. The duplicates are dispatched to the Head Office under cover of a transmittal note and accompanied by statistical returns from the DR. The duplicates received at the Head Office are counted to verify their number, put into hard cover folders and subsequently used for further data processing. Later, the duplicates are bound ready for final storage. The originals will later be sent to the Head Office for binding in exchange for the bound duplicates. Eventually, the bound originals are returned to the district registries once again in exchange for the duplicates which finally go into archive.</p>
7. <i>Issuing of Certificates</i>	<p>When an individual applies for a birth or death certificate, the district registry first looks for the corresponding register from which information is going to be extracted. This can be done by using either, serial number on the ADN/PB (which also appears on the corresponding register) or by using the date of occurrence/filling as a guide. After a complete year, computer printouts are expected to be produced which show the births arranged according to the alphabetical order of the name of the child, alphabetical order of the name of the mother, chronological order of the date of birth of the child and the serial number of the register of birth. Deaths are arranged according to the alphabetical order of the name of the deceased, chronological order of the date of death and the serial number of the register of death. Such computer printouts greatly ease the otherwise arduous task of locating a particular record.</p> <p>Following the application, the applicant is required to pay a fee for the certificate, the amount of which is entered in the application form and a receipt issued to the applicant. A typist then extracts from the register the particulars needed in the relevant certificate on which the seal of the Principal Civil Registrar has been impressed. The typing is checked and verified by a clerk, then the DR signs after verifying the related document. The certificate can then be handed over to the applicant or mailed if requested.</p>

REPUBLIC OF KENYA

CERTIFICATE OF BIRTH 0832057

Birth in the KIAMBU District in the CENTRAL Province

Entry No.		Where Born	Ndumberi	Name
Date of Birth	09-04-1983	Sex	Male	Name and Surname of Father
Name and Maiden Name of Mother				
Name and Description of Informant	Sgd. Self			
Name of Registering officer	J. M. Wanjiru (Mr.)	Date of Registration	30/07/2013	

I, W. O. Oyugi District/Assistant Registrar for Central Records Division District, hereby certify that this certificate is compiled from an entry/return in the Register of Births in the District.

CRD/CA.1875 of 30/07/2013
Auth.NO.4800/CRD of 30/07/2013

[Signature]
District/Assistant Registrar

Given under the Seal of the Director of Civil Registration on the 30 day of July, 2013

This certificate is issued in pursuance of the Births and Deaths Registration Act (Cap. 149) which provides that a certified copy of any entry in any register or return purporting to be sealed or stamped with the seal of the Director of Civil Registration shall be received as evidence of the dates and facts therein contained without any or other proof of such entry.

GPK (SP) 7229—10,000 Bks—12/2012 PN

Figure 2. 4: Sample Certificate of Birth

2.4.1.2 The certificate application process

There are different types of applications that can be made to obtain a birth or a death certificate: Child Birth Certificate, Adult Birth Certificate, Street Child and Orphan Birth Certificate and Death Certificate (Ministry of Information and Registration of Persons, 2013a).

a) Application for a Child Birth Certificate

A birth certificate application form is obtained from school Head Teacher, Assistant Chief or from the District Civil Registrar. The application form is filled and attached with an Acknowledgment of Birth Notification of child to facilitate search of the birth record at the

District Civil Registrar's office. Where the birth notification is missing, a child's clinic card that shows exact place and date of birth is attached. The completed birth certificate application form with the relevant fee is returned to the Head Teacher, Assistant Chief or the District Civil Registrar. After some few days (normally seven days) from the date of submission, the certificate becomes ready for collection at the place where the application forms were submitted.

b) Application for an Adult Birth Certificate

A birth certificate application form is obtained from the school Head Teacher, Assistant chief or from the District Civil Registrar. The application form is filled and relevant supporting documents which include clinic card or baptismal/dedication card or school leaving certificate or all if available are attached. In the absence of an existing document showing the date of birth, a letter from the Head Teacher indicating date of birth as declared during admission to school should be attached to the application. Additionally, identity cards of parents, or their death certificates if deceased or an Assistant Chief's letter if they are deceased and a death certificate is unavailable, are also required. After a few days (normally seven days) from the date of submission, the certificate becomes ready for collection at the place where the application forms were submitted.

c) Application for Street Child and Orphan Birth Certificate

For this application, committal documents from a court indicating that custody of the child has been duly granted or a letter from the Children's Department indicating that the child in question is indeed abandoned, are required. If the child is housed by an Institution such as a children's home, a letter from the institution, providing the child's history including the date of birth according to an age assessment test, must be provided. Additionally, a police report indicating where the report was made when the abandoned child was found is required before the process of certificate issuance.

d) Application for Death Certificate

It is required by Kenyan law that occurrence of a death must be reported as soon as it occurs and not later than one month after occurrence. The report is made to the area Assistant Chief's office if the death occurs at home and to the hospital personnel if the death occurs in

hospital. The Assistant chief or the hospital personnel will issue a burial permit free of charge.

If the death was registered at occurrence, a death application form is obtained from the District Registrar’s office. After the form is filled, a burial permit is attached to facilitate the search of record at the District civil Registrars’ office. For an adult, his/her national identity card is also attached. The completed birth certificate application form is returned to the District Civil Registrar, and later, a death certificate will be collected. If the death was not registered at occurrence, a late registration of death form is obtained from the District Registrar’s office. After the form is filled, relevant supporting documents including a letter from Assistant Chief where the death occurred, sworn affidavit, deceased’s national identity card, letter from the hospital where the death occurred and applicant’s national identity card are attached. The completed death certificate application form is then returned to the District Civil Registrar, and later, a death certificate will be collected.

2.4.1.3 System Architecture for Pilot Civil Registration System

The Department of Civil Registration piloted a web-based Civil Registration System. The high -level architectural of the system is as shown in *Figure 2.5*.

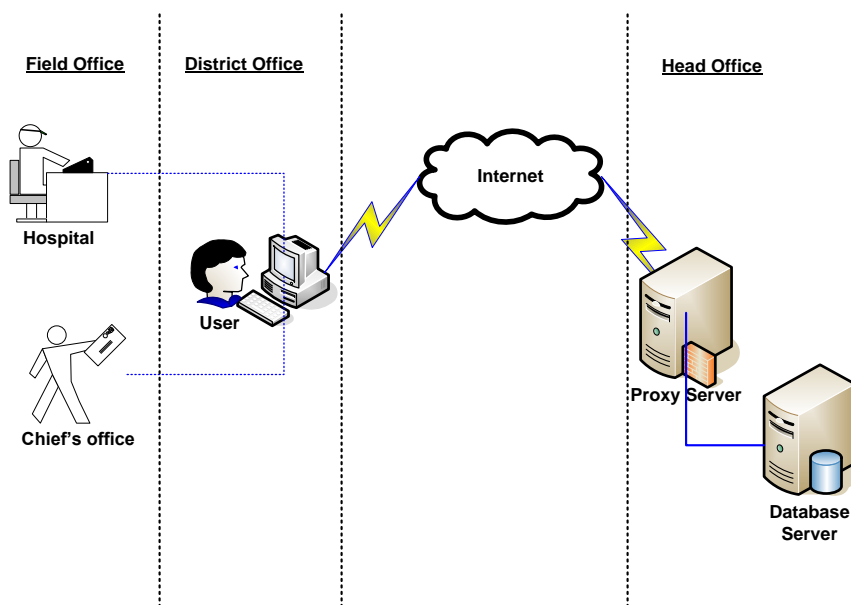


Figure 2. 5: Civil Registration System Architecture

The architecture consists of a client tier at the end user side, and a 3-tier processing server side (presentation tier, business tier and back-office tier). The client tier consists of a web

browser that has been extended with client-side application components including a VPN application. The tier interacts with a web proxy server through HTML over HTTP. The presentation tier performs formatting of processed information before returning it to the client, and for handling client requests by performing input validation and delegating them to the appropriate units within the business tier. The processed information is formatted using XML. The main infrastructural component within the presentation tier is a webserver that is connected to the application server. The business tier contains the application server. The application server implements the actual business logic. In order to achieve its functionality, the application server has been provided with several services from the back-office tier. The web server from the presentation tier interacts with the application server using remote procedure calls and web services. The back-office tier provides the database management system. SQL query language is used in requests towards the database system.

2.4.2 National Registration and Identification System

The Kenya National Registration and Identification System (KENRIS) helps in identifying, registering and issuing identity cards to all citizens of Kenya who have attained the age of eighteen (18) years and above. It is composed of three subsystems, namely: Identification System; Automated Fingerprint Identification System (AFIS); and Production System. In addition, there is an Alien interface that is used for the production of alien and refugee identity documents. The system is based on a process workflow that combines manual and semi-automated processes at the field and headquarter offices respectively.

2.4.2.1 The Registration Process

a) National Identity Card

The registration process for a national identity card is semi-automated. An applicant starts by presenting all the necessary supporting documents required to prove citizenship. These documents are parent(s) identity card(s), birth certificate, school leaving certificate and birth clinic card. After a positive identification has been done, an applicant is authorized to apply for an identity card using paper application forms. There are three types of application forms; form 136A, form 101 and form 136C. Form 136A is used to capture civil status data, form 101 is used to capture biometrics data and form 136C, which has a bar code is used to verify the issued card against stored information.

Six (6) types of application for registration can be made:- (i) *Initial Registration / Not Previously Registered* (An application meant for a citizen who has never been registered, and therefore his/her data does not exist in any identification system - currently in neither 1st nor 2nd Generation Identification System), (ii) *Replacement of 1st Generation Identity Card* (An application request for the replacement of 1st Generation Identity card with the 2nd Generation Identity Card), (iii) *Change of Particulars of 2nd Generation Identity Card* (An application to change the particulars of an applicant as a result of marriages or change of names), (iv) *Duplicate* (An application for applicants whose identity cards are lost or mutilated), (v) *Correction on Civil Status Data* (An application request to correct errors made on civil status data for applicants), and (vi) *Other Corrections* (An application requesting for corrections on photograph or fingerprints rejected in the previous application).

In the final stage of a successful registration process, the applicant is issued with a waiting card (registration certificate) and advised on when to collect the national identity card. Completed application forms are taken to National Registration Bureau's Headquarters for processing and final production of the identity card. *Figure 2.6* shows a sample of the national identity card.

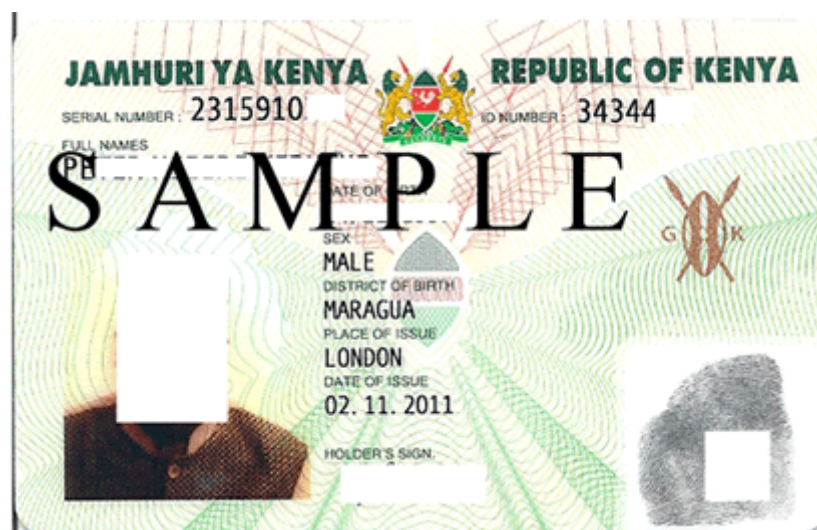


Figure 2. 6: Sample National Identity Card

b) Alien Identity Card

An Alien refers to any visitor to Kenya who is over 18 years of age and his/her stay in Kenya will exceed 90 days from the date of entry. An applicant for Alien registration presents him/herself to a registration office at the Department of Immigration with valid travel

documents. He/she is required to complete an application form, provide fingerprints and pay the necessary registration fee. The Registration office will then prepare a registration certificate to be issued to the applicant. It will also forward the application form to National Registration Bureau, which will in turn process the Alien Identity Card. When the card is ready, it will be forwarded to Immigration Department where the applicant will collect. *Figure 2.7* shows a sample of the alien identity card.



Figure 2. 7: Sample Alien Identity Card

c) Refugee Identity Card

An asylum seeker who has entered Kenya and wishes to remain within Kenya as a refugee is required to present himself/herself before a registration officer and apply to be recognized as a refugee immediately upon arrival or within 30 days of entry into Kenya. He/she is required to present himself/herself to an appointed officer who will direct him/her to the nearest reception centre, which are currently the Department of Refugee Affairs (DRA) offices at Dadaab, Kakuma or Nairobi. The Registration officer will fill the asylum seeker's information in a form and issue him/her with a waiting slip that is valid for one year until final decision is made on the asylum claim. The asylum seeker will be informed where to appear for the Refugee Status Determination Interview. The application will be considered and the decision communicated to the Asylum seeker. In case the Asylum Seeker is not satisfied with the decision by the Commissioner he/she has the right to appeal to the Appeals Board. *Figure 2.8* shows a sample of the refugee identity card.



Figure 2. 8: Sample Refugee Identity Card

Data captured during registration is processed with the assistance of computer-based systems. The process involves data verification, validation and storage. The production process culminates with the production of identity cards that must be checked for quality before being issued to their respective owners. Quality checks are undertaken at three levels: 1) Physical damage checks; 2) Text, data, photo and fingerprint visual checks; and 3) Optical Character Recognition (OCR) checks, where data printed on the machine readable zone of the card is checked for consistency with the data stored in the central database.

Each production batch containing identity cards are sorted and packed according to registration offices. Packaged identity cards and rejection statements are placed in tin boxes for dispatch to the respective registration offices where applicants will collect them.

2.4.2.2 System Architecture

The Identity Card System is an integration of three systems, namely; 1) The Civil Identification System, 2) The Automatic Fingerprint Identification System (AFIS) and 3) The Production System. *Figure 2.9* shows a high level architecture of the national identity card system.

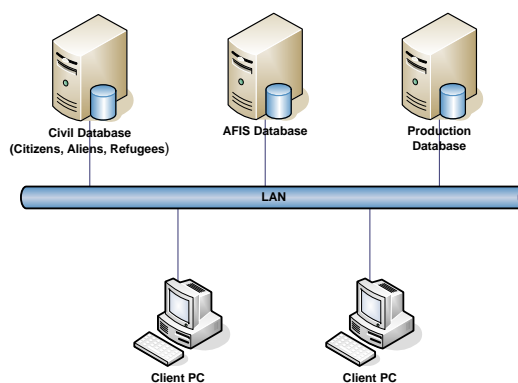


Figure 2. 9: National Identity Card System High Level Architecture

The Civil Identification System is composed of two subsystems; Citizen Identification and Alien/Refugee Identification. The Citizen Identification subsystem manages citizens' civil status data (i.e. full names, date of birth, sex, county/district/country of birth, etc.). The system generates identity card numbers for all new authentic applicants. On the other hand, the Alien/Refugee Identification Subsystem manages aliens and refugees civil status data. The records of aliens and refugees are stored in one database but are differentiated by serial numbers derived from the enrolment forms. These serial numbers are sequentially allocated in two different number ranges, one for aliens and the other for refugees. A complete application record from these subsystems is sent to AFIS for final verification.

AFIS is used to capture fingerprint impressions, perform searches and archive fingerprint images. Fingerprints are scanned from applicants' paper forms. AFIS automatically verifies the authenticity of all applications against the archived fingerprints. Authentic records are confirmed to the Civil Identification System in order to be cleared and processed further. The main objective of AFIS is to detect double and illegal registrations.

The production system is used to capture photo images, thumbprints and signatures of applicants. This data is archived in a Microsoft Windows folder. A reference field to the records in the archives is stored in the production database. The system prints, laminates and cuts identity cards for applicants whose records have been verified to be complete through a process known as "card personalization". They are then packed, ready for delivery.

2.5 Identity Fraud

Identity fraud is still on the rise despite the advancements in identification technologies, Identity fraud refers to the use of false identifiers, false identification documents or a stolen identity (identity theft) in the commission of crime (Gordon & Willox, 2003). According to Jamieson et al. (2012), identity fraud is the deliberate use of identity theft and/or identity deception details for a financial gain, avoidance of a loss, or to seek anonymity to commit identity-related crimes. The Australian Centre for Policing Research defines identity fraud as "the gaining of money, goods, services, other benefits or the avoidance of obligation through the use of a false identity and should include instances of 'skimming' (Susan Sproule & Archer, 2006)". They further observe that identity fraud is composed of identity theft which refers to "the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent, and, whether, in the case of an individual, the person is alive or dead." "Identity theft occurs when a party acquires, transfers, possesses, or uses personal

information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with fraud or other crimes (Acoca, 2009)". Other researchers have used the term "identity-related crime" to encompass both identity theft and identity fraud. These definitions agree that identity fraud happens when a real person's identity or a fictitious identity is used by another person illegally. In this study, identity fraud is defined as the deliberate use of identity deception details and/or stolen identity in the commission of crime.

2.5.1 Perpetration Methods

There are different techniques used to perpetrate identity fraud in both the online and offline environments. Some of these techniques include identity fabrication (Hopkins, 2005), phishing (Aburrous, Hossain, Dahal, & Thabtah, 2010; Eisen, 2009; McCarty, 2003), dumpster diving (Jones, 2005), forgery (Chollet et al., 2012) and exploitation of human weaknesses (Bang, Lee, Bae, & Ahn, 2012; Furnell, 2010). Phishing, which is a form of electronic identity theft in which a combination of social and technical techniques is used to trick a user into revealing confidential information (Aburrous et al., 2010), has been the most commonly used method.

2.5.2 Detection and Prevention

Several papers have suggested different ways of detecting and preventing identity fraud. Some of the proposed detection models have been designed for online environment by (Becker, Volinsky, & Wilks, 2010; Dong, Clark, & Jacob, 2010). On the other hand, solution to the problem of identity fraud has been suggested from different perspectives. Some have attempted to address it from a policy perspective (Acoca, 2009; Record, 2008). Grijpink (2004) suggested that policies on identity verification should be considered in addition to technical solutions in order to effectively frustrate and combat identity fraud. Others have proposed purely technical solutions to the problem. Li, Wang, and Chen (2011) proposed an identity matching technique that uses both personal and social identity features in order to solve the problem of identity verification. Grijpink (2005) proposed key ideas for an overall biometrics strategy that could resist identity fraud by using fingerprints stored in a database together with those on the identity document to verify one's identity. Olabode (2011) developed a distributed database model for continuous national identity registration that is intended to solve problems associated with multiple identification in a society. The model was implemented using client/server architecture. On the other hand, Deswarte and Gambos

(2010) proposed a replacement of the national identity card by a personal device that allows its user to prove some binary statements about himself while minimizing personal information leakage.

2.6 Models of Identity Management Systems

There are technical models that have been developed to assist in designing identity management solutions. Models represent the construction and working of some system of interest (Baechler, Fivaz, Ribaux, & Margot, 2011). They are operationalized through simulation because in most cases the real system cannot be engaged, or it may not be accessible, or it is being designed but not yet built, or it may simply not exist (Rebovich, 2009). A model must be verified and validated to gain grounds from which to place confidence in its results (Robinson, 1997). Verification is the process of ensuring that the conceptual model has been transformed into a computer model with sufficient accuracy (Davis, 1992); in other words, ensuring that the model has been built right. Validation, on the other hand is the process of ensuring that the model is sufficiently accurate for the purpose at hand (Carson, 1986) ; in other words, the right model has been built. According to Sargent (2007) validation is a substantiation that a computerised model within its domain of applicability possesses a satisfactory range of accuracy consistent with the intended application of the model. Giannasi, Lovett, and Godwin (2001) defines validation as the process of determining that the model on which the simulation is based is an acceptably accurate representation of reality.

There are four main models of identity management systems in use today: “Siloed”, Centralized, Federated and User-Centric Identity Systems.

2.6.1 ‘Siloed’ Identity Systems

A ‘Siloed’ identity system is one that is designed to operate independently without formal connections with other identity systems. It is sometimes called ‘isolated user identity model’ because a user has to get separate unique identifiers from each service provider he transacts with (Mannan & Van Oorschot, 2009). The model has the advantage of eliminating data corruption since user attributes in one system cannot be easily linked to different identifiers of the same users in other domains (Brisis, Mansfield, & Rundle, 2009). This model however leaves the user with a burden of having to maintain a host of login credentials for different identity systems. In most cases, users tend to forget the credentials for infrequently used

services. These identity systems lack the convenience enjoyed by linked-up systems. Providing multiple services to an individual in this model is inefficient since identity data has to be maintained in multiple accounts within an organisation. For identity systems that require confirmation of user credentials from the other system(s) in order to perform a transaction, such a model becomes ineffective. This is because a change in identity information in one system will not be known by the other dependent system(s).

2.6.2 Centralized Identity Systems

To address the inconveniences of the ‘silo’ model, a centralized approach to identity has been proposed. With this approach, identity data is held by a central credential provider that serves all the service providers (Mannan & Van Oorschot, 2009). An example is where user identity data is stored in a repository such as a directory from which service providers can have access.

2.6.3 Federated Identity Systems

In the federated model, SPs establish a central IdP who keep track of which user identifiers correspond to the same user (Brisis et al., 2009). In other words the providers share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to services. A user is able to access services by authenticating to the central IdP, which in turn informs other SPs in the federation about the authentication status. The IdP in effect becomes a trusted third party.

2.6.4 User-Centric Identity Systems

On the other hand, user-centric approach give users more control over their personal information. They choose their IdPs independent of SPs and do not need to provide personal information to SPs in order to receive services. Unlike the federated model, IdPs in this model are not part of a federation and therefore operate in the interest of the users rather than of the SPs. Users have the power to choose what information to disclose to the SPs in particular transactions, although SPs may at time require certain information for the transaction to take place.

2.7 Summary and Conclusion

This review looked at various aspects of personal identification systems with an intention of identifying gaps that offer opportunity for future research. This was in light of a growing trend in identity-related crimes and a lack of authoritative models to guide in developing secure identification systems. The review found out that a lot of research has been done on personal identification systems, but gaps still exist on: 1) The ways and methods used by criminals to perpetrate identity fraud, which need to be investigated, 2) Models, theories, frameworks, methods, techniques and tools for combating identity fraud, which need to be developed, and 3) Identification system studies in the context of developing countries, which need to be commenced. From these findings, the study embarked on a research to develop a model of an integrated personal identification system that is secure.

2.8 Conceptual Framework

The study was conceptualized from the model of identity federation. A federation is a set of system components participating in a group to coordinate sharing and exchange of information while each component retains its autonomy (Heimbigner, 1985). Each component decides what information is to be shared, which other components may participate in the sharing and in what ways the sharing is to be done. With regard to identification systems, a federation is an infrastructure connecting identity management systems from different institutions to provide standardized access to information about users from these institutions. In identity federation, every organization participating in a federation manages its user credentials through a local identity management system. A service is built on top of each local identity management system, providing a standardized interface to access authentication information and other attributes about the users. Any member of the federation can get this information by calling the service of the identity provider using a standardized protocol. Standardized Protocols are able to process the data returned by the user's home identity provider and use it to make access control decisions. Before users are allowed to use a service, they have to present a set of assertions issued by their home identity provider. These assertions are provided to users or to a service working on their behalf upon proper authentication of the user with the identity provider. *Figure 2.10* below shows the conceptual framework.

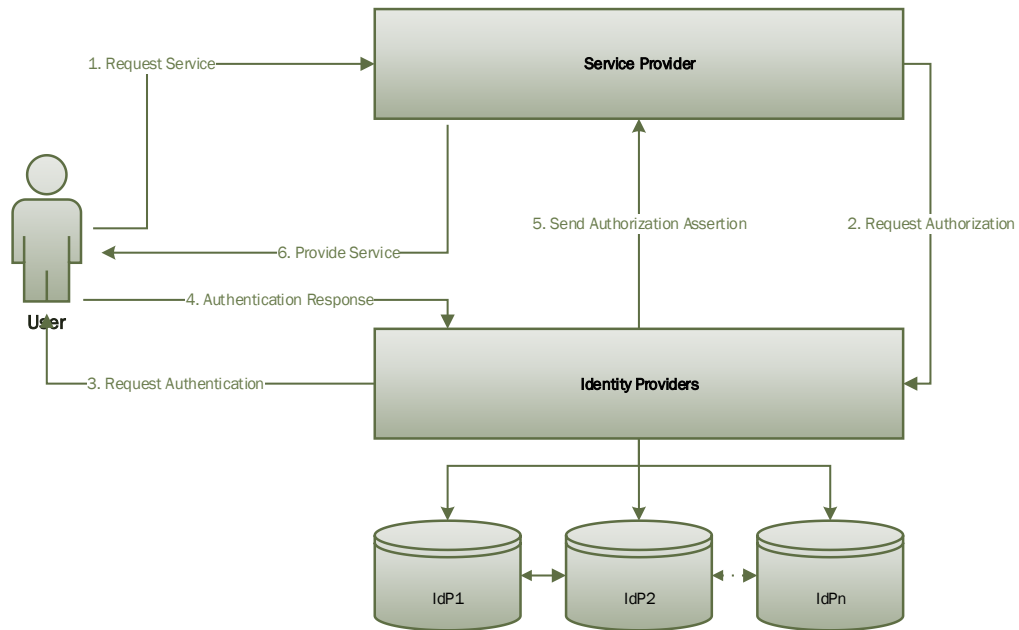


Figure 2. 10: Conceptual Framework

In this concept, a **User** requests a service from a **Service Provider (SP)**, which does not have any identifying information about him/her. The **SP** will therefore communicate with a federation of **Identity Providers (IdPs)** to obtain authentication assertions about the user. The user will be sent a request for authentication credentials. If the credentials are correct, the federated **IdP** creates a response containing confirmation of successful authentication and additional information about the user. The response is then sent to the **SP**. The **SP** verifies the validity of the response and extracts information about the user. The **SP** will then have to make an authorization decision to either let the user access the service or not. The user can access other **SPs** in the same way.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the methodology adopted for the research to achieve the objectives stated in Section 1.3 of Chapter 1. In Section 3.2, the research design is presented: Section 3.3 presents the target population: Section 3.4 describes the sampling procedure: Section 3.5 presents the instrumentation: Section 3.6 explains the data collection procedure: Section 3.7 presents the data analysis process: Section 3.8 outlines the process of model development and construction: Section 3.9 discusses the model verification and validation process: and finally, Section 3.10 discusses ethical considerations and research limitations.

3.2 Research Design

This study was conducted through a system modelling method which involves obtaining information about the behaviour of a real world system without performing real life tests on it. The method follows a series of steps that include (a) problem definition, (b) data collection and processing, (c) model development, (d) model verification and (e) model validation, to arrive at the desired solution.

The goal of the study was to develop an integrated personal identification system that is secure and capable of curbing identity fraud. Data to support the attainment of this goal was collected in two surveys. The first survey was on identity fraud in selected public and private institutions. The aim of the survey was to understand the methods used by criminals to perpetrate identity fraud. The second survey was on primary registration and identification systems. It was aimed at identifying their weaknesses in order to craft requirements for an effective personal identification system. The outcome of the surveys guided in designing the model. The model was developed and constructed using relevant software tools. It was then verified through a requirements traceability (relational) matrix together with expert knowledge and validated using the constructed prototype. *Figure 3.1* below summarizes the research design.

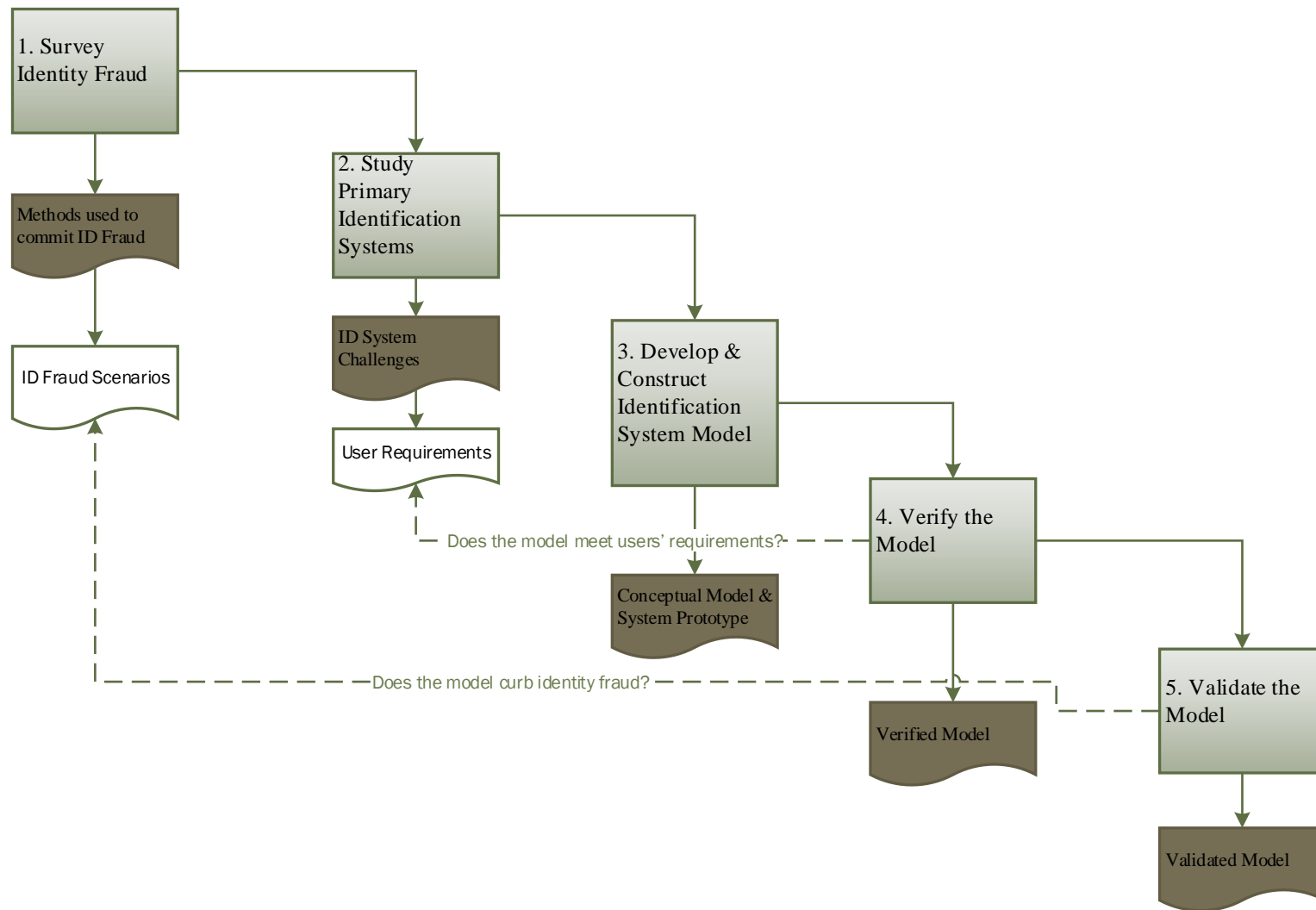


Figure 3. 1: Research Design

3.3 Target Population

The study targeted institutions within Nairobi County that were concerned with issuing the frequently used identification documents. The institutions and the document(s) they issue are presented in *Table 3.1* below.

Table 3. 1: Target Population for the Survey

	ID Document	Classification by IPRS	Issuing Institution	Institution Sector
1.	National ID Card	Primary	National Registration Bureau	Security
2.	Alien ID Card	Primary	Department of Immigration	Security
3.	Refugee ID Card	Primary	Department of Refugee Affairs	Security
4.	Birth Certificate	Primary	Civil Registration Department	Security
5.	Death Certificate	Primary	Civil Registration Department	Security
6.	Marriage Certificate	Primary	State Law Office	Legal
7.	Passport	Primary	Department of Immigration	Security
8.	Driving Licence	Secondary	Kenya Revenue Authority	Finance
9.	Log Book	Secondary	Kenya Revenue Authority	Finance
10	NSSF Card	Secondary	National Social Security Fund	Labour
11	Election Card	Secondary	IEBC	Political
12	Title Deed	Secondary	Ministry of Lands	Property
13	Medical Insurance Card	Tertiary	Medical Insurance Companies (NHIF, CIC, Jubilee, etc.)	Health
14	ATM Card	Tertiary	Banks	Finance
15	Student ID Card	Tertiary	Schools	Education
16	Academic Certificate	Tertiary	Universities, Colleges, KNEC	Education
17	Employment ID Card	Tertiary	Multiple	Multiple
18	SIM Card	Tertiary	Mobile Operators (Safaricom, Airtel, Orange, Yu)	Telecom
19	Certificate of Good Conduct	Tertiary	National Police Service	Security

The Institutions (Agencies) classified as ‘primary’ are those that were earmarked by IPRS department as the principal sources of identity registration data for its central database. ‘Secondary’ institutions were those that would use the data to verify the identities of people they intend to register in their local databases and at the same time update the central IPRS database with the data they collect. ‘Tertiary’ institutions were those that would only use the IPRS database for identity verification.

3.4 Sampling Procedure

A random sampling method was used to select the institutions to be surveyed. This choice was informed by the sensitive nature of fraud-related research. Early research has shown that most institutions are unwilling to discuss issues of fraud with third parties for fear of tainting their corporate image. Hence in this study, the researcher chose the institutions that were accessible and had reported incidences of identity fraud. These institutions were:-

- 1) *Banking Fraud Investigations Department (represents banks) - Financial Sector,*
- 2) *Department of Immigrations - Security sector,*
- 3) *Safaricom Limited - Telecommunication Sector, and*
- 4) *National Hospital Insurance Fund - Health Sector*

The sample for registration and identification systems' survey was picked from the primary agencies as defined by IPRS. Thus, *Civil Registration Department* and *National Registration Bureau* were selected. Though Immigration Department is categorized as a primary agency, preliminary investigation established that it suits more to the description of a secondary agency. The institutions responsible for issuing Alien ID cards and Refugee ID cards were left out because their identification systems were being managed by the National Registration Bureau.

The selection of participants from the sampled institutions was based on their roles. Those selected for the identity fraud survey were employees who work in legal, risk management, fraud investigation and/or security departments. Preliminary investigation had established that these departments were responsible for handling issues to do with fraud. On the other hand, system administrators and system users were selected as participants for the survey on registration and identification systems. This was informed by the fact that system administrators understand the technical design of the system they administer as well as its implementation and functional weakness/challenges. The users on the other hand understand the strengths and limitations of the system from its usage perspective. *Table 3.2* shows the participants selected for the survey on identity fraud.

Table 3. 2: Selected Participants for Identity Fraud Survey

	Institution	Survey on	Participants Selected	Total No. of Participants Per Institution
1.	Banking Fraud Investigations Department	Identity Fraud	2 – Fraud Investigators	2
2.	Department of Immigration	Identity Fraud	1 – Investigation officer 4 – Immigration officers	5
3.	Safaricom Limited	Identity Fraud	1 – Risk Management Officer 4 – M-PESA agents 4 – Customers	9
4.	National Hospital Insurance Fund	Identity Fraud	1 – Legal officer 1 – Security officer	2
Sub-Total				18
5.	Civil Registration Bureau	Registration and Identification System	1 – System Administrator 3 – Users at Head Office 2 – Users at Field Office	6
6.	National Registration Bureau	Registration and Identification System	1 – System Administrator 3 – Users at Head Office 2 – Users at Field Office	6
Sub-Total				12
Total Number of Participants				30

3.5 Research Instruments

Questionnaires and interview schedules were used to obtain data from the respondents. Structured questionnaires with open-ended and closed-ended questions were used to collect data for the identity fraud survey. The questions were divided into two sections: Background Information and Identity Fraud, and were arranged in such a way that the easy to answer ones were put in the beginning and the difficult ones towards the end. These questions were designed to capture data in line with objective one of the study. Interview schedules were used to obtain data from the survey on personal registration and identification systems. They were divided into five parts with each part having specific questions to a particular component of the system. The schedules captured data in line with objective two of the study. The data collection instruments were scrutinized by a group of experts with the aim of testing their validity before use. On the other hand, their reliability was tested through a pilot study that was undertaken in two institutions.

3.6 Data Collection Procedures

A number of data collection procedures were adopted in this research as described in subsections 3.6.1 and 3.6.2.

3.6.1 Identity Fraud Survey

A total of eighteen (18) participants were involved in this survey. They were sent electronic questionnaires with instructions on how to fill and return them back. By the end of one month, only six (6) participants had managed to return. The responses in these questionnaires were however shallow and incomplete. A second strategy that involved booking an appointment with each participant for face-to-face interview was employed as an alternative. The participants were asked the same questions on the questionnaire but in a semi-structured way. The interviews took an average of 40 minutes.

3.6.2 Personal Registration and Identification System Survey

Twelve (12) members of staff from the departments of Civil Registration and National Registration Bureau participated in the survey. Two (2) of them were system administrators and ten (10) were system users. Interviews were conducted at the departments' headquarters and field offices with the guidance of an interview schedule. The system administrators were asked to describe the functionality of their respective systems and the corresponding technology infrastructure. Users on the other hand were asked to narrate their day to day interaction with the system. Both the administrators and users were also asked to identify the challenges that contributed to the ineffectiveness of their respective systems. Though there were no comprehensive technical and user manuals for the systems, in-house developed documents were availed for the study. These were mainly reports on the system that had been prepared by consultants and system manuals prepared by internal system administrators.

3.7 Data Analysis

Data collected from the surveys was checked for completeness, consistency, accuracy, and uniformity. That from identity fraud survey was analysed through thematic content analysis. This involved discovering themes in the interview transcripts and attempting to verify, confirm and qualify them by searching through the data and repeating the process to identify further themes

and categories. The interviews were transcribed verbatim and then the researcher read each transcript and made notes of short phrases that sum up what is being said in the text. The aim was to offer a summary statement that was discussed in the transcript. An initial coding framework with a list of themes was first developed. By applying analytical and theoretical ideas developed during the research, these themes were further refined and reduced by grouping them together. This reduced list formed the final category system that was used to produce a list of the methods used to perpetrate identity fraud.

Data from the survey on identification systems was categorized according to issues of system background, system functionality, technology, system architecture, and system security. The answers provided by the interviewees in each category were then analysed by comparing them with preferred system requirements. This enabled the identification of gaps in each category. The gaps were extracted and further analysed to produce a list of challenges hindering the systems from curbing identity fraud.

3.8 Developing and Constructing the Model

The output from the surveys assisted in developing the model. The actual design was done using Enterprise Architect modelling software and Microsoft Visio Professional. The task started with a critical analysis of the survey outputs. This analysis assisted in understanding the needs of the intended system. Appropriate architectural patterns were then defined and choices on the core technologies and architectural elements of the system were made. With the guidance of SDLC methodology, the model was finally developed. It was then constructed on ASP.NET platform using Microsoft Visual Studio and related software tools. The details of the model are provided in Section 4.3 and Section 4.4.

3.9 Verifying and Validating the Model

The results of the survey on registration and identification systems were used to develop requirements for the desired system. The actual development of the model passed through a series of iterative tests before all the user requirements were satisfied. A system prototype was then designed, built and taken to a selected group of users for evaluation. The users critiqued the prototype until a desired one was finally produced. The results of identity fraud survey on the other hand were used to develop scenarios for validating the model.

3.10 Ethical consideration and Limitations

Data collection for this research involved asking participants to volunteer information some of which was deemed sensitive to their work. Participants were however assured that their participation would be treated in confidence and that the data collected would be used for academic purposes only. The study therefore did not include any information deemed to jeopardize the security of the participants. However, a limitation of this is that the validity of the results might have been threatened.

CHAPTER 4

RESULTS PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter presents the results of the study. The purpose of the study was to develop a model of a personal identification system that is resilient, secure and capable of curbing identity fraud. The researcher identified the methods used by criminals to perpetrate identity fraud and established the challenges that make Kenya's identification systems vulnerable to fraud (Section 4.2). These findings together with those from the literature review were used to develop the model (Section 4.3). The model was prototyped using modern software development tools (Section 4.4). It was then verified through a requirements traceability (relational) matrix and common logic (Section 4.5) and validated using the constructed prototype (Section 4.6).

4.2 Survey

Data was collected in two surveys. The first survey was aimed at identifying the methods used by criminals to perpetrate identity fraud while the second one was intended to establish the challenges that make Kenya's identification systems vulnerable to identity fraud.

4.2.1 Identity Fraud Survey

This survey was undertaken at the Banking Fraud Investigations Department (BFID) of the Central Bank of Kenya, Department of Immigration (DOI), Safaricom Limited and the National Hospital Insurance Fund (NHIF).

4.2.1.1 Banking Fraud Investigations Department

The survey established that BFID is charged with the responsibility of investigating financial crimes, recovering stolen money and providing fraud-related advisory services to commercial banks. It also revealed that bank customers can deposit and withdraw money Over the Counter, at Automated Teller Machines (ATM) or using mobile devices. However, criminals were said to have devised fraudulent ways of stealing money from the bank. They mainly used

skimmed ATM cards to make illegitimate cash withdrawals and stolen personal documents to apply for undeserved loans.

(i). Use of skimmed ATM cards to carry out illegitimate cash withdrawals

It was reported that bank customers occasionally lose their money through ATM card skimming. This is a technology driven fraud carried out on automated teller machines. It is a way of obtaining details of an ATM card with the intent of cloning the card and stealing money associated with it. Normally, a fraudulent card stripe reader is attached to a publicly accessible ATM in order to gain unauthorized access to the contents of the magnetic stripe, and a hidden camera is mounted to illegally record a user's authorization code (PIN). The data recorded by the camera and the fraudulent card stripe reader is subsequently used to produce duplicate cards that can be used to make ATM withdrawals from the victim's bank account. Figure 4.1 shows how skimming is carried out on an ATM machine.

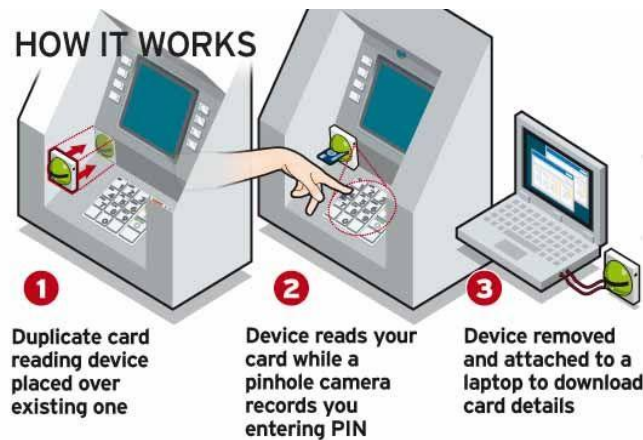


Figure 4. 1: Card Skimming

One of the BFID officials who was interviewed during the survey gave a story of a bank customer who lost money in his account through card skimming. Below is an excerpt from the interview:

Researcher: Describe how the bank customer lost his Kshs. 70,000 in his account.

Respondent BFID01: The customer was a Nairobi resident who had travelled to Nakuru to attend a seminar. While in Nakuru, he decided to visit an ATM machine with the intention of

withdrawing some cash. On inserting his debit card to the ATM slot, he was shocked to find out that there was no money in the account. The customer then printed out a mini statement from the ATM and found that two withdrawals had been done from another ATM in Nairobi's Westlands area. He informed the bank of the incident and was advised to wait for an investigation to be carried out. After the investigation, the customer was informed that there was a fraudulent activity in the Westlands' ATM machine, and therefore he would be refunded his money.

(ii). Use of stolen/lost personal documents to apply for a loan

It was also reported that some criminals were able to obtain information about bank customers and thereafter use the information to apply for identity cards, bank accounts and credit in that person's name. They steal breeder documents such as birth certificates and then use them to acquire national identity cards, passports or any other identification documents.

A second BFID official narrated an incident of impersonation that happened to a teachers SACCO. Below is an excerpt of the interview:

Researcher: What other incidences of identity fraud have you come across?

Respondent BFID02: An identity fraud in a SACCO. A legal officer reported a case of fraud that happened at their teachers SACCO. She said that a fraudster who had impersonated himself as one of its members benefited from an illegitimate loan. The fraudster applied for a SACCO loan using documents of one of the members. This fraudster had stolen the member's national identity card and payslips. He also swapped the member's SIM card to allow him receive calls and messages destined to the SIM card number. He then opened a bank account with the stolen national identity card and applied for a SACCO loan attaching copies of payslips and national identity card as required. The SACCO approved the loan and then contacted the applicant through a phone to confirm his application details. The fraudster was able to receive the call. He confirmed the details which included the bank account information. After confirmation, the SACCO deposited the money to the fraudster's account.

4.2.1.2 Department of Immigration

The survey established that the Department of Immigration has two main functions: issuing of travel documents; and controlling and regulating entry and exit of all persons at the airports, seaports and land border posts. It further revealed that the main document issued by the department is the passport. This is an internationally recognized travel document that certifies the identity and nationality of its holder. Any person applying for a Kenyan passport is required to provide documentary evidence of citizenship i.e. original & copies of birth certificate and national identity card, or a certificate of naturalization or registration and renunciation certificate of former citizenship. The application must be recommended by a Kenyan citizen, and preferably a minister of religion, a legal practitioner, an established civil servant or a bank official personally acquainted with the applicant, but not by immediate relatives. The recommender must attach a copy of his/her national identity card or passport. For an applicant who is below the age of eighteen (18) years, a parent's or legal guardian's written consent is required, and for an applicant who is adopted, the original adoption certificate, clearance letter from the children's department, and or, the court ruling or award is required.

It was reported that any person entering into Kenya reports his/her arrival to the immigration officer at the point of entry. He/she must complete an entry declaration form and personally deliver it to the immigration officer. The immigration officer examines the passport and upon being convinced, stamps it and allows the traveller into the country. On the other hand, a person travelling outside the country fills in a departure declaration form and hands it to the immigration officer together with the passport. The officer will examine the validity of the passport and after getting satisfied, allows the traveller to proceed with the journey. Criminals have however discovered ways of bypassing the immigration system. They use (i) stolen or lost breeder documents to apply for passports, (ii) look-alike passports to travel, and (iii) altered passports to travel.

(i). Use of stolen/lost breeder documents to apply for a passport

An immigration officer revealed that criminals were using lost identity documents such as national identity cards to acquire genuine passports. This revelation came out during an interview with the immigration officer as shown below:

Researcher: Briefly describe how identity fraud was carried out.

Respondent DOI01: A foreign national collected a lost Kenyan national identity card and used it to apply for a birth certificate. The unsuspecting government official at the Department of Civil Registration issued the foreigner with the birth certificate. The certificate and the national identity card were then used by the foreigner to successfully apply for a passport, which was later issued to him.

Researcher: Does it mean the fraudster had used the passport to travel elsewhere?

Respondent DOI01: Yes.

(ii).Use of look-alike passport to travel

It was also reported that criminals could steal passports and sell them to persons who resemble the photo on the passport. This was revealed by one of the immigration officers through the following interview excerpt.

Researcher: How did identity fraud happen in your case?

Respondent DOI02: A person was arrested at Jomo Kenyatta International Airport for having used a stolen passport to travel abroad. It was not easy to detect the fraud since the photo on the passport resembled the fraudster's face.

In a similar incident, an investigation officer at the Department of Immigration narrated an incident in which a man was arrested at Jomo Kenyatta International Airport for attempting to travel with his sister's British Passport. Below is the interview excerpt of the same:

Researcher: You said a man was using a lady's passport?

Respondent DOI03: Yes, a Kenyan lady who had immigrated to Britain and got married to a British citizen in the 1980's attempted to smuggle her brother into Britain using her British passport. She had sent him the passport through the Post Office so that he could use it to travel. On the day of travel, the man dressed like a lady and armed with her sister's passport managed to successfully pass through the immigration desk at the airport. On approaching the waiting lobby,

a police officer noticed ‘her’ manly walking style. She stopped ‘her’ only to realise that ‘she’ was indeed a man.

(iii). Use of altered passport to travel

It was also revealed that details of a stolen or lost passport can be altered to suit the identity of a fraudster. The alteration is done using machines that are capable of erasing original passport details and replacing them with new ones which look equally original. For example, in the following interview excerpt, it is clear that passport details can be altered.

Researcher: Any other fraud incidences?

Respondent DOI04: Yes, a fraudster was arrested for being in possession of a forged passport. He had managed to alter personal details (i.e. full name, date and place of birth, photograph and signature) on the passport and replaced them with his own.

A similar incident was reported by an immigration security officer. This is what he narrated during the interview.

Respondent DOI05: A person was arrested for being in possession of two passports bearing different personal details, but having the same photograph. He was planning to leave the country for unknown reasons.

4.2.1.3 Safaricom Limited

The survey targeted Safaricom’s M-PESA service. It was reported that M-PESA service is utilized by most people in Kenya to transfer funds amongst themselves in a quick and easy way using their mobile phones. The fund recipient collects the cash by going to any M-PESA agent, entering a secret code and showing an identification document. All M-PESA customers are registered through an agent, usually a cell phone dealer, gas station, chemist, supermarket or shop. During registration, a customer gives the agent his/her mobile number, full name, date of birth, and a copy of an identification document. The accepted identification documents include a

Kenyan National Identity Card, a Passport, a Military Identity Card, a Diplomatic Identity Document or an Alien Identity Card.

Since the introduction of M-PESA service, Safaricom was said to have received a dozen complaints on its misuse. These complaints were mainly about the loss of their customer's money to anonymous criminals.

(i). Registration of M-PESA accounts using forged identity documents

Forged identity documents were said to have been used by some individuals to register themselves for M-PESA service. During an interview with an M-PESA customer, it was established that fraudsters usually impersonate a person that is influential on a highly demanded service such as employment. This can be exemplified by an incident that befell an M-PESA customer as shown in the following interview excerpt:

Researcher: Describe how identity fraud was carried out and how it was discovered.

Respondent SAF01: I was introduced by my neighbour to someone who claimed to have connections with a recruitment officer at the Kenya Wildlife Service (KWS). My neighbour knew that I had two children who had completed high school and were interested in joining the military. I had a chat with the contact of the recruitment officer whom I informed of my desire to have my children join KWS. He gave me the cell phone number of the recruitment officer. When I talked to the recruitment officer over the phone, he indeed confirmed that he was a retired Major from the Kenya Defence Forces and currently works with KWS. He went ahead to say that I could confirm his identity from Safaricom's M-PESA service by sending 100 shillings to his phone. I did this and got a reply message showing that his name was indeed having a title of a "Major". I was convinced that he was a recruitment officer and quickly embarked on discussing the requirements for the recruitment process. He gave me a brief highlight of the requirements, of which according to him, did not matter. What mattered was the size of my pocket. We therefore agreed that I pay KShs. 60,000 for each of my children. I saw this as a dream come true, and went ahead to send him the amount through M-PESA. On receipt of the money, he called me back and said that I should take the 'recruits' to Nairobi in exactly two weeks' time. When I reached Nairobi, I called the Major only to hear that his phone was

unreachable. I tried calling him several times, but to no avail. I then sought assistance from the police who later informed me that there was no such person in KWS.

(ii).Using fake MPESA messages to defraud agents/customers

The survey found out that fake messages presumed to be from M-PESA system are sent to unsuspecting persons with the intention of defrauding them. An M-PESA agent gave a story on how they lost KShs. 30,000 to a fraudster as shown in the following interview excerpt:

Researcher: Have you ever lost money to a fraudster?

Respondent SAF02: Yes.

Researcher: Describe how you lost it.

Respondent SAF02: About 2.00PM, a lady and a gentleman who looked to be in their mid-twenties visited an M-PESA outlet, claiming to be Safaricom supervisors. The two wore valid looking M-PESA badges and even carried M-PESA promotional material for the outlet. The two inspected the outlet's log books then left. About 20 minutes after the purported supervisors left, an old looking man estimated to be at his late 50s or early 60s came to the same outlet requesting to withdraw Ksh.35, 000. The man was allowed to withdraw the desired Kshs. 35,000 and went ahead to initiate the withdrawal from his phone, as is the normal procedure. Shortly after, the outlet attendants received an SMS purporting to record and authenticate the old man's withdrawal transaction. The SMS received by the attendant had a valid looking M-PESA transaction number and the old man's purported names which were verified against an original national ID which he presented.

The M-PESA attendant, convinced about the validity of the transaction (just like hundreds of others processed daily) gave the old man an initial Ksh. 30,000 and was reaching out for the remaining Ksh. 5,000. Before the extra amount could be retrieved, the old man calmly signed the outlet transaction and walked away saying he would come for the remainder later. The M-PESA attendant continued with the next customer, expecting their float to have increased by Ksh. 35,000 as a result of the withdrawal. The expected float was then not reflected in the valid M-PESA SMS after the next customer's transaction – raising a red flag to the M-PESA attendant.

The M-PESA attendant shortly after, called 234 (Safaricom's M-PESA service line) for clarification and the service support person on the other end reported that the transaction withdrawing Ksh. 35,000 was not reflected in the M-PESA system. Alarmed at the Safaricom claim, the M-PESA attendant frantically attempted to call out for the old man who had disappeared by then without a trace. Late in the afternoon, the M-PESA agent went to the police station to report the incident. The police officers took initial details and promised to visit the outlet the following day for further investigations.

An analysis on the above incident suggests that the conman might have had access to the agent's phone and was able to create a contact in the phone book by the name MPESA. He/she then edited a normal M-PESA message and sent it as a normal SMS to the dispensing phone. Below is an example of a message that might have been received by the agent's phone.

*'P47DT685 confirmed.
on 01/2/2010 at 2.20PM
Give Ksh35, 000 to CUSTOMER1
New M-PESA balance is Ksh42, 049 Sender:
MPESA +254771831462'*

4.2.1.4 National Hospital Insurance Fund

It was established that the Fund's core mandate is to provide medical insurance cover (hospitalization cover) to all its members and their declared dependants (spouse and children). This mandate ensures that formally employed salaried people contribute to the Fund through their employers. For those in the informal sector and retirees, membership is open and voluntary. All Kenyans who have attained the age of 18 years and have a monthly income of more than KShs. 1,000 are eligible for membership. The Fund pays a rebate to service providers who serve its members. The rebate is a reimbursement rate payable to contracted providers based on their types of contracts. Currently, the rebate reimburses hospitals for providing in-patient and out-patient services to members. The survey found out that impersonation, data alteration and forgery were the main methods used to perpetrate identity fraud.

(i). Impersonating an NHIF member

One of the respondents explained how fraudsters were able to access medical services for free. They do so using genuine stolen medical cards. This is exhibited through the following interview excerpt:

Researcher: Have you come across an incident of identity fraud at your work place?

Respondent NHIF01: Yes, in fact I have seen patients enjoying NHIF benefits upon hospitalization by pretending to be spouses or children of genuine members. They use members' NHIF cards to settle hospital bills. This has resulted into a loss of several millions in NHIF.

(ii). Backdating of NHIF member's registration date

It was also discovered that some employees of NHIF were colluding with criminals to defraud the Fund. One of the respondents explained how these employees circumvent the Fund's policies so as to assist the fraudsters. This is exemplified in the following interview excerpt:

Researcher: You said employees misuse policies, what exactly do you mean?

Respondent NHIF02: The NHIF policy stipulates that members will qualify for health benefits after contributing for a minimum period of six (6) months. However, there are some who despite having not completed the six month period of contribution enjoy the benefits. Such members collude with the Fund's employees to assist them backdate their dates of contributions.

(iii). Use of forged NHIF member's card

It was also reported that forged NHIF cards were used to access NHIF benefits at the hospital. This is evident from the following interview excerpt:

Researcher: What other type of fraud has been reported?

Respondent NHIF03: Card forgery fraud.

Researcher: How?

Respondent NHIF03: Forged NHIF cards have been used to access NHIF benefits at the hospital. These forged cards are exactly the same as the original ones only that the photo is replaced with that of the fraudster.

The survey established that NHIF was providing government employees and their dependants with both inpatient and outpatient medical covers. Each employee could only use up to a certain amount of money to access medical services depending on his/her job group. One of the scheme's members narrated an incident in which someone fraudulently accessed her benefits. This is exemplified in the following interview excerpt:

Researcher: How did they exhaust your medical cover allocation?

Respondent NHIF04: I had used the cover for only two times as an outpatient and the total amount spent were far below my allocation. During my third visit to the hospital, I was informed that my allocation had already been exhausted. I therefore requested for a print out of my expenditure from NHIF and was surprised to find out that someone had used my card to access treatment from a number of hospitals.

The themes discussed above can be categorized according to their similarities. The resultant categories define the main methods that were used to perpetrate identity fraud as presented in Table 4.1.

Table 4. 1: Methods of Identity Fraud.

Method of ID Fraud	Short Description	Themes from Discussion
1. Identity Theft	Unauthorized use of someone else's identity information with an intention of committing a fraud	<ul style="list-style-type: none"> • Use of stolen/lost personal documents to apply for a loan • Use of stolen/lost breeder documents to apply for a passport • Use of look-alike passport to travel • Impersonating as an NHIF member
2. Identity Fabrication	Creation of a fictitious identity	<ul style="list-style-type: none"> • Registration of M-PESA accounts using forged identity documents
3. Identity Manipulation	Illegal modification of an identity document such as an ID card for the purpose of facilitating a fraud or deliberate change of some key identity information such as passport photo or number	<ul style="list-style-type: none"> • Use of forged NHIF member's card • Use of altered passport to travel
4. Data Manipulation	Unauthorized editing of stored identity data with an intention of committing a fraud	<ul style="list-style-type: none"> • Backdating of NHIF member's registration date
5. Phishing	Unauthorized acquisition of personal information for purposes of identity theft	<ul style="list-style-type: none"> • Use of skimmed ATM cards to carry out illegitimate cash withdrawals
6. Social Engineering	Psychological manipulation of people into performing actions that leave them defrauded	<ul style="list-style-type: none"> • Using fake M-PESA messages to defraud agents/customers

Identity theft, identity fabrication, identity manipulation, data manipulation, phishing and social engineering were identified as the main methods used to perpetrate identity fraud in Kenya. The survey revealed that identity theft was mainly committed through the use of stolen or lost identification documents. This may be attributed to the lack of concrete identity information and adequate security features on the documents. The second generation identity card (see Figure 2.6) for example had a blurred black and white photo. The birth certificate bore textual personal details (see Figure 2.4) only. In addition, these documents could easily be fabricated or altered. Information from an ATM card was ‘phished’ through skimming because most banks were issuing magnetic-stripped cards. Fraudsters were also employing technology-driven social engineering to access illegitimate services or money. A good example is where employment ‘facilitation fee’ was paid to a fraudster through mobile money. This is an emerging form of identity fraud that is not known to most people. The unauthorized manipulation of data suggests that some institutions operated databases that had inadequate security controls.

These methods of identity fraud are similar to those reviewed in the literature. However, in this research, the methods were established through an empirical study. Further, the study looked at identity fraud from the context of both the offline and online environments while previous works concentrated mainly on the online environment (Aburrous et al., 2010; Bang et al., 2012; Eisen, 2009; Furnell, 2010; Hopkins, 2005; McCarty, 2003). There was little mention of data manipulation in the literature with respect to identity fraud. The little mention might be explained by the fact that previous studies were done in developed countries where information systems are more advanced and fairly difficult to manipulate.

4.2.6 Registration and Identification Systems’ Survey

This survey was undertaken at the Civil Registration Department and the National Registration Bureau with the guidance of the interview schedule provided in **APPENDIX D**. The details of the survey interview are provided in the following interview transcripts.

(i) Interview Transcripts from Civil Registration Department

Table 4. 2: Background of CRD System

Interview Transcript	Remarks
<i>Researcher:</i> ‘What is the system’s name?’	
<i>Respondent CRD:</i> ‘Civil Registration and Vital Statistics System (CRVSS).’	
<i>Researcher:</i> ‘When was it implemented?’	
<i>Respondent CRD:</i> ‘2010.’	Fairly new system.
<i>Researcher:</i> ‘Why was it implemented?’	
<i>Respondent CRD:</i> ‘To automate manual processes of CRD thus creating a central database of all birth and death registrations.’	Restricted to birth and death registration.
<i>Researcher:</i> ‘Were there other previous versions of the system? If “Yes”, which ones?’	
<i>Respondent CRD:</i> ‘No.’	The department has been operating a manual registration system before CRVSS

Table 4. 3: CRD Registration Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘What are the requirements needed for one to register into the identification system?’	
<i>Respondent CRD:</i> ‘See Table 2- 1 and Table 2- 2.’	Paper-based supporting documents.
<i>Researcher:</i> ‘How is the registration done?’	
<i>Respondent CRD:</i> ‘See Table 2- 1 and Table 2- 2.’	Registration involves a lot of paperwork.
<i>Researcher:</i> ‘Who does the registration?’	
<i>Respondent CRD:</i> ‘Hospital Staff and Assistant Chief.’	Institutional cooperation exist.
<i>Researcher:</i> ‘Where is it done?’	
<i>Respondent CRD:</i> ‘At Hospital or Assistant Chief’s Office.’	Distributed Registration.
<i>Researcher:</i> ‘When is it done?’	
<i>Respondent CRD:</i> ‘Whenever a birth or death event is reported.’	No strict policies to enforce compulsory registration.
<i>Researcher:</i> ‘How often is it done?’	
<i>Respondent CRD:</i> ‘Continuous.’	System availability is crucial
<i>Researcher:</i> ‘What is the current registered population?’	
<i>Respondent CRD:</i> ‘Birth registration stands at sixty percent (60%) of the total population and death registration stands at fifty percent (50%) of all reported deaths.’	40% of births and 50% of deaths were not known by the department.

Table 4. 4: CRD Data Transmission Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘Is there any transmission of registration data to some other site?’	
<i>Respondent CRD:</i> ‘Yes.’	
<i>Researcher:</i> ‘How is it transmitted?’	
<i>Respondent CRD:</i> ‘Birth and death documents in paper and digital format are sent manually to sub-county office from where they are entered into the central database located at the CRD headquarters.’	The process in the field station is manual but some processes have been automated at the headquarters.
<i>Researcher:</i> ‘How long does it take the data to reach its final destination?’	
<i>Respondent CRD:</i> ‘An average of 7 days.’	System does not operate on real time.

Table 4. 5: CRD Data Processing Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘What is involved during processing of registration data?’	
<i>Respondent CRD:</i> ‘Registration forms received at the sub-county from field offices are checked for correctness, and if satisfactory, each is given a registration number and signed. Duplicates are scanned and sent to headquarters electronically. See Table 2- 2 for more details.’	Process is tedious and semi-automated.
<i>Researcher:</i> ‘Who does the processing?’	
<i>Respondent CRD:</i> ‘District/Sub-County Registrar and registry clerks.’	Some CRD staff operate from remote sites.
<i>Researcher:</i> ‘Where is it done?’	
<i>Respondent CRD:</i> ‘Sub-County Headquarters.’	Processing at designated remote sites.
<i>Researcher:</i> ‘What is the product of the processed data?’	
<i>Respondent CRD:</i> ‘Birth or Death Certificate.’	Paper-based documents.
<i>Researcher:</i> ‘Who are the consumers of this product?’	
<i>Respondent CRD:</i> ‘Individual citizens.’	Kenyan citizens.
<i>Researcher:</i> ‘How do the consumers get the product?’	
<i>Respondent CRD:</i> ‘An application for the acquisition of the document is made by the concerned party. The document will then be processed and picked at the district registrar’s office or any other place where the application was made.’	Process is semi-automated.

Table 4. 6: CRD Data Storage Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘What stores the processed and the unprocessed data?’	
<i>Respondent CRD:</i> ‘Data is stored in NetApp servers.’	Storage done on separate servers from the application.
<i>Researcher:</i> ‘Where is the storage area located?’	
<i>Respondent CRD:</i> ‘CRD Headquarters.’	Centralized storage.
<i>Researcher:</i> ‘Who does the storage?’	
<i>Respondent CRD:</i> ‘System Administrator.’	System Administrator doubles as database administrator.
<i>Researcher:</i> ‘Is there a secondary storage facility? If yes, how frequently is data backed up?’	
<i>Respondent CRD:</i> ‘No secondary site. Backup done at the primary site.’	Lack of a failover site.

Table 4. 7: CRD Verification and Validation Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘Can the system identify incorrect registration data? If yes, explain how?’	
<i>Respondent CRD:</i> ‘See Table 2- 2 procedure number 5.’	Verification and validation is mainly done manually

Table 4. 8: CRD Technology

Interview Transcript	Remarks
<i>Researcher:</i> ‘What are the components of the identification system?’	
<i>Respondent CRD:</i> ‘Client Computers, Servers, Data Network, DBMS, Client Application and Server Application.’	
<i>Researcher:</i> ‘What kind of technology is used for data registration, transmission and storage?’	
<i>Respondent CRD:</i> ‘Client-Server technology.’	
<i>Researcher:</i> ‘Is the system networked? If yes, under what topology?’	
<i>Respondent CRD:</i> ‘The network has a Star topology.’	A problem at the central site would make the system inaccessible.
<i>Researcher:</i> ‘What Operating System(s) is/are in use?’	
<i>Respondent CRD:</i> ‘Database server runs on Linux Oracle OS while client computers run on windows OS.’	Proprietary software utilized.
<i>Researcher:</i> ‘What application software is/are running?’	
<i>Respondent CRD:</i> ‘Client application is developed on .NET and PHP and the database runs on Oracle 11g.’	Proprietary software utilized.
<i>Researcher:</i> ‘How are electronic documents managed?’	
<i>Respondent CRD:</i> ‘Stored on windows folders’.	No proper document management system in place.

Table 4. 9: CRD System Architecture

Interview Transcript	Remarks
<i>Researcher:</i> ‘How are the components of the system connected?’	
<i>Respondent CRD:</i> ‘The architecture consists of a client tier at the end user side, and a 3-tier processing server side (presentation tier, business tier and back-office tier).’	Client-Server Architecture
<i>Researcher:</i> ‘Does the system interact with other external systems? If so, how?’	
<i>Respondent CRD:</i> ‘System is stand alone.’	It is hard to establish a relationship between a person’s records spread across the various systems
<i>Researcher:</i> ‘How does data flow within the system?’	
<i>Respondent CRD:</i> ‘Data flow from the field office to the district/sub-county office and finally to headquarters and vice versa.’	Involves both electronic and paper-based documents.

Table 4. 10: CRD System Security

Interview Transcript	Remarks
<i>Researcher:</i> ‘What kind of security has been implemented on:’ <ul style="list-style-type: none"> • Equipment. • Gateway. • Platform. • Database. 	
<i>Respondent CRD:</i> ‘Equipment has no security, Gateway has firewalls and Intrusion Detection System, The platform is protected by anti-virus and the Database has Oracle inbuilt security features.’	Insufficient security features. Cyber-attacks such as SQL injection and cross-site scripting can easily be carried out on the system
<i>Researcher:</i> ‘Who is in charge of security?’	
<i>Respondent CRD:</i> ‘System Administrator.’	No specialization. This task is ideally done by an information security expert.

4.2.7 Civil Registration System Challenges

There were a number of Civil Registration Challenges identified. They are identified as below

1. Statistics from CRD showed that the birth register had only 60% of the total Kenyan population and the death register had only 50% of the total deaths. This means that 40% of births and 50% of deaths were not known by the department.
2. CRD business processes were semi-automated and involved the use of paper-based documents. Data captured from the application forms into the system at the sub-county was at times incorrect. Additionally, it was hard to fully authenticate the paper documents.

3. The birth and death certificates issued by the system did not have sufficient security features. It was possible for criminals to forge the certificate and use them to perpetrate identity fraud.
4. CRVSS was not linked to any other external identification system such as KENRIS. It was therefore not possible to establish a relationship between a person's records spread across the various systems.
5. The existing system security architecture was not elaborate enough. Cyber-attacks such as SQL injection and cross-site scripting could easily be carried out on the system.

(ii) Interview Transcripts from the National Registration Bureau

Table 4. 11: Background of KENRIS System

Interview Transcript	Remarks
<i>Researcher:</i> 'What is the system's name?'	
<i>Respondent NRB:</i> 'Kenya National Registration and Identification System (KENRIS).'	
<i>Researcher:</i> 'When was it implemented?'	
<i>Respondent NRB:</i> '1995.'	Technology may be outdated.
<i>Researcher:</i> 'Why was it implemented?'	
<i>Respondent NRB:</i> 'To assist in identifying Kenyan Citizens.'	Meant for managing identification data for Kenyans only.
<i>Researcher:</i> 'Were there other previous versions of the system? If "Yes", which ones?'	
<i>Respondent NRB:</i> 'Yes, a semi-automated 1 st Generation ID Card System.'	Experience in automated ID card system in place.

Table 4. 12: KENRIS Registration Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘What are the requirements needed for one to register into the identification system?’	
<i>Respondent NRB:</i> ‘See Section 2.4.’	Verification through paper-based documents.
<i>Researcher:</i> ‘How is the registration done?’	
<i>Respondent NRB:</i> ‘See Section 2.4.’	Involves a lot of paperwork at the field station.
<i>Researcher:</i> ‘Who does the registration?’	
<i>Respondent NRB:</i> ‘National ID is done by NRB Registrar, Alien ID is done by Immigration Registrar and Refugee ID is done by DRA Registrar.’	Apart from registering citizens, NRB also manages data for refugees.
<i>Researcher:</i> ‘Where is it done?’	
<i>Respondent NRB:</i> ‘NRB offices in 290 sub-counties as well as Immigration and DRA offices.’	System operates countrywide.
<i>Researcher:</i> ‘When is it done?’	
<i>Respondent NRB:</i> ‘Any week day.’	
<i>Researcher:</i> ‘How often is it done?’	
<i>Respondent NRB:</i> ‘It is a continuous exercise’.	System availability is crucial.
<i>Researcher:</i> ‘What is the current registered population?’	
<i>Respondent NRB:</i> ‘There are 21 million registered citizens, aliens and refugees. Out of these, 2 million are records of dead people. Approximately 16,000 records are duplicates. The AFIS system has 25 million records.’	Integrity of data is questionable.

Table 4. 13: KENRIS Data Transmission Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘Is there any transmission of registration data to some other site?’	
<i>Respondent NRB:</i> ‘Yes.’	
<i>Researcher:</i> ‘How is it transmitted?’	
<i>Respondent NRB:</i> ‘Registration documents are manually transmitted to NRB headquarters.’	Process is manual
<i>Researcher:</i> ‘How long does it take the data to reach its final destination?’	
<i>Respondent NRB:</i> ‘An average of 7 days.’	System does not operate on real time.

Table 4. 14: KENRIS Data Processing Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘What is involved during processing of registration data?’	
<i>Respondent NRB:</i> ‘Data processed with the assistance of Citizen, AFIS, Aliens and Production sub-systems.’	Modular system.
<i>Researcher:</i> ‘Who does the processing?’	
<i>Respondent NRB:</i> ‘Users of the individual sub-systems.’	User specialization exist.
<i>Researcher:</i> ‘Where is it done?’	
<i>Respondent NRB:</i> ‘NRB Headquarters.’	Centralized processing.
<i>Researcher:</i> ‘What is the product of the processed data?’	
<i>Respondent NRB:</i> ‘National Identity Card, Alien Identity Card and Refugee Identity Card.’	Paper/plastic-based card.
<i>Researcher:</i> ‘Who are the consumers of this product?’	
<i>Respondent NRB:</i> ‘Citizens who are above 18 years and have applied for the document.’	Manages data of adult population only.
<i>Researcher:</i> ‘How do the consumers get the product?’	
<i>Respondent NRB:</i> ‘They collect from where they did the application. This is usually at the district registrar’s office.’	Distributed system.

Table 4. 15: KENRIS Data Storage Process

Interview Transcript	Remarks
<i>Researcher:</i> ‘What stores the processed and the unprocessed data?’	
<i>Respondent NRB:</i> ‘Data stored in HP Servers.’	
<i>Researcher:</i> ‘Where is the storage area located?’	
<i>Respondent NRB:</i> ‘At NRB Headquarters.’	Centralized storage.
<i>Researcher:</i> ‘Who does the storage?’	
<i>Respondent NRB:</i> ‘Database Administrator.’	System Administrator doubles as Database Administrator.
<i>Researcher:</i> ‘Is there a secondary storage facility? If yes, how frequently is data backed up?’	
<i>Respondent NRB:</i> ‘No secondary site. Backup done at the primary site.’	Lack of a failover site.

Table 4. 16: KENRIS Verification and Validation process

Interview Transcript	Remarks
<i>Researcher:</i> ‘Can the system identify incorrect registration data? If yes, explain how?’	
<i>Respondent NRB:</i> ‘Application documents are checked to ensure that they came from the correct registration station, are sealed and have authorized signatures. They are then authorized and validated against data in central database.’	Checks are manual and hence not full proof.

Table 4. 17: KENRIS Technology

Interview Transcript	Remarks
<i>Researcher:</i> ‘What are the components of the identification system?’	
<i>Respondent NRB:</i> ‘Client Computers, Servers, Data Network, DBMS, Client Applications, Card Production System.’	
<i>Researcher:</i> ‘What kind of technology is used for data registration, transmission and storage?’	
<i>Respondent NRB:</i> ‘Data registration and transmission is currently manual. However, data is scanned/input into the KENRIS database at the headquarters.’	
<i>Researcher:</i> ‘Is the system networked? If yes, under what topology?’	
<i>Respondent NRB:</i> ‘Bus topology.’	System runs on Local Area Network only
<i>Researcher:</i> ‘What Operating System(s) is/are in use?’	
<i>Respondent NRB:</i> ‘Windows.’	Proprietary software utilized.
<i>Researcher:</i> ‘What application software is/are running?’	
<i>Respondent NRB:</i> ‘Oracle-based application.’	Proprietary software utilized.
<i>Researcher:</i> ‘How are electronic documents managed?’	
<i>Respondent NRB:</i> ‘They are saved on windows folders in a server.’	No proper document management system in place.

Table 4. 18: KENRIS System Architecture

Interview Transcript	Remarks
<i>Researcher:</i> ‘How are the components of the system connected?’	
<i>Respondent NRB:</i> ‘Sub-systems are interlinked through a local area network at NRB headquarters.’	Bus topology
<i>Researcher:</i> ‘Does the system interact with other external systems? If so, how?’	
<i>Respondent NRB:</i> ‘Integrated with IPRS system.’	Links with IPRS but do not link with civil registration system.
<i>Researcher:</i> ‘How does data flow within the system?’	
<i>Respondent NRB:</i> ‘Data flow manually from the field office to the district/sub-county office and finally to headquarters and vice versa.’	This is a manual process.

Table 4. 19: KENRIS System Security

Interview Transcript	Remarks
<p><i>Researcher:</i> ‘What kind of security has been implemented on:’</p> <ul style="list-style-type: none"> • Equipment. • Gateway. • Platform. • Database. 	
<p><i>Respondent NRB:</i> ‘Equipment has no security, Gateway has a firewall, The platform is protected by anti-virus and the Database has Oracle inbuilt security features.’</p>	<p>Insufficient security features. Cyber-attacks such as SQL injection and cross-site scripting can easily be carried out on the system</p>
<p><i>Researcher:</i> ‘Who is in charge of security?’</p>	
<p><i>Respondent NRB:</i> ‘System Administrator.’</p>	<p>No specialization. This task is ideally done by an information security expert.</p>

4.2.8 Kenya National Registration and Identification System Challenges

There were a number of system challenges identified with regards to the Kenya National Registration Identification System. These challenges include

- 1) KENRIS database had approximately twenty one (21) million records. About two (2) million of these records belonged to citizens who had died, yet they appeared ‘alive’ in the system. Additionally, the database did not have records of about 2.5% of the adult population (those who are 18 years and above).
- 2) There were about sixteen thousand (16,000) duplicate records in the database.
- 3) The business processes in the field offices were purely manual and involved the use of paper-based documents. This presented fertile grounds for document loss and forgery.
- 4) The identification cards produced by the system had inadequate security features and unclear personal details. In particular, most of the cards had a blurred black and white photo.
- 5) KENRIS was not linked to any other registration system such as CRVSS (birth and death register). That is why it was not easy to differentiate the records of those who had died from those who were still alive.

- 6) The existing security architecture was not elaborate enough thus enabling such cyber-attacks as SQL injection to be carried out.

The survey established that the birth register had only 60% of the total population in the country and the death register had only 50% of the total deaths. Interviewees cited poor accessibility to several registration centres and lack of incentives for parents to register their children as the main reasons behind the low registration. Further, about 2.5% of the adult population (18 years and above) was missing in the KENRIS database. Most citizens residing in remote rural parts of Kenya had little exposure to services that required formal identification to access, and thus may not have had anything to motivate them to register. Additionally, their level of education was reported to be generally low, and by extension, there was little awareness on the need to register. The study also established that about two (2) million of the twenty one (21) million records in KENRIS database belonged to citizens who had died, yet they appeared 'alive' in the system. This might have been caused by CRVSS and KENRIS systems operating independent of each other ('in silo') and therefore may not have been able to synchronize their data. This kind of system arrangement makes it difficult to establish a relationship between the records of an individual in disparate databases. The sixteen thousand (16,000) duplicate records found in KENRIS database might have been entered during the migration of data from the first generation identity card system to the current second generation identity card system. This is because there was a lot of manual intervention in the process.

Further, the registration process in KENRIS and CRVSS systems was mainly manual and paper-based. This presented fertile grounds for document counterfeiting. A person applying for a national identity card was required to present supporting paper documents to the registration officer. These documents were easy to counterfeit and thus facilitated easy acquisition of illegitimate ones. Further, the identification documents did not have adequate security features. It was easy for example to forge a birth certificate and use it to acquire a national identity card, which together may then be used to apply for a passport. Finally, the design of both CRVSS and KENRIS may not have considered the emerging security challenges. That is why it was found that different types of cyber-attacks could easily be carried out on the systems.

The ‘silo’ design of CRVSS and KENRIS is similar to Mannan and Van Oorschot (2009) ‘siloed’ identity system model. With this model, it is difficult to establish a relationship between records of a given identity. In addition, the systems’ business processes involve a lot of paper work, while those of other countries such as Malaysia, China, USA and Mexico are mainly undertaken in an electronic environment. On technology adoption, a study on the Malaysian electronic identification system established factors that were similar to those suggested by interviewees as affecting CRVSS and KENRIS. However, in many countries within the European Union, privacy was suggested as being the main factor affecting the adoption of their identification systems.

4.3 Model Development

The system was modelled from the view of a service provider, an identity provider and a security architect as shown in Figure 4.2. The service provider view was designed with Enterprise Architect, version 7.5 while the identity provider and security architect views were designed with Microsoft Office tools, and in particular, Visio Professional 2013. Enterprise Architect is a Unified Modelling Language (UML) tool. UML is a standardized (ISO/IEC 19501:2005) general-purpose modelling language that was developed by Grady Booch, Ivar Jacobson and James Rumbaugh at Rational Software in the 1990s and adopted by the Object Management Group (OMG) in 1997. It is now the de facto standard for modelling software applications and hardware systems.

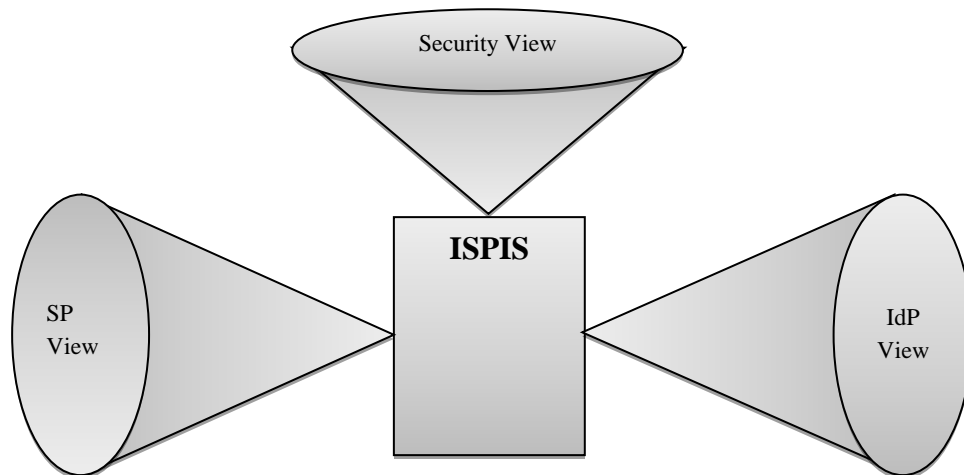


Figure 4. 2: System Model Views

The Service Provider (SP) view models the system from the perspective of its intended users while the Identity Provider (IdP) view models its back-end processes. The security view models its security architecture.

4.3.1 The Service Provider View

The modelling process started with capturing the user requirements into a *Requirements Model*. This model defines high level requirements for the system and provides a foundation for the Use Case model. It typically captures both functional and non-functional requirements.

The *Use Case Model* was mapped to the Requirements Model to define the exact system functionality. As each Use Case was added, a traceable link was created from the appropriate system processes to the Use Case. This mapping clearly stated what functionality the system would provide to meet the end-user requirements as outlined in the requirements model. It also ensured that no Use Cases existed without a purpose. The resultant Use Cases were refined to include requirements, constraints, notes and scenarios. This information unambiguously describes what the Use Case does, how it is executed and the constraints on its execution while making sure that it still meets the business process requirements. From the details of the use cases, *sequence diagrams* were constructed to describe the way things interact in the system and the interface a user will use to execute the use case. Figure 4.3 below shows the model development process.

From the sequence diagrams, a *class model* was created. This is a precise specification of the objects in the system, their data or attributes and their behaviour or operations. Sequence diagram messages will typically map to class operations. For each class, unit tests and integration tests are defined to thoroughly test: (i) that the class functions as specified internally and that (ii) the class interacts with other related classes and components as expected. As the Class Model developed it was broken into discrete packages and components. A component represents a deployable chunk of software that collects the behaviour and data of one or more classes and exposes a strict interface to other consumers of its services. Data to be stored and retrieved as part of the overall system design was described in a *Data Model*. This is typically a relational database model which describes the tables and data in detail and allows generation of DDL scripts to create and setup databases.

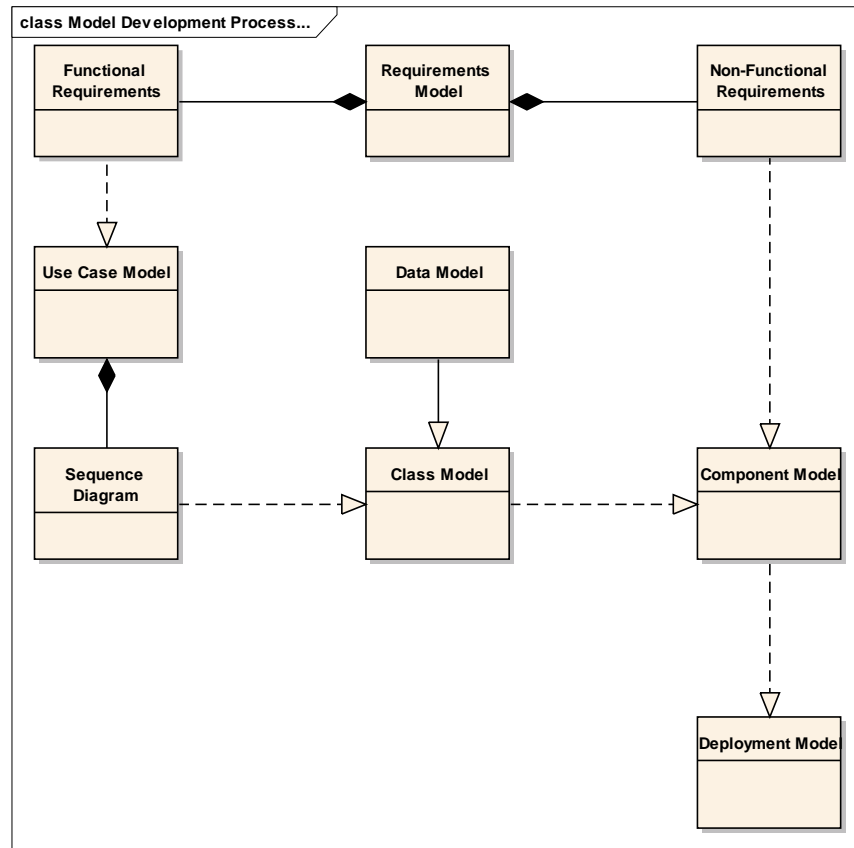


Figure 4. 3: Model Development Process

So from the Class and Data Models, a *Component Model* was built to define the logical packaging of classes. For each component, integration tests were defined to confirm that the component's interface met the specification given in relation to other software elements. Additionally, Non- Functional requirements were incorporated in the model.

A *Deployment model*, which defines the physical architecture of the system, was finally developed. This work began early in order to capture the physical deployment characteristics (i.e. what hardware, operating systems, network capabilities, interfaces and support software will make up the system and where it will be deployed). As the model developed, the physical architecture was updated to reflect the actual system being proposed.

4.3.1.1 Requirements Model

Requirements are a collection of needs expressed by users while considering the constraints under which the system must operate. They can be broad and high-level or more specialized and detailed. Detailed requirements can be organized into a hierarchy culminating in a high-level requirement, so that satisfying each of the detailed requirements results in meeting the higher-level requirements. This hierarchical structure helps manage the complexity of large systems with dozens of requirements and many processes being developed to implement the requirements.

The requirements for ISPIS were informed by the survey results and a review of literature on similar systems.

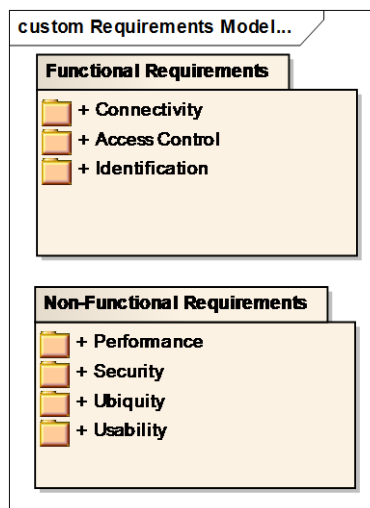


Figure 4. 4: Requirements Model

They were categorized into functional and non-functional requirements. Functional requirements define the functional behaviour to be supported by the system while the non-functional requirements define the constraints to be met by the system. Figure 4.4 shows a high-level view of the requirements model.

a) Functional Requirements

ISPIS system has three high-level functional requirements: Connectivity, Access Control and Identification (identity validation and identity verification). Figure 4- 5 shows a summary of ISPIS functional requirements.

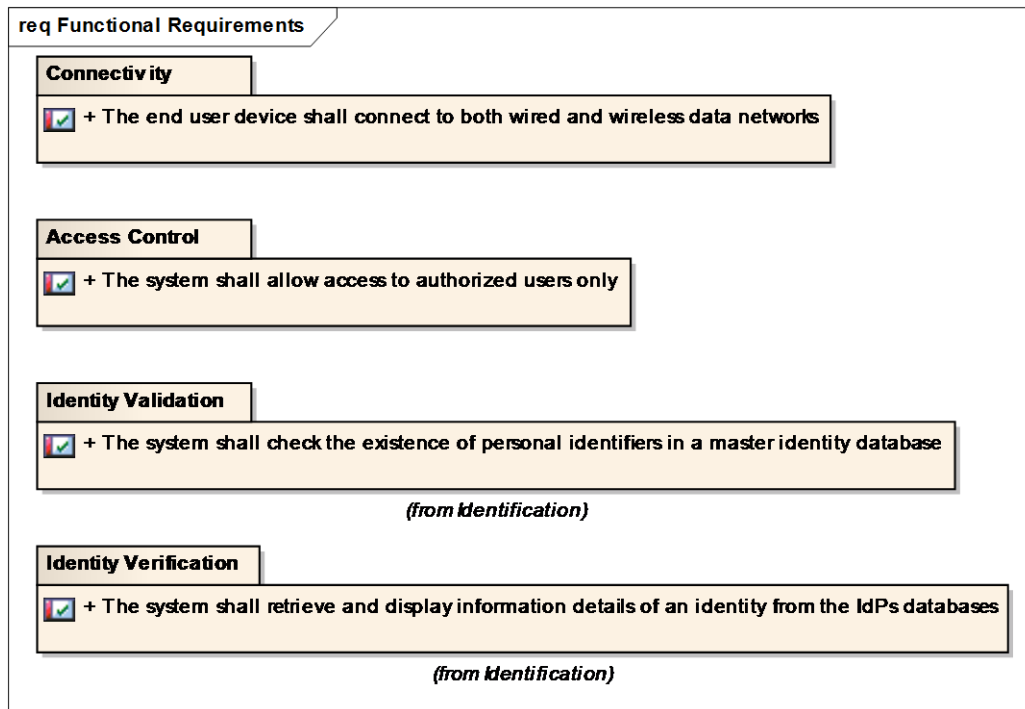


Figure 4. 5: Functional Requirements

b) Non-Functional Requirements

The high-level non-functional requirements for ISPIS system are Performance, Security, Ubiquity and Usability. Figure 4- 6 shows a summary of ISPIS non-functional requirements.

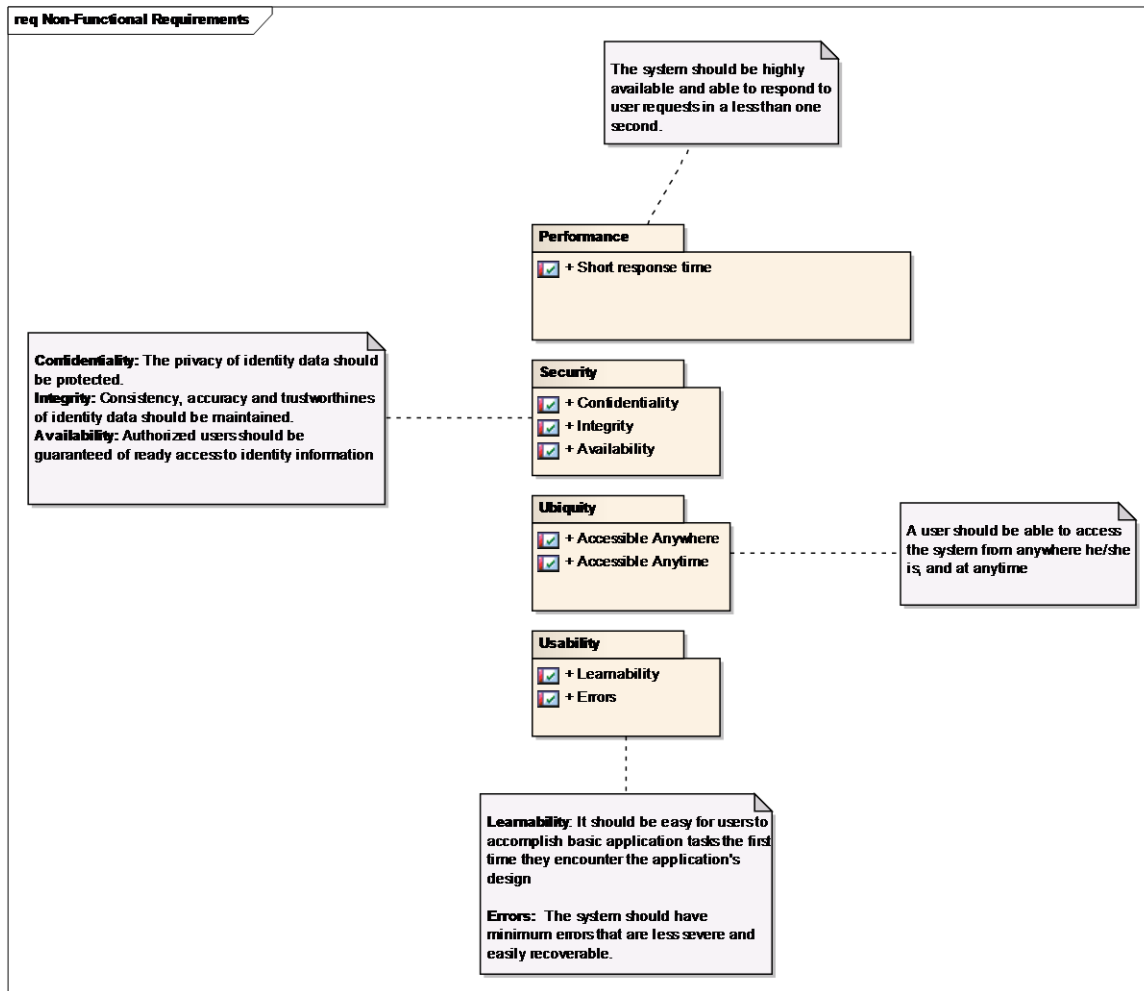


Figure 4. 6: Non-Functional Requirements

4.3.1.2 Use Case Model

A Use Case model is a catalogue of system functionality described using UML Use Cases. Each Use Case represents a single, repeatable interaction that a user or ‘actor’ experiences when using the system. A Use Case typically includes one or more ‘scenarios’ which describe the interactions that go on between the Actor and the System, and documents the results and exceptions that occur from the user's perspective. Use Cases may include other Use Cases as part of a larger pattern of interaction and may also be extended by other use cases to handle exceptional conditions. A Use Case diagram captures Use Cases and relationships between Actors and the Subject (system). It describes the functional requirements of the system, the

manner in which outside things (Actors) interact at the system boundary, and the response of the system. Figure 4.7 shows a high-level use case model for the ISPIS system.

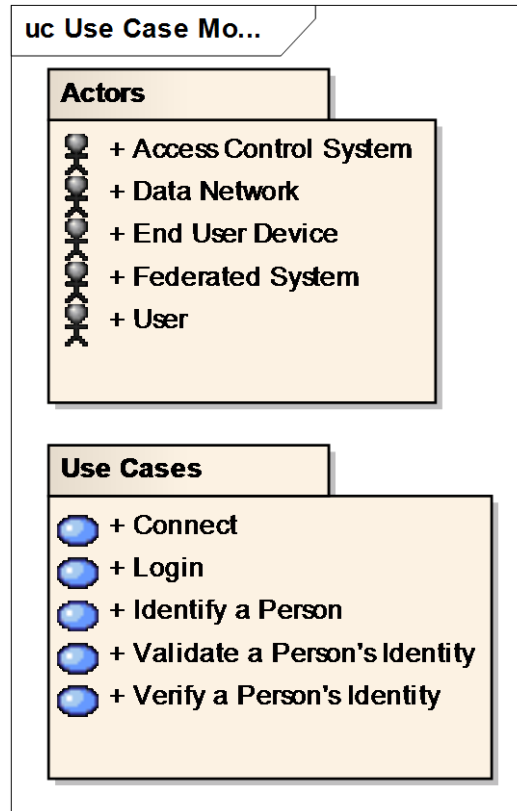


Figure 4. 7: Use Case Model

Use Cases

ISPIS consists of five use cases, namely: *Connect*, *Login*, *Identify a Person*, *Validate a Person's Identity* and *Verify a Person's Identity*. These use cases are related to each other in that post-condition of use case *Connect* is pre-conditioned for use case *Login*, while post-condition of *Login* is pre-conditioned for use case *Identify a Person*. Post-condition of *Identify a Person* is pre-conditioned for use case *Verify a Person's Identity*, while post-condition of *Verify a Person's Identity* is pre-conditioned for use case *Validate a Person's Identity*.

The system Actors are: (1) *User*, (2) *End-User Device*: Personal Computer or Mobile Phone, (3) *Access Control System*: part of the system that identify, authenticate and authorize users to the system, (4) *Data Network*: resources of the network that connects end-user device to

ISPIS databases, and finally (5) *Federated System*: a system that links disparate identity providers' databases. Figure 4.8 shows the relationships of ISPIS use cases.

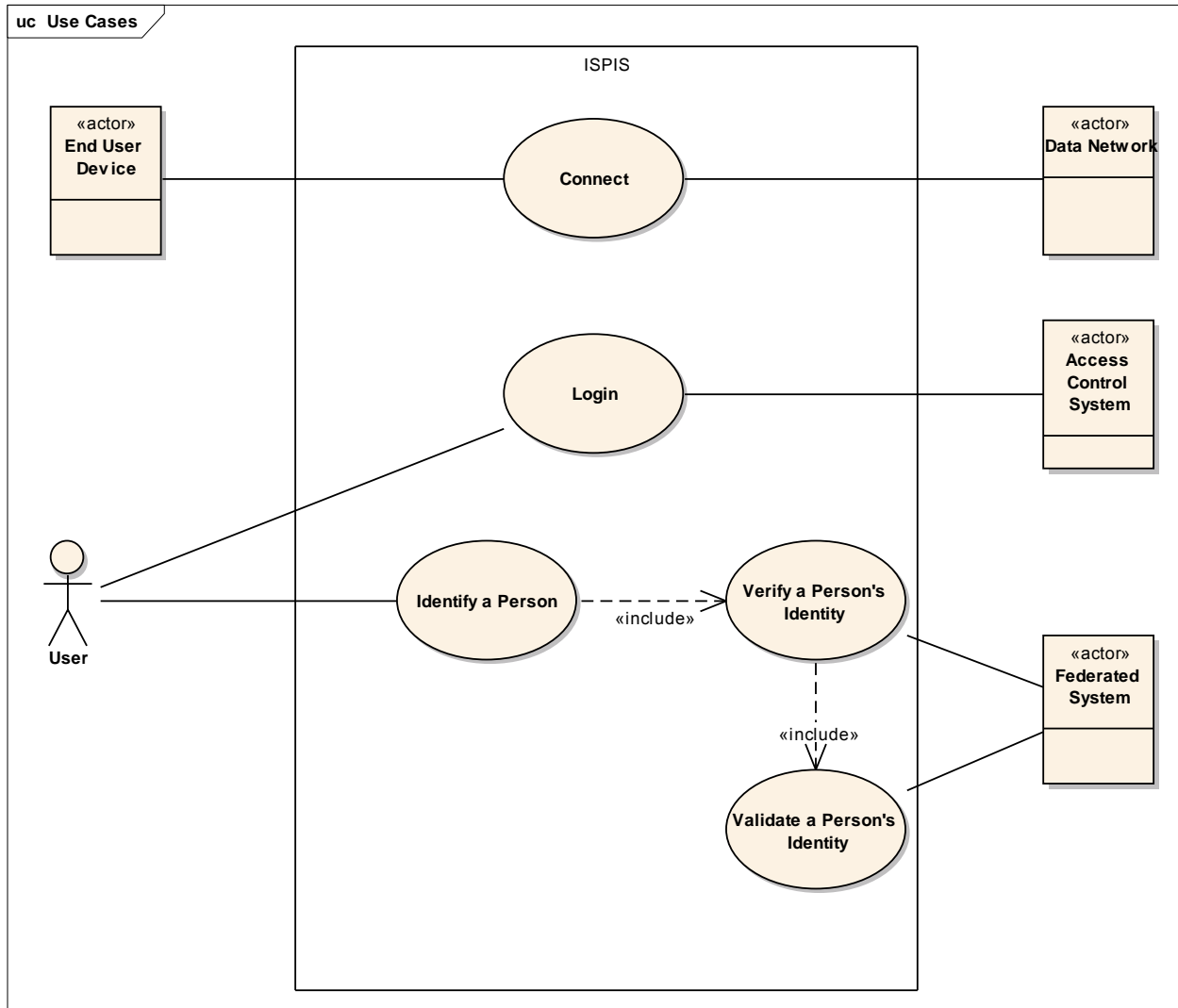


Figure 4. 8: Use Cases

1) Use Case Connect

Actors: End-User Device and Data Network.

Short Description: Use Case Connect realizes connection of End-User Device to the ISPIS Data Network.

Pre-condition: End-User Device is in the Data Network area

Invariant: if time-out occurs, restart the connection procedure

Post-Condition: After the execution, End-User Device is connected to the Data Network and authenticated by a connection algorithm based on its hardware signature. Only registered devices may access the network.

2) Use Case Login

Actors: User and Access Control System (ACS)

Short Description: Login Use Case verifies user access to the ISPIS system based on Username and Password pair that is entered by the user on the End-User Device (Personal Computer or Smartphone).

1. User initializes the device

Pre-condition: End-User Device is connected to the Data Network

Invariant: If time-out occurs, restart the procedure (go to step 1)

2. User launches the application

Pre-Condition: User unidentified

Invariant: If time-out occurs, restart the procedure (go to step 1)

2. a. ACS prompts “Enter Username” and “Password”

2. b. User enters Username and Password

2. c. ACS checks Username

If Username does not exist in ACS database

ACS sends “Invalid User Name” (go back to 2. a.)

Else go to 2.d.

Post-Condition: User Identified

Pre-Condition: User not authenticated

2. d. ACS checks Password

If Password doesn't match

Count=Count+1

If (Count equal 3), go back to 2.a.

ACS sends “Invalid Password”

If Password matches, go to 3

3. User accesses the System

Post-Condition: User authenticated

Interaction Overview Diagram for Login Use Case

The Login Use Case described above can be summarized with an interaction diagram as shown in Figure 4.9 below. The diagram includes an interaction occurrence object: *EnterUserName&Password*, which gives a concise representation of the whole Login use case.

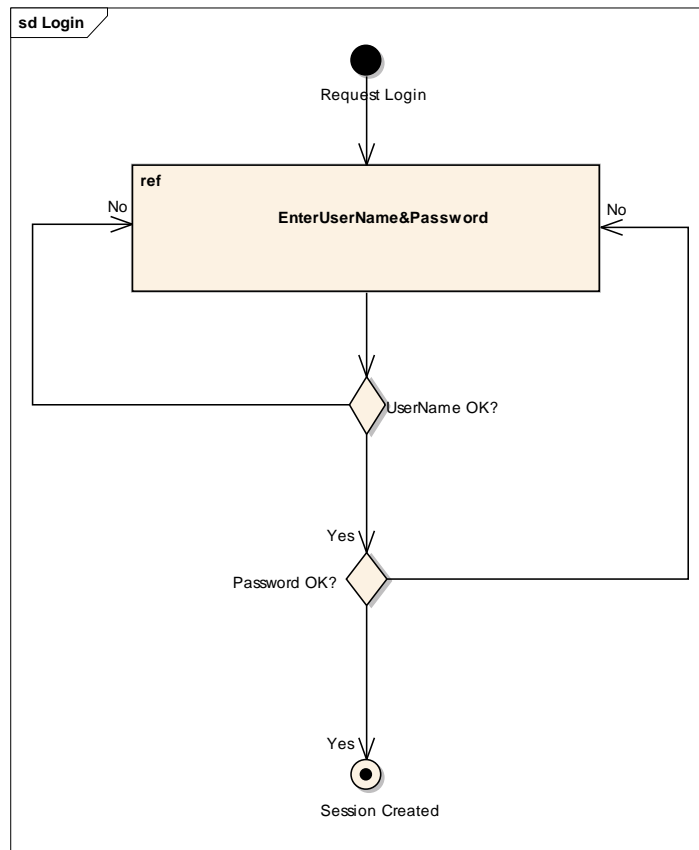


Figure 4. 9: Interaction Overview Diagram for Login Use Case

In Figure 4- 9, it is clear which activities are realized by use case Login. To begin with, a user requests login and then enters his/her identification (Username). If Username is in the users' database, the procedure continues, else it goes back to the first step. Likewise, if the entered password is correct, then the client application session will be initiated, else the user will be given some few more chances to try, and if not successful, it goes back to step one.

Sequence Diagram for Login Use Case

The Login sequence diagram shown in Figure 4.10 gives details for *EnterUserName&Password* object referenced in the interaction overview diagram. The sequence diagram has complete information about event/message flow between the User, Client Application Login, Server Application Login, Server Application and User Details.

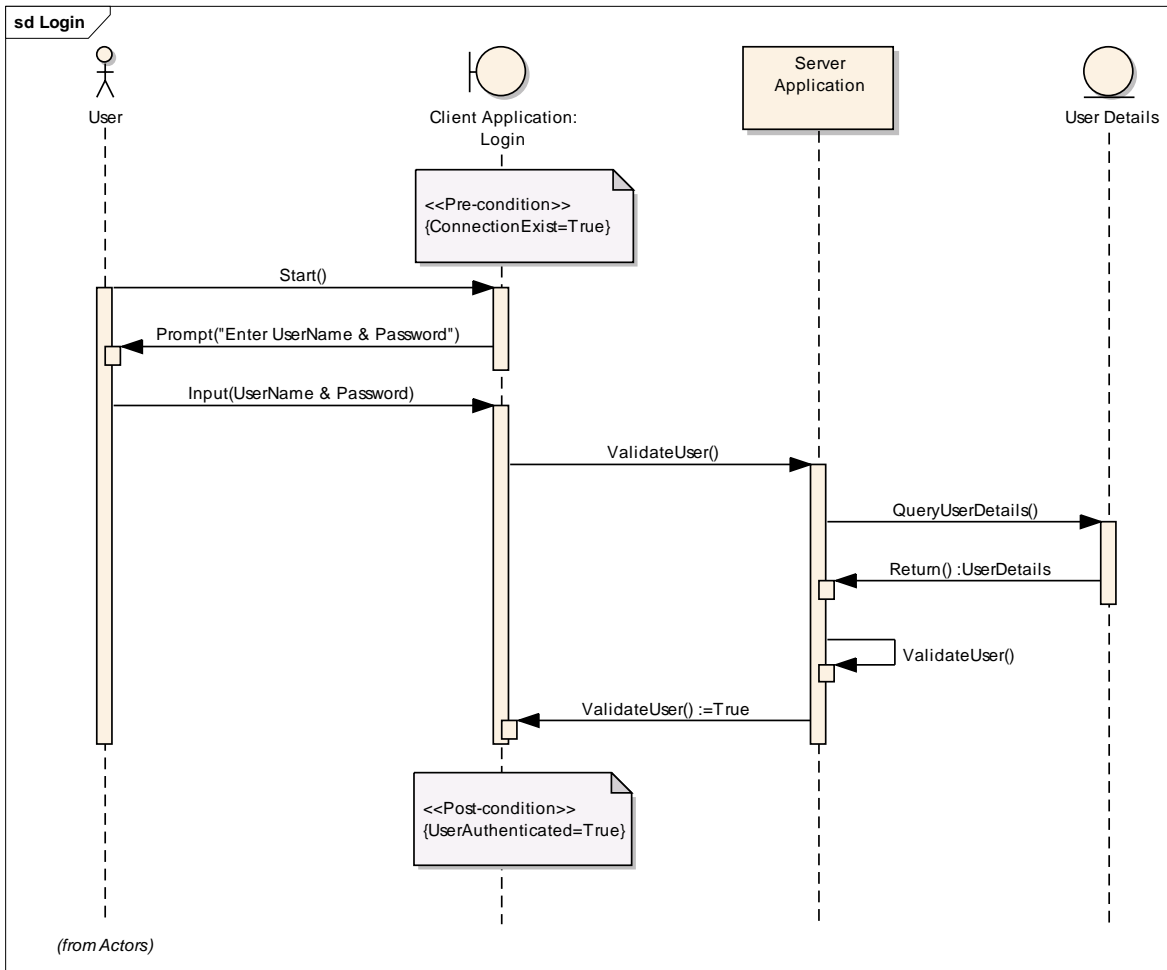


Figure 4. 10: Login Sequence Diagram

The user starts by double-clicking the application's executable file. The application returns a prompt "Enter Username and Password". When the user inputs the username and password and pushes a *Login button*, the Client Application Login sends the login credentials to

a Server Application which in turn queries a user details database. If the username and password exist in the database, a Client Application Identification interface is activated.

The OCL constraints in Login sequence diagram define pre-conditions and post-conditions that should be satisfied at the beginning and at the end of the execution. The pre-condition is the existence of a connection between the client application and user database (i.e. ConnectionExist = True). The post-condition is that the user must be authenticated in order to use the application (i.e. UserAuthenticated = True).

3) Use Case Identify a Person

Identify a person use case includes *verify a person's identity* use case which in turn includes *validate a person's identity* use case.

Actors: User and Federated System

Short Description: Identify a person use case establishes the identity of a particular person by first proving the existence of that identity in the ISPIS database (validation) and then recognizing the real identity owner (verification).

1. Validate a Person's Identity

Pre-Condition: PI not validated

1a. Federated System prompts "Enter PI"

1b. User enters PI

1c. Federated System checks PI

If PI does not exist in Federated System database then

Federated System sends "Invalid PI"

Post-Condition: PI not valid

If PI exist in Federated System database then

PI is valid (Proceed to 2)

Post-Condition: Identity not verified

2. Verify a Person's Identity

Pre-Condition: PI validated

Pre-Condition: Identity not verified

2a. Federated System queries identity provider's databases and retrieves authorized identity details

Post-Condition: Identity verified

Interaction Overview Diagram for Identify a Person Use Case

The interaction diagram for Identify a Person Use Case is shown in Figure 4.11 below. The diagram includes two interaction occurrence objects: *ValidateIdentity* and *VerifyIdentity*. These objects are references for the corresponding sequence diagrams as shown in Figure 4- 12 and Figure 4.13.

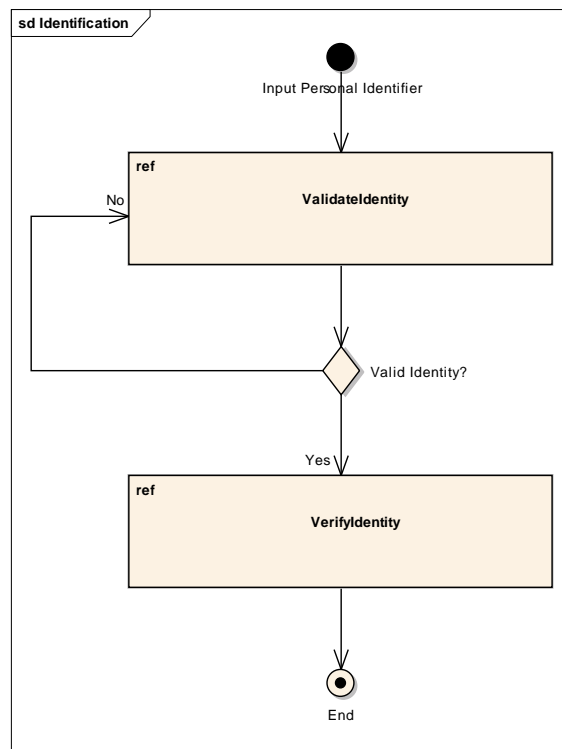


Figure 4. 11: Interaction Overview Diagram for Identify a Person Use Case

As shown in the above diagram (Figure 4.11), a user inputs an identifier for the person to be identified. If the identifier is in the federated identity database, the procedure continues to verify the identity: otherwise it goes back to the first step.

Sequence Diagram for Validate a Person's Identity Use Case

The Validate a Person's Identity sequence diagram gives details for *ValidateIdentity* object which was referenced in the Identify a Person interaction overview diagram. The sequence diagram has complete information about event/message flow between the User, Client Application Identification, Server Application, Federated Server and Federated Database as shown in Figure 4- 12 below.

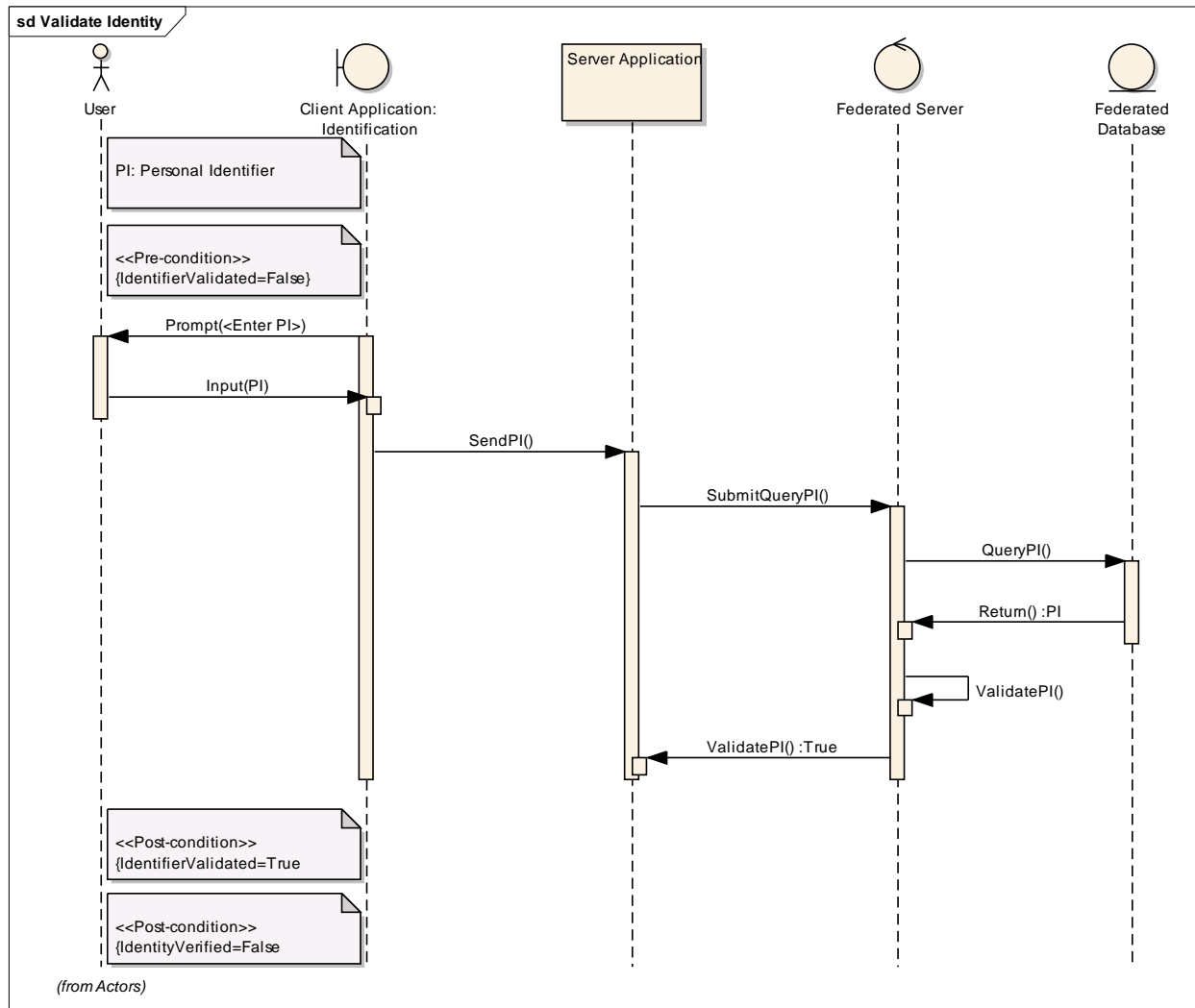


Figure 4. 12: Validate Identity Sequence Diagram

After a successful login, the Client Application Identification interface prompts the User for a Personal Identifier. The User inputs the identifier which is then sent to a Server Application for processing. The Server Application prepares and submits a query to the Federated Server to

locate the identifier in the Federated Database. If the Identifier exists, the Federated Database informs the Federated Server, which in turn informs the Server Application.

The pre-condition for Validate a Person's Identity sequence diagram is existence of an identifier that has not been validated (i.e. IdentifierValidated=False). The post-condition is the existence of a valid identifier (i.e. IdentifierValidated=True) and unverified identity (i.e. IdentityVerified = False).

Sequence Diagram for Verify a Person's Identity

The Verify a Person's Identity sequence diagram gives details for *VerifyIdentity* object which was also referenced in the Identify a Person interaction overview diagram. The sequence diagram has complete information about event/message flow between the User, Client Application Identification, Server Application, Federated Server, Federated Database, Wrapper and Identity Details as shown in Figure 4- 13 below.

After a person's identifier has been validated, the Server Application submits an identity details retrieval query to the Federated Server. The Federated Server optimizes the query and pushes it over to the Federated Database. The database invokes a Wrapper to execute the query on the identity providers' databases. The query returns Identity Details which are displayed by the Client Application Identification interface. This gives the User an opportunity to compare the retrieved identity details with what was presented, and hence achieve verification.

The pre-condition for Verify a Person's Identity sequence diagram is the existence of an identifier that has been validated (i.e. IdentifierValidated=True) and identity that has not been verified (i.e. IdentityVerified = False). The post-condition is the existence of a verified identity (i.e. IdentityVerified = True).

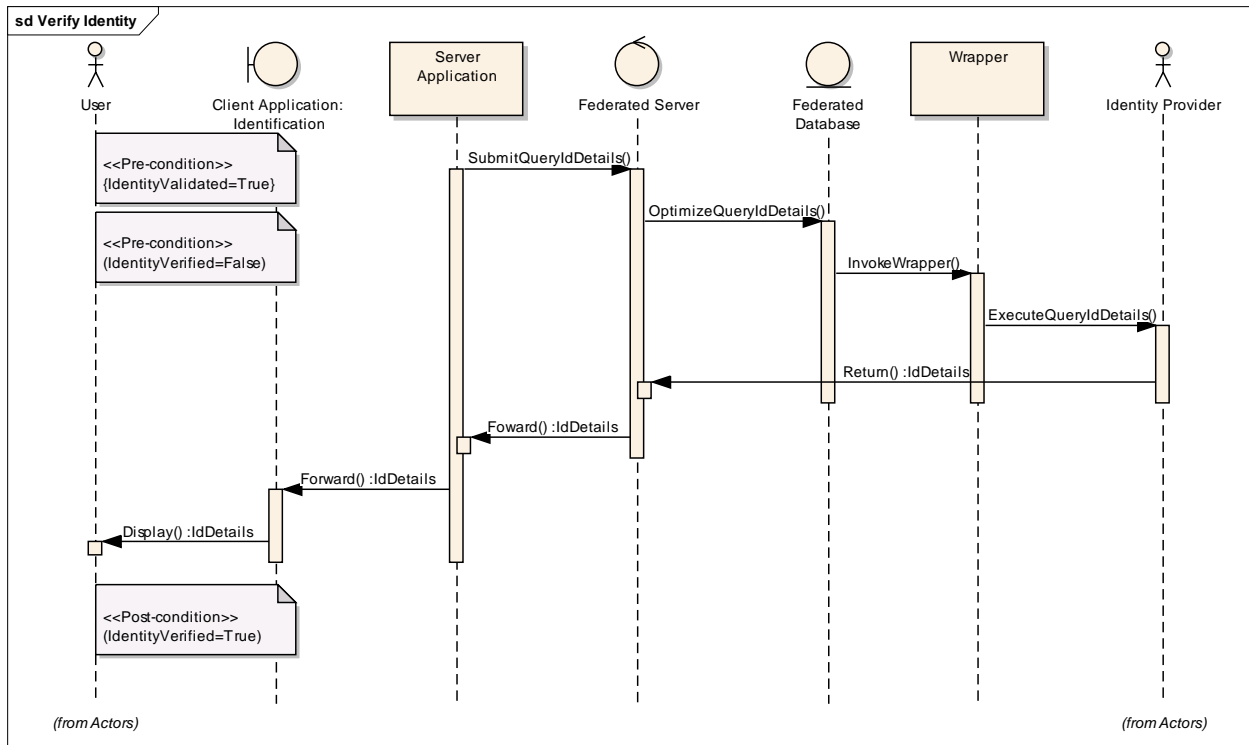


Figure 4. 13: Verify Identity Sequence Diagram

4.3.1.3 Class Model

The Class Model is a logical representation of the software system under construction. Classes generally have a direct relationship to source code or other software artifacts that can be grouped together into executable components. The model contains classes and artifacts which are being built or designed as part of the current system as well as classes and components that have been designed and built earlier and are being reused.

A class model is derived from the sequence diagrams. Every communicating object in the sequence diagram represents a class while message flows between classes form an association. There are three sequence diagrams in this model, i.e., Login (Figure 4.10), Validate Identity (Figure 4.12) and Verify Identity (Figure 4.13). The *Login sequence diagram* has three communicating objects: Client Application Login, Server Application and User Details: *Validate Identity sequence diagram* has ClientApplicationIdentification, ServerApplication, FederatedServer and FederatedDatabase: and finally, *Verify Identity sequence diagram* has ClientApplicationIdentification, ServerApplication, FederatedServer, FederatedDatabase,

Wrapper and Identity Details. A complete class definition diagram (Figure 4.14) is merged from the three sequence diagrams. The class attributes and methods/operations have been defined according to Java syntax.

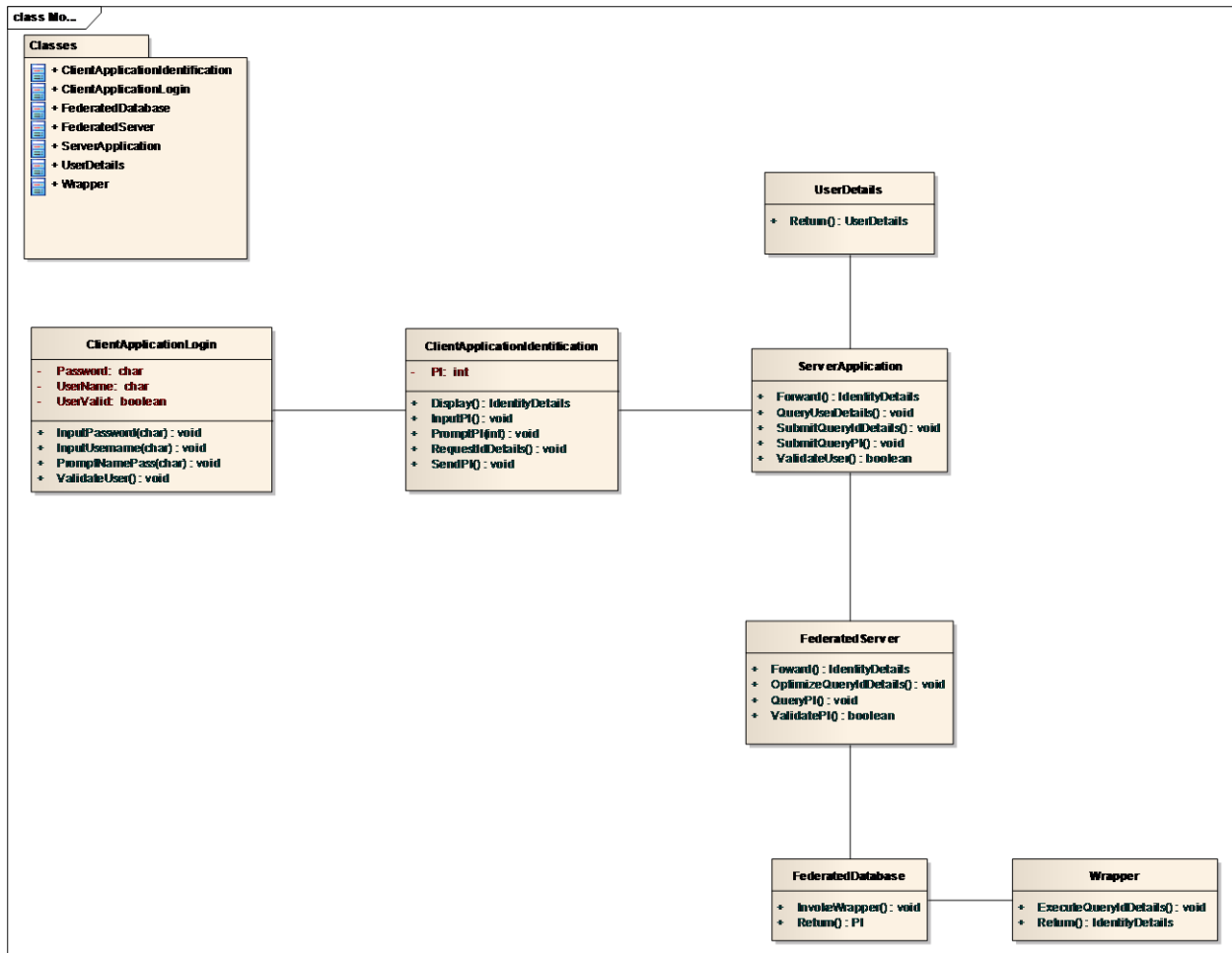


Figure 4. 14: Class Model

The ClientApplicationLogin class has Password, UserName and UserValid as attributes and PromptNamePass (char), InputUsername (char), InputPassword (char) and ValidateUser() as methods. This class provides a mechanism for controlling access to the system. The ValidateUser() method sends a request to the ServerApplication to validate a user based on UserName and Password. The ServerApplication class in turn invokes the QueryUserDetails() method which checks for the existence of UserName and Password in the users' database. This is an iterative process that is managed by ValidateUserDetails() method. From the Login sequence

diagram, it is clear that ClientApplicationLogin::UserValid attribute is set to the return value of ServerApplication::ValidUser() method during program execution.

```
public class ClientApplicationLogin {

    private char Password;
    private char UserName;
    private boolean UserValid;
    public ClientApplicationIdentification m_ClientApplicationIdentification;

    public ClientApplicationLogin(){

    }

    public void finalize() throws Throwable {
    }

    /**
     *
     * @param pass
     */
    public void InputPassword(char pass){

    }

    /**
     *
     * @param username
     */
    public void InputUsername(char username){
    }

    /**
     *
     * @param nameandpass
     */
    public void PromptNamePass(char nameandpass){

    }

    public void ValidateUser(){
```

UserDetails class has only Return(): UserDetails method that returns a value depending on the existence of user in the database.

```
public class UserDetails {

    public ServerApplication m_ServerApplication;

    public UserDetails(){

    }

    public void finalize() throws Throwable {
    }

    public UserDetails Return(){
        return null;
    }
}
```

ClientApplicationIdentification class has PI as its attribute and PromptPI(int), InputPI(), SendPI(), RequestIdDetails() and Display(): IdentityDetails as methods. After successful login, PromptPI (int) method is called to allow the user to input personal identifier. The identifier is accepted through the InputPI() method and then sent to the server application by the SendPI()

method. For a valid identity, a request for identity details is made to establish the owner of the identity. This is carried out by the RequestIdDetails() method. The Display(): IdentityDetails is the actual method that displays identity details to the user.

```
public class ClientApplicationIdentification {  
  
    private int PI;  
    public ServerApplication m_ServerApplication;  
  
    public ClientApplicationIdentification(){  
  
    }  
    public void finalize() throws Throwable {  
    }  
    public IdentityDetails Display(){  
        return null;  
    }  
    public void InputPI(){  
    }  
    /**  
     *  
     * @param PI  
     */  
    public void PromptPI(int PI){  
    }  
    public void RequestIdDetails(){  
    }  
    public void SendPI(){  
    }  
}
```

ServerApplication class has SubmitQueryPI(), SubmitQueryIdDetails() and Forward(): IdentityDetails methods. SubmitQueryPI() sends a query for searching Personal Identifier to Federated Server Object. SubmitQueryIdDetails() on the other hand sends a query to retrieve the details of a valid identity. Upon retrieving identity details, Forward(): IdentityDetails forwards these details to Client Application Identification interface for display.

```
public class ServerApplication {  
  
    public FederatedServer m_FederatedServer;  
  
    public ServerApplication(){  
    }  
    public void finalize() throws Throwable {  
    }  
    public IdentityDetails Forward(){  
        return null;  
    }  
    public void QueryUserDetails(){  
    }  
    public void SubmitQueryIdDetails(){  
    }  
    public void SubmitQueryPI(){  
    }  
    public boolean ValidateUser(){  
        return false;  
    }  
}
```

FederatedServer class has methods QueryPI(), ValidatePI(), OptimizeQueryIdDetails() and Forward():IdentityDetails. QueryPI() checks the existence of PI in the Federated Database. The existence status of PI is reported by ValidatePI() method. OptimizeQueryIdDetails() determines the best way to execute queries with a view to improving performance. Forward():IdentityDetails moves the retrieved identity details towards Client Application Identification Interface so that they can be displayed to the User.

```
public class FederatedServer {  
    public FederatedDatabase m_FederatedDatabase;  
    public FederatedServer(){  
    }  
    public void finalize() throws Throwable {  
    }  
    public IdentityDetails Foward(){  
        return null;  
    }  
    public void OptimizeQueryIdDetails(){  
    }  
    public void QueryPI(){  
    }  
    public boolean ValidatePI(){  
        return false;  
    }  
}
```

FederatedDatabase class has InvokeWrapper() and Return():PI methods. InvokeWrapper() calls a database wrapper to establish a connection to external identity data sources. Return():PI sends retrieved personal identifier to Federated Server for validation.

```
public class FederatedDatabase {  
    public Wrapper m_Wrapper;  
    public FederatedDatabase(){  
    }  
    public void finalize() throws Throwable {  
    }  
    public void InvokeWrapper(){  
    }  
    public PI Return(){  
        return null;  
    }  
}
```

The Wrapper class has ExecuteQueryIdDetails() and Return():IdentityDetails methods. ExecuteQueryIdDetails() method submits queries to the data source in SQL or the native query

language of the source and thereafter receives the query results sets. The results are returned by Return():IdentityDetails method.

```
public class Wrapper {
    public Wrapper() {
    }
    public void finalize() throws Throwable {
    }
    public void ExecuteQueryIdDetails() {
    }
    public IdentityDetails Return() {
        return null;
    }
}
```

4.3.1.4 Data Model

The *Database Model* describes the data that must be stored and retrieved as part of the overall system design as shown in figure 4.15.

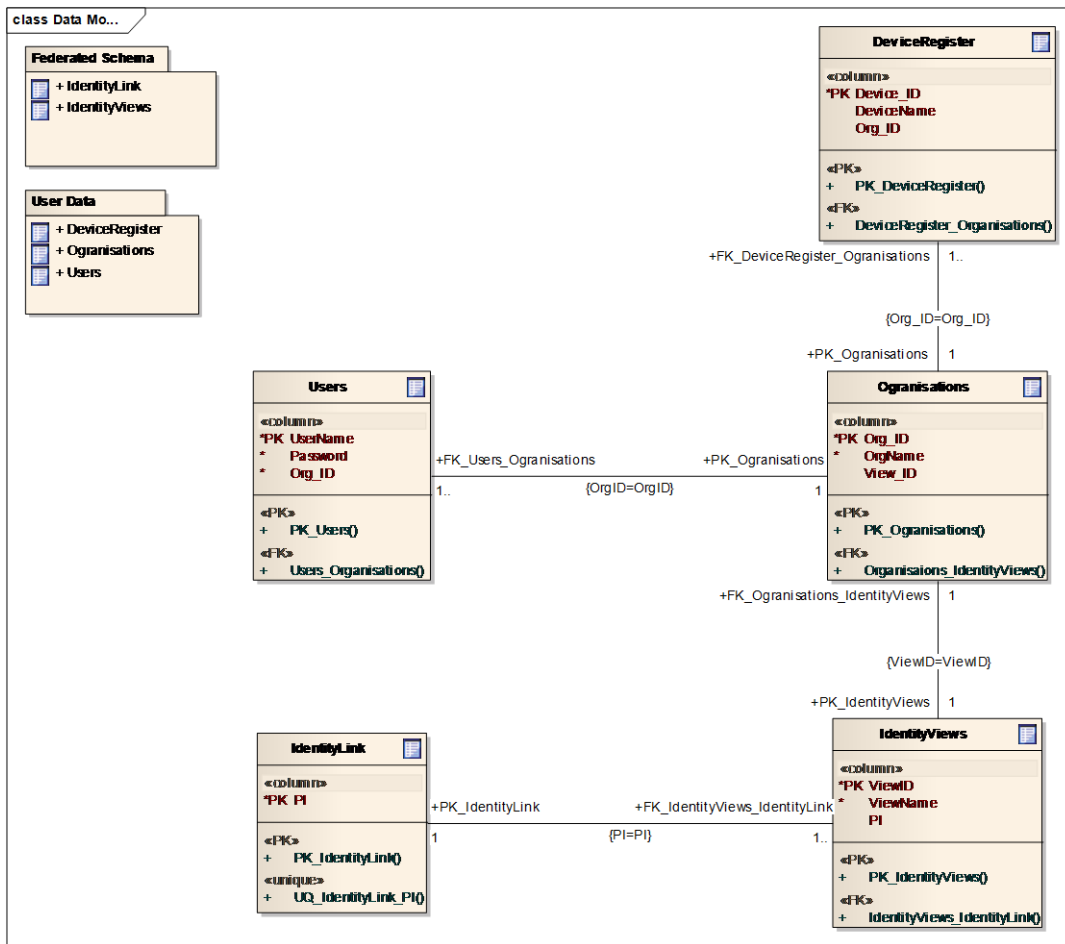


Figure 4. 15: Data Model

This model has Federated Schema and User Data packages. Federated Schema contains IdentityLink and IdentityViews table objects. IdentityLink contains personal identifiers that allow the creation of identity views from the identity providers' databases. User Data on the other hand contains DeviceRegister, Organisations and Users tables. DeviceRegister stores registration details of devices that are allowed to connect to ISPIS system. Users table has details of ISPIS users. Each user belongs to an organisation and each organisation has been assigned specific identity views. Therefore a user is allowed to see only identity details assigned to his/her organisation.

4.3.1.5 Component Model

The main components of the ISPIS systems are client application, server application and federation manager. The federation manager is composed of a federation server and a data wrapper. Further, the federation server has federated database and a federated database engine as its sub-components. Figure 4.16 presents a high level definition of the component model.

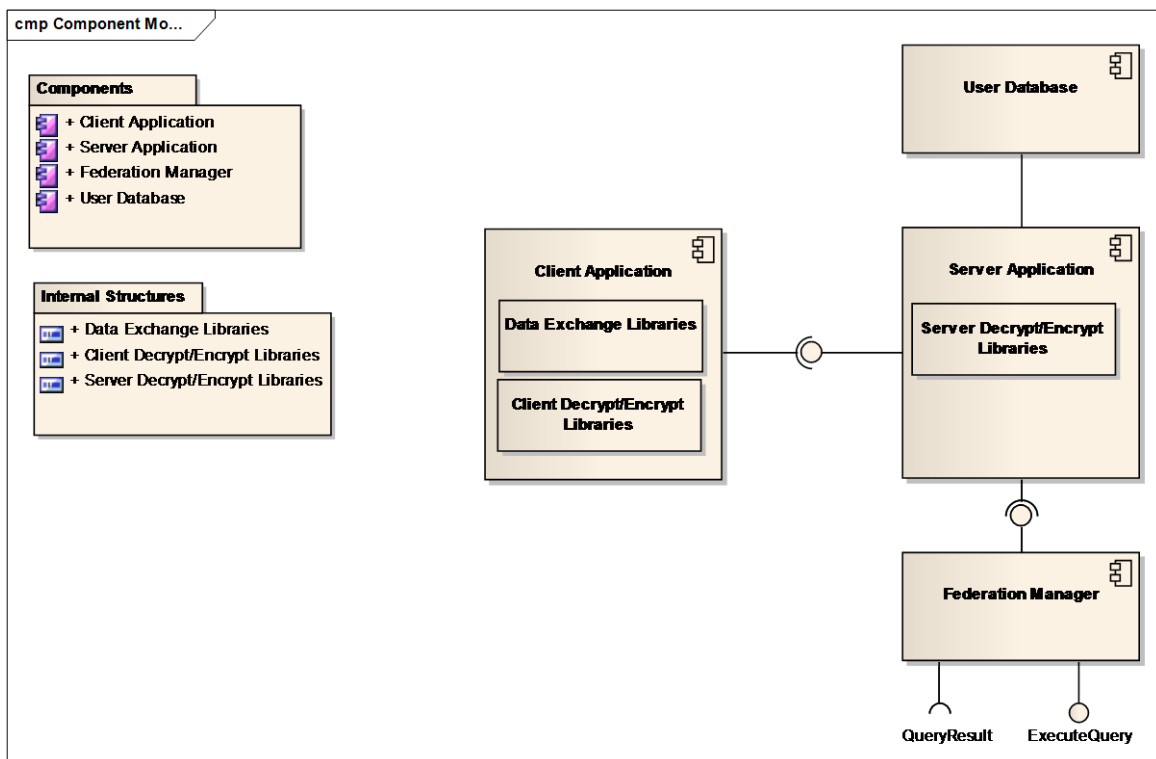


Figure 4. 16: Component Model

The *client application* provides an interface through which users interact with the system. It contains communication and cryptographic protocols for reading encrypted personal identifiers from identity tokens. It is also able to extract biometric data captured through biometric readers. The *identity token* contains digitized data about its owner such as personal identification number, full name and photo. It also has data exchange libraries that allow identity data to be automatically transferred to the client application. This token is an electronic identity card readable by end user devices on close proximity. There are two versions of the client application: one designed for personal computer and the other for mobile phone.

The *server application* provides the business logic for the client application. It processes request from the client application and re-routes them to the federation manager, and vice versa. Additionally, it does encryption and decryption of data to and from the client application. It therefore acts as a middleware between the client application and the federation manager. Figure 4.17 shows the main components of the federation manager.

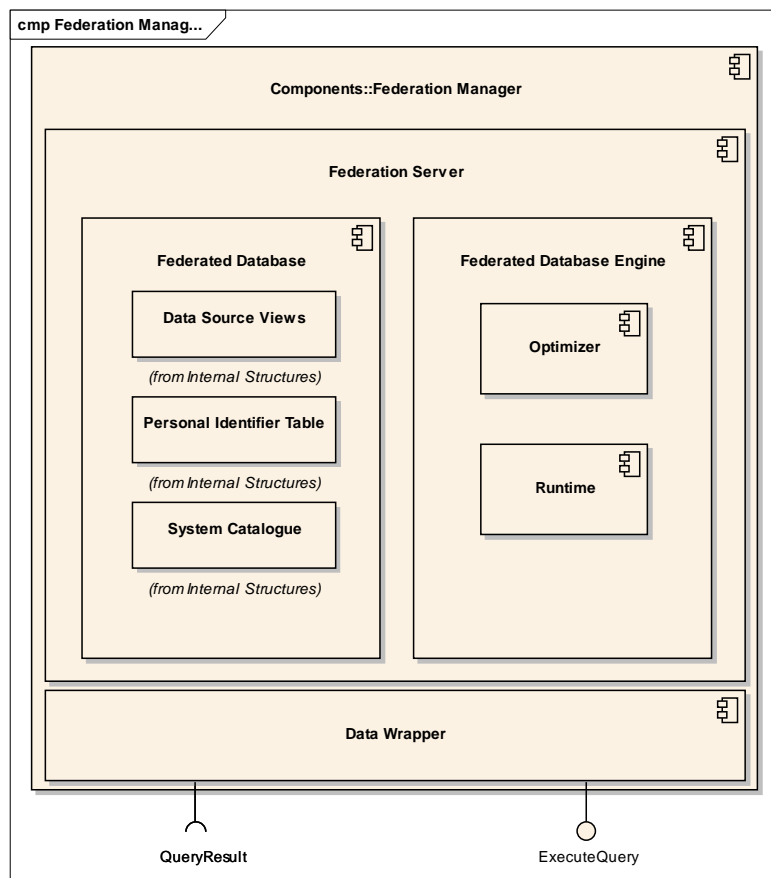


Figure 4. 17: Federation Manager

The Federation Manager contains a *federation sever*, which is a database instance that responds to requests from client applications through the server application. It often sends parts of the requests it receives to data sources for processing. Application processes connect and submit requests to the database within the federation server. It is configured to receive requests that might be partially or entirely intended for data sources and distributes them to the data sources. It uses the native client of the data source to access the data source. For example, it will use the Microsoft SQL Server ODBC Driver to access Microsoft SQL Server data sources.

The *federated database* is managed by the federation server. It contains a *system catalogue* that stores information about data. This catalogue contains entries that identify data sources and their characteristics. The federation server consults the information stored in the system catalogue and the data source wrapper to determine the best plan for processing SQL statements. The federated system processes SQL statements as if the data from the data sources were ordinary relational tables or views within the federated database. It also contains a table of personal identifiers which provides the actual link to identity data in the remote data sources.

The *Federated Database Engine* is the underlying software component that the federated database management system will use to store and retrieve data from the database. It is mainly composed of a query optimizer and runtime libraries. The *optimizer* is the component that determines the best way to execute each query. It considers the various possible strategies, modelling the likely cost of each, and choosing the one with the least cost (cost is measured in terms of system resources consumed). In a federated system, the optimizer must decide whether the different operations involved in a query should be done by the federation server or by the source where the data is stored. It must also determine the order of the operations, and what implementations to use to do local portions of the query. To make these decisions, the optimizer must have some way of knowing what each data source can do, and how much it costs. For example, if the data source is a file, it would not make sense to assume it was smart, and ask it to perform a sort or to apply some function. On the other hand, if the source is a relational database system capable of applying predicates and doing joins, it might be a good idea to take advantage of its power if it will reduce the amount of data that needs to be brought back to the federated engine. This will typically depend on the details of the individual query. It works with the wrappers for the different sources involved in a query to evaluate the possibilities. Often the

difference between a good and a bad decision on the execution strategy is several orders of magnitude in performance. As a result, users can expect the best performance possible from their federated system. To further enhance performance, each wrapper implementation takes advantage of the operational knobs provided by each data source using the source's native API. The query compiler will communicate with the wrapper to indicate which query fragments can utilize block fetch and thus achieve the maximal performance at runtime without loss of query semantics. The *runtime* component therefore executes a query execution plan generated by the optimizer. It accesses the objects being referenced by the SQL statement according to the query plan.

A *Data Wrapper* is a mechanism by which the federated database interacts with data sources. It connects to the data source using standard connection Application Programming Interface (API) of the data source. After successful connection, it submits queries to the data source in SQL or the native query language of the source or into a series of source API calls and thereafter receives the query results sets using standard APIs. Another wrapper function is to respond to federated database queries about the default data type mappings for a data source. The wrapper contains the default type mappings that are used when remote table names are created for a data source object. For relational wrappers, data type mappings that are created override the default data type mappings. User-defined data type mappings are stored in the system catalogue. It responds to federated database queries about the default function mappings for a data source. The federated database needs data type mapping information for query planning purposes. The wrapper contains information that the federated database needs to determine if central database functions are mapped to functions of the data source, and how the functions are mapped. This information is used by the SQL Compiler to determine if the data source is able to perform the query operations. For relational wrappers, function mappings that are created override the default function type mappings. User-defined function mappings are stored in the system catalogue.

The *user database* contains details of the system users. These include user biographical information, their organizations/institutions, and access privileges.

4.3.1.6 Deployment Model

A *Deployment diagram* shows how and where the system is to be deployed; i.e., its execution architecture. Hardware devices, processors and software execution environments are reflected as Nodes, and the internal construction can be depicted by embedding or nesting Nodes. Application software and associated files are reflected as artifacts.

The client application artifact is deployed to the end user device (i.e. personal computer or smartphone). This application connects to the server via a GPRS connection over HTTP protocol. Server Application and User Database are deployed in a high performance application server. This server performs most of the processing tasks. The Federation Database Engine, Federated Database and Data Wrappers are deployed in the Federation Server. Figure 4.18 shows the deployment model.

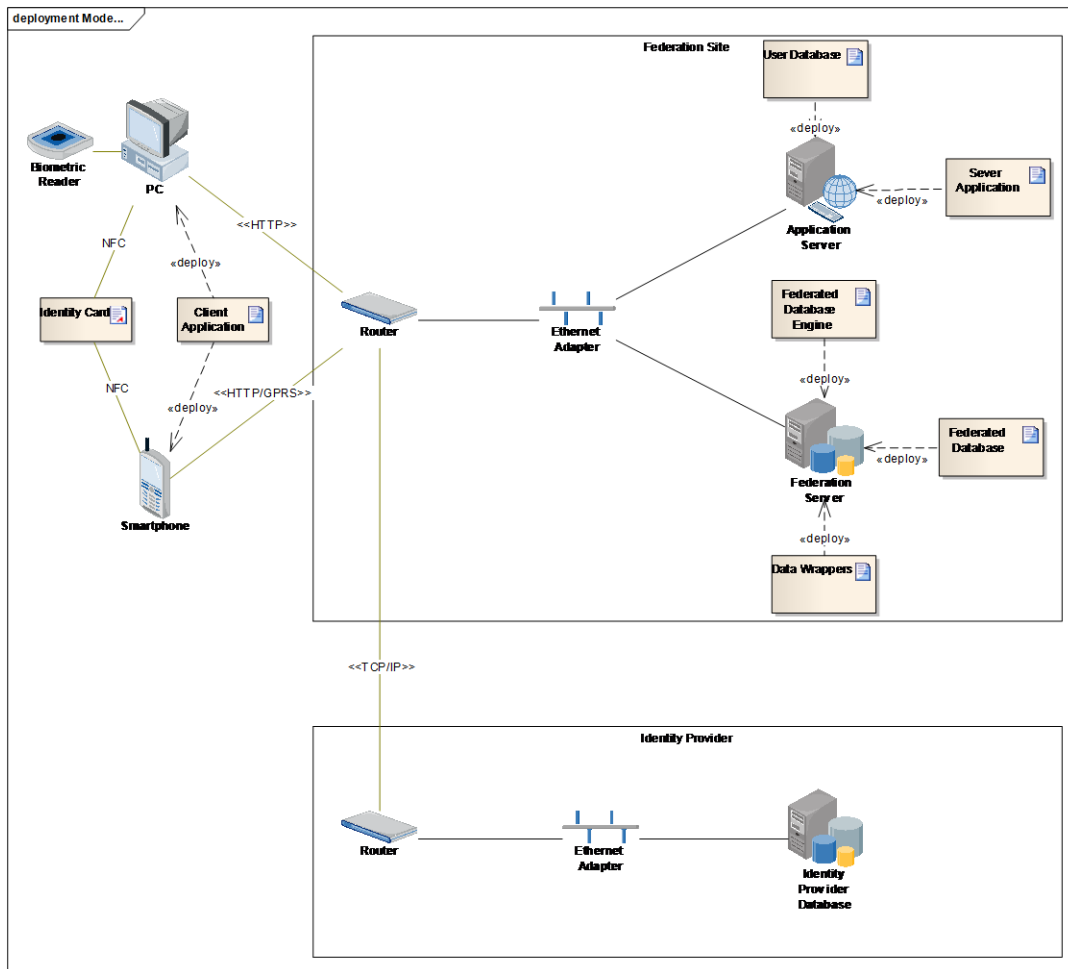


Figure 4. 18: Deployment Model

The system allows both token-based and biometric-based identifications. In token-based identification, an Identity Card is read by the client application upon holding it close to end user device (i.e. Personal Computer or Smartphone). The automatic reading of an ID card is enabled by Near Field Communication (NFC) technology. NFC operates at a shorter distance of about 4 inches (10 centimetres) at 13.56 MHz and data transfer rate of up to 424 Kbits per second. NFC standards are based on different communications protocols and data exchange formats, including existing radio-frequency identification (RFID) standards such as the ISO/IEC 14443, which is specific to identification cards, proximity cards and contactless integrated circuit cards.

Modern computing devices such as smartphones and personal computers produced today are NFC-enabled. NFC implementation in personal computers is however still immature as compared to smartphones. A smartphone is capable of performing many of the computer functions. It has a relatively large screen and an operating system that can run general-purpose applications. Being NFC-enabled, means that a user need to only place the identity card (NFC card) close to it and wait for identification results. An NFC card has a chip that stores identity data and an antenna for communicating with the NFC Smartphone. This phone is typically composed of integrated circuits, Secure Element(s) and an NFC Interface.

The NFC interface is made up of a contactless front end called an NFC Contactless Front-End (NFC CLF), an NFC Antenna and NFC Controller for enabling NFC transactions. There is at least one Secure Element (SE) in an NFC-enabled phone which is connected to the NFC controller for performing secure proximity transactions with external NFC devices. The SE provides a dynamic and secure environment for programs and data. It enables secure storage of valuable and private data. More than one SE can be directly connected to the NFC controller. The supported common interfaces between SEs and the NFC controller are the Single Wire Protocol (SWP) and the NFC Wired Interface (NFC-WI). The SE can be accessed and controlled from the host controller internally as well as from the Radio Frequency (RF) field externally. The host controller (baseband controller) is the heart of any mobile phone. Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The host controller sets the operating modes of the NFC controller through the HCI, processes data that are sent and received, and establishes a connection between the NFC controller and the SE. Figure 4.19 shows a high-level the architecture of an NFC-enabled mobile phone.

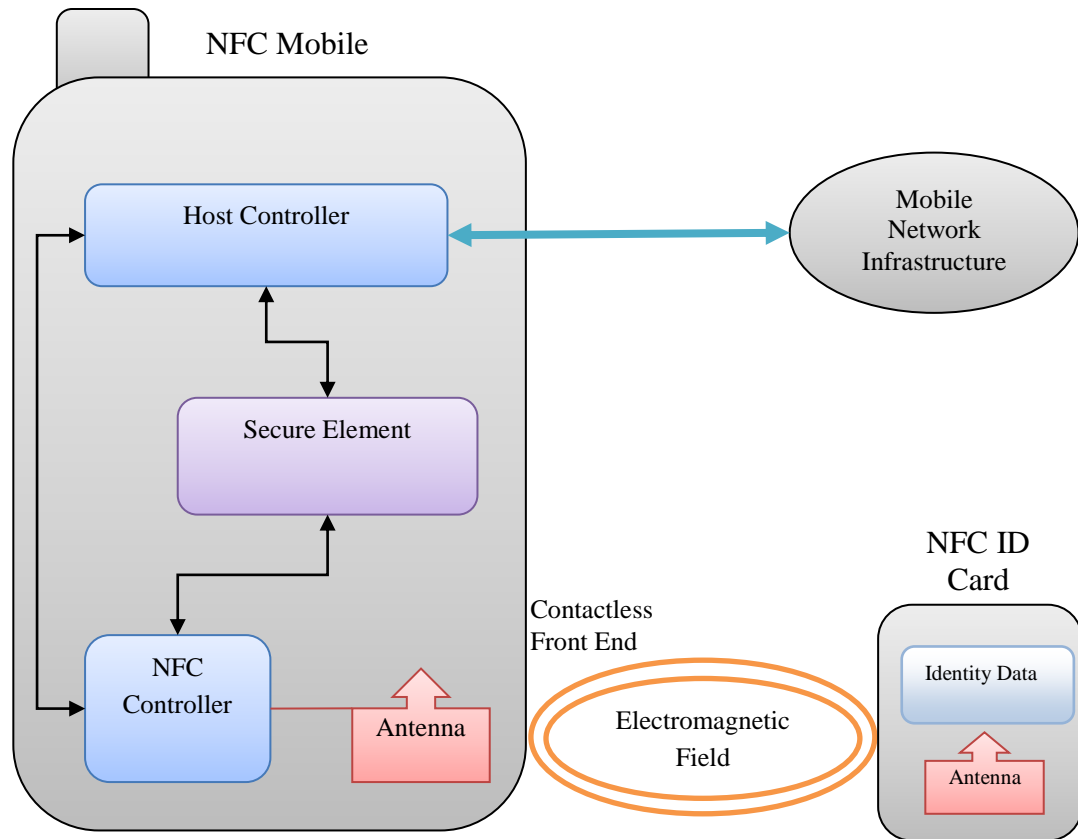


Figure 4. 19: Architecture of NFC-Enabled Phone

The Secure Element (secure memory and execution environment) is a dynamic environment in which application code and application data can be securely stored and administered and in which secure execution of applications occur. The element resides in highly secure crypto chips (usually a smart card chip). The element provides delimited memory for each application and other functions that can encrypt, decrypt, and sign the data packet. The secure element could be implemented either by a separate secure smart card chip (currently implemented in most of the NFC-enabled mobile phone pilots), in the SIM/UICC (which is used by GSM mobile phone operators to authenticate subscribers on their networks and maintain personalized subscriber information and applications), or in an SD card that can be inserted in the mobile phone.

In biometric-based identification, a biometric system recognizes an individual's physical characteristics such as face, fingerprint and iris by acquiring biometric data from the individual, extracting a feature set from the acquired data, and comparing this feature set against the

template set in the database. Biometric system operates either in verification mode or identification mode.

In the verification mode, the system validates a person’s identity by comparing his captured biometric data with that of his own biometric template(s) stored in the federated database. An individual would normally claim a certain identity usually via a personal identification number (PIN) or a smart card, and the system performs a one-to-one comparison to determine whether the claim is true or not. This mode of verification is used for positive recognition and is aimed at preventing multiple people from using the same identity.

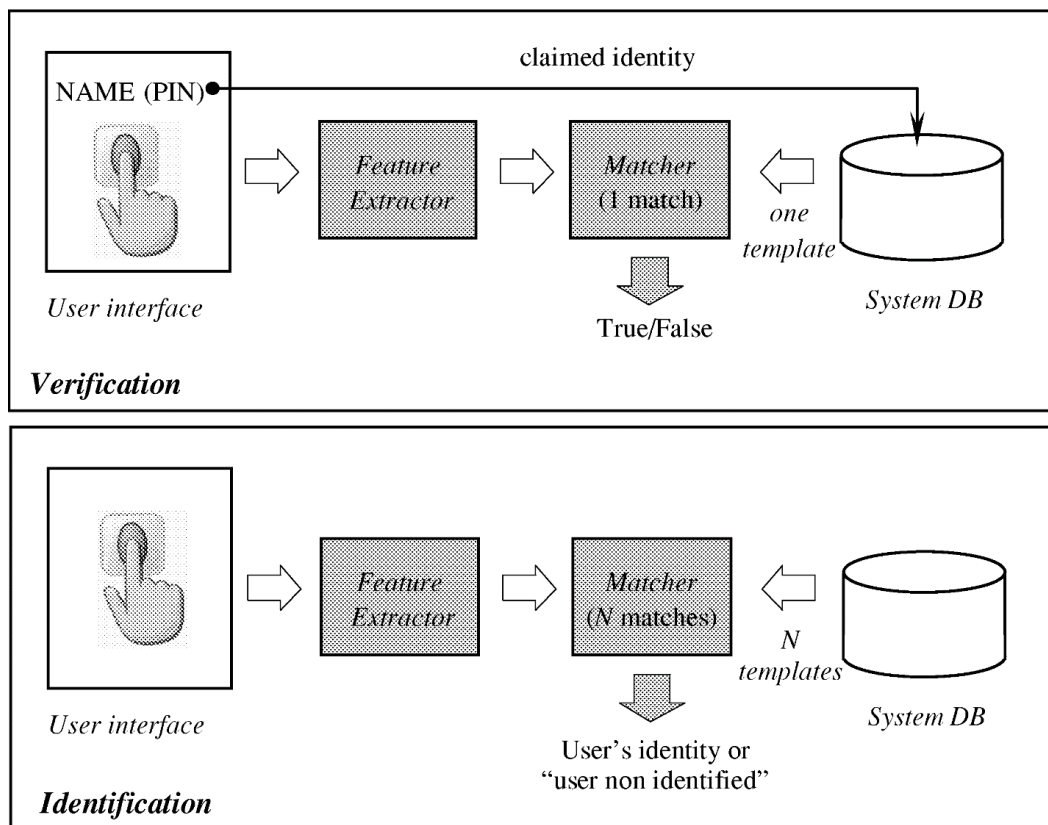


Figure 4. 20: Biometric Verification and Identification

In the identification mode, the templates of all the users in the database are searched for a match. In this way, the system performs a one-to-many comparison to establish an individual’s identity without the individual having to claim an identity. This mode is a critical component in negative recognition where the system establishes whether the person is who he/she denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities.

While token-based identification may work for positive recognition, negative recognition can only be established through biometrics.

4.3.2 Identity Provider View

This view presents the processes that take place at the side of identity provider, which include electronic registration of identity data, its transmission and subsequent storage, as described in the following work flow.

- i. The applicant submits relevant registration support documents to the identity registrar for verification.
- ii. If the documents are in order, the applicant's biometric identifier (e.g. fingerprint, iris or face) is searched in the federated identity database to confirm if it's already registered. For an applicant who is a child, her parent's biometric identifier is searched. The system is designed in such a way that a child's identity information is able to link with that of her parent(s). If the documents are not in order, the applicant is advised accordingly.
- iii. If the identity exists in the database, the process is terminated or an update on the identity is done.
- iv. If the identity is not in the database, an append screen is activated to allow for the creation of a new record.
- v. This record is saved in the local identity database. A unique personal identifier is generated for the record and saved in the federated identity database as well. For applicants who have reached the mandatory age of submitting biometric data, the biometric identifier is captured and a copy is saved to the federated identity database.

Figure 4.21 below presents a workflow diagram of an Identity Provider.

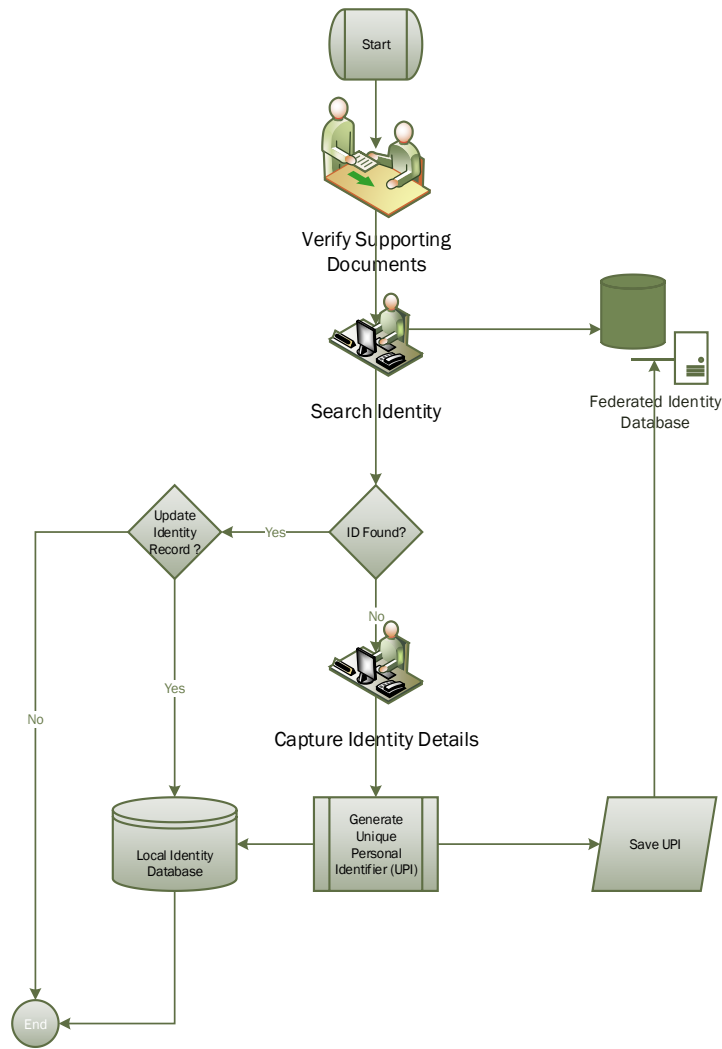


Figure 4. 21: IdP System workflow

4.3.2.1 Identity Registration Technologies

a) Civil Data Acquisition

Civil data is entered into the identity database via an application user interface. A return screen is provided to enable the applicant confirm the correctness of the captured data. Figure 4.22 shows how a laptop computer can be connected to a return screen via a dual display adaptor.



Figure 4. 22: Picture of Return Screen

b) Biometric Data Acquisition

Biometric data is captured using biometric acquisition devices. The main types of biometrics that can be captured are fingerprints, iris and face.

c) Fingerprint Acquisition

Ten (10) flat fingerprints set are captured using a fingerprint sensor. The biometric software ensures that fingerprints are captured in correct sequence. The software performs automatic quality control on fingerprint images and converts them into templates of minutiae in compliance with international standards (ISO19794-2) to allow for use in Automated Fingerprint Identification System (AFIS). It also provides live feedback to the data capture operator instructing the proper placement of fingers. During enrolment, an individual's fingerprint is placed on a fingerprint scanner to produce digital representation of the print. A fingerprint extractor processes the digital representation into a compact but expressive representation called a template which facilitates matching. The template is stored in a biometric database. Figure 4.23 shows the process of enrolling a fingerprint.

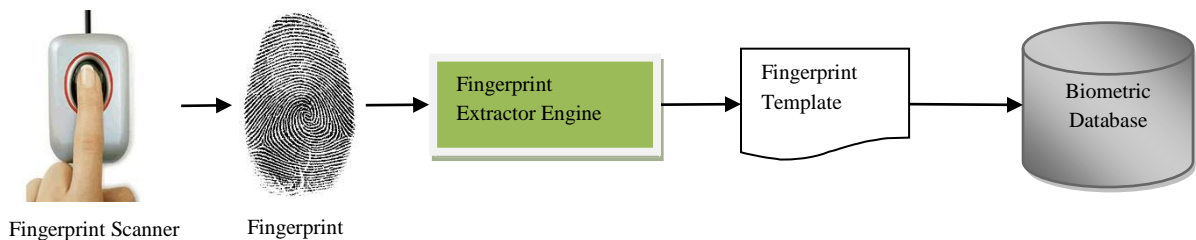


Figure 4. 23: Fingerprint Enrolment

d) Iris Acquisition

Iris is the colored ring on the human eye between the pupil and the white sclera as shown in figure 4.24.

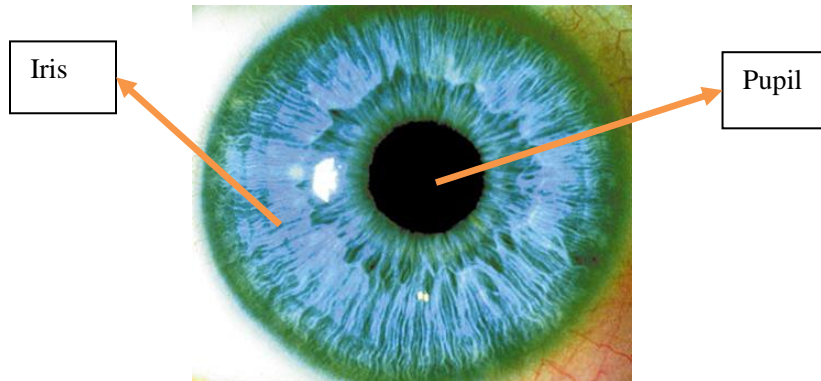


Figure 4. 24: Human Iris

Most iris scanners capture good quality data at a distance of about 4cm to 13cm under a good illumination environment. The person whose iris is to be captured is required to fully cooperate. This decreases the quantity of iris pre-processing and improves its ability to be recognized. Figure 4.25 shows the main stages of capturing correct iris biometrics.

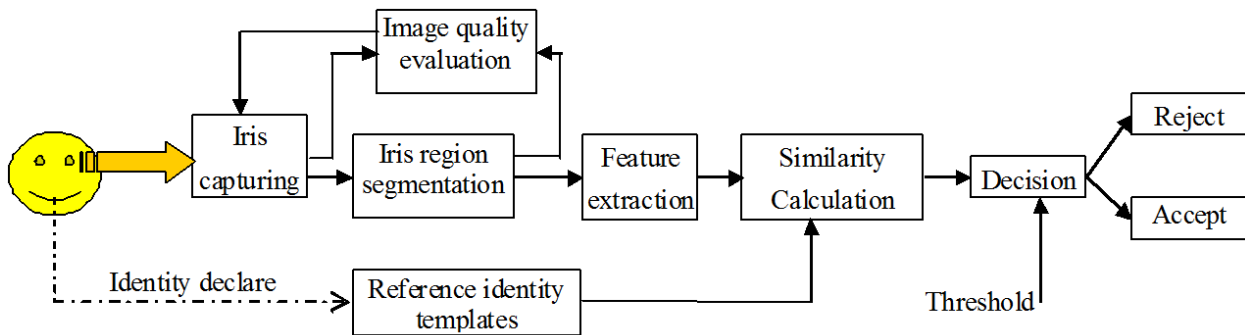


Figure 4. 25: Iris Acquisition System

e) Face Acquisition

The process of capturing a face as an identifier is based on the standard biometric sequence of image acquisition, image processing, distinctive characteristic location, template creation, and matching. An image is captured through a high-resolution camera, with moderate lighting. The person whose face is to be captured has to face the camera directly.

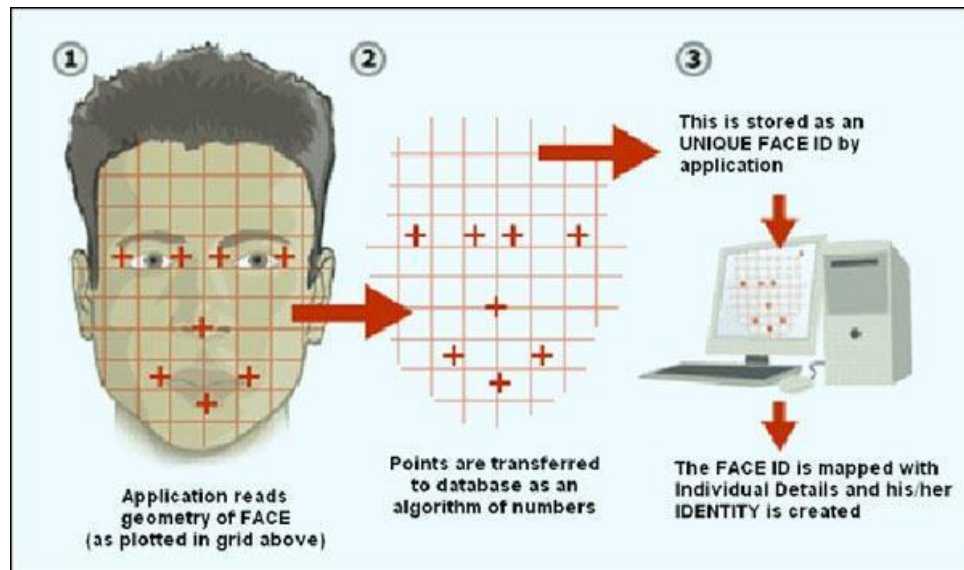


Figure 4. 26: Face Acquisition

Most facial biometric algorithms are based on either the geometrical approach or the pictorial approach. The geometrical approach is based on geometrical relationship between facial landmarks, or in other words the spatial configuration of facial features. The main geometrical features of the face such as eyes, nose and mouth are first located. Faces are then classified on the basis of various geometrical distances and angles between features. The pictorial approach on the other hand is based on the photometric characteristics of image. The method uses the templates of the major facial features and entire face to perform recognition on the front view of face.

f) Photo Capture

Photographs are captured using digital cameras. International standards (such as ISO/IEC FCD 19794-5) define the requirements of good quality photographs. The quality of the photo is verified and corrected during enrolment.

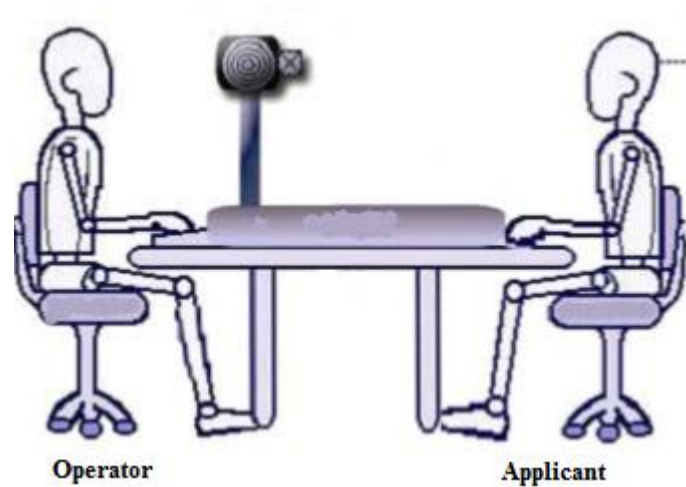






Figure 4. 27: Correct Photo Capture Position

g) Signature

The electronic signature is captured digitally using a digital signature pad. An example of a signature pad is provided in Table 4.20.

Table 4. 20: Examples of Modern Data Capture Devices

	Name	Function	Image
1.	Integrated mobile Registration Kit	Capturing biographic and biometric data	
2.	Biometric Tablet	Capturing and verifying fingerprint and face images	
3.	Signature Pad	Capturing digital signatures	
4.	Iris Camera	Capturing digital photo of the iris pattern and recreating an encrypted digital template of that pattern	

h) Supporting Documents

The enrolment station software allows scanning and creation of digitized documents. The software checks and validates the quality of scanned images. The digitized documents are linked to the applicant's civil and biometric records but archived in an electronic document management system.

4.3.2.2 Data Transmission

Data captured during registration/enrolment is transmitted to the respective identity provider's central database through wired and wireless networks. Real-time transmission is preferred though batch and offline transmission may be used where network connectivity is poor.

4.3.2.3 Data Integration

Identity Provider databases are linked to the federated database through appropriate integration architecture as shown in Figure 4.28.

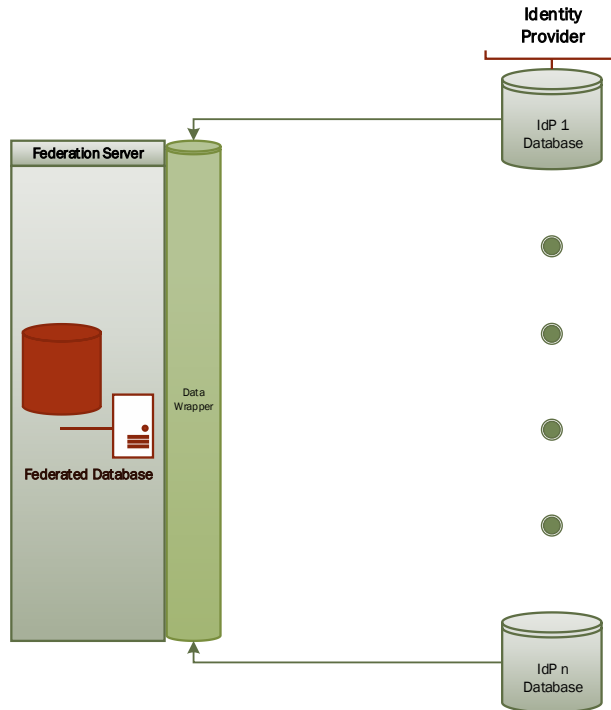


Figure 4. 28: Database Integration

4.3.3 Security View

The security architecture of ISPIS presented in Figure 4.29 was designed from Chappelle (2013) security in depth reference architecture. The architecture comprises a series of platforms and infrastructure that apply and enforce security controls, an enterprise security framework that manages security, and a set of security interfaces that enable communication between security components. Secure computing platforms and inter-communications throughout the processing chain enable each node in the chain to inject security controls in order to protect data in use, in transit, and at rest. Thus data is protected from end to end, starting from the end user devices through all processing nodes, networks and databases, all the way to offline backup media.

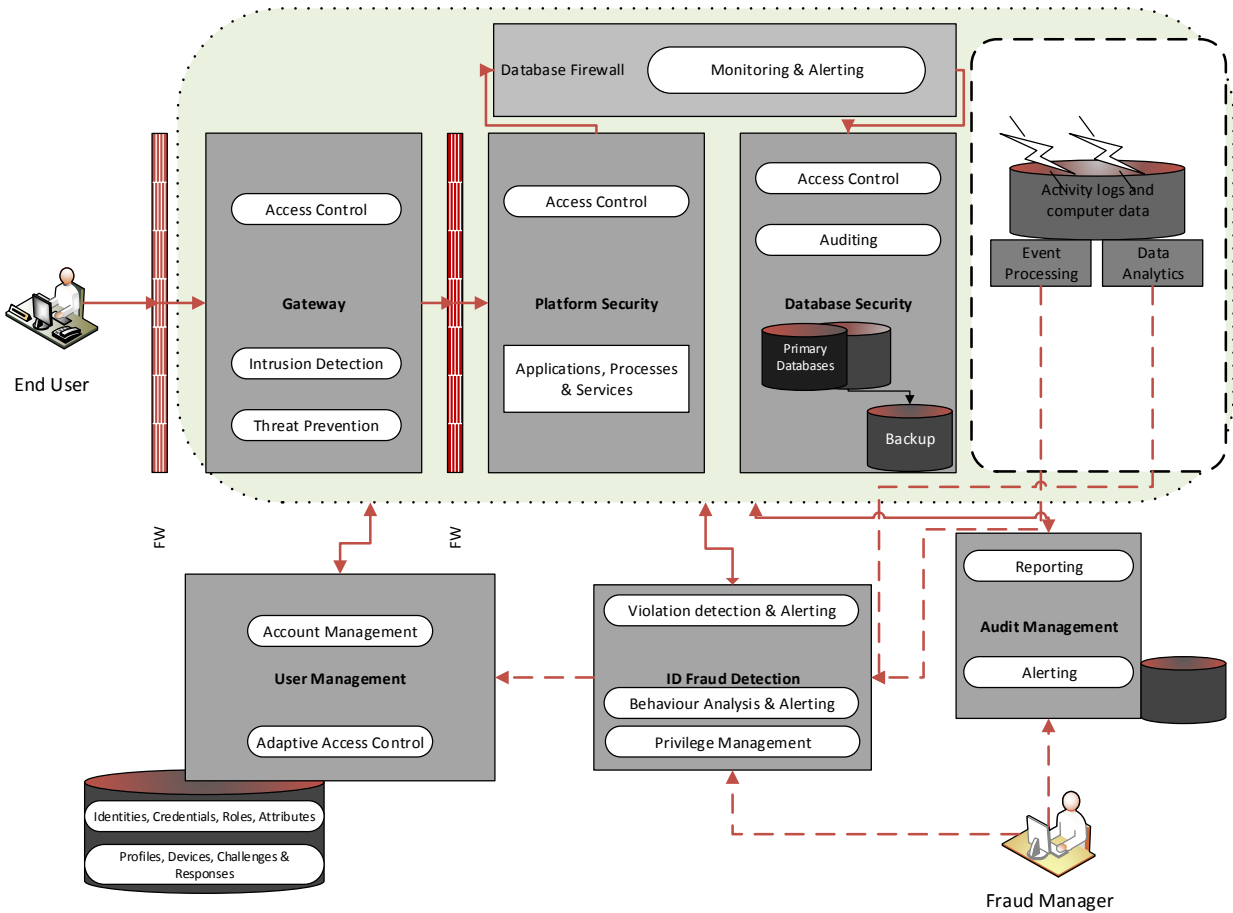


Figure 4. 29: ISPIS Security Model

4.3.3.1 Infrastructure Security

a) End User Device Security

Physical security is the first line of defence for end user devices. These devices are kept in well secured rooms. Access to each device is through login credentials. The credentials whether local to the computer or stored on an authentication server, are used by authorized users only. Anti-malware software is installed in each user device to protect them against viruses, worms, Trojan horses etc. Additionally, users connect with other computers and servers using secured protocols only. Personal firewall is installed on the end user device to protect it from attacks that get through, as well as attacks that originate from within the corporate network.

b) Gateway security

The gateway component adds fraud detection capabilities by examining inbound requests. It inspects messages and payloads looking for potential signs of hacking. Common attacks, such as malformed content, recursive payloads, and cross-site scripting, are thwarted before they result in any actual fraudulent activity. The gateway is designed to handle multiple delivery channels such as standard HTML, Web Services, and mobile devices.

c) Platform Security

A common management platform is defined that provides access to platform configurations, logs, and settings. It provides a way to manage configurations and patching across the whole environment. This makes it easier to ensure that critical security patches are being installed on all platforms and that configurations are maintained according to recommended security practices.

d) Database Security

ISPIS has a secure database management system that controls access to data via programmatic interfaces as well as by privileged users. The DBMS supports programmatic access control at the row and/or column level. Access controls are also applied to administrative functions performed by privileged users. They allow the configuration of privileges based on administrative role, and can enable administrative functions without providing access to the actual data. Access can also be maintained on tables and schemas, providing further segregation

of administrative duties. In addition, the identity and access management component provides the capability to manage and track administrative user access by issuing one-time passwords for administrative access. Access control is applied at other layers of the architecture as well. Attempts to access data by end-users pass through several components that perform authentication and/or authorization.

The database firewall provides both active and passive security controls to protect the database from inappropriate access. It is used to actively filter out SQL requests that are deemed unsafe, such as nested statements that are typically used in SQL Injection attacks. It can also passively monitor SQL traffic, generate reports, and send alerts.

e) Network Security

The data security architecture supports encryption between all components of the architecture. This is accomplished using transport layer security (TLS), message level security, (such as XML-Encryption within Web Service Security), or a combination of both. Encryption is handled by the platforms, allowing it to be configured easily, and eliminating the need to provide such functions with custom-developed code. Encryption is also used to protect data at rest. Data can be automatically encrypted when it is stored to disk or backup media. This protects the data from disclosure that could occur through the use of disk or tape scanning tools. Disk encryption is performed during write operations in a way that greatly minimizes latency, making it virtually transparent to the end users. In addition, key management techniques are used to enable the easy rotation of encryption keys and the management of large numbers of keys across backup devices. To further protect data where encryption is not possible, the architecture supports data masking. This allows sensitive information to be transposed in a manner that will not hinder ordinary database operations, such as maintaining referential integrity and data type constraints. Data values are changed yet conform to schema requirements, allowing database extracts that ordinarily contain sensitive data to be used for development and testing purposes.

4.3.3.2 Security Management

a) User management

The architecture includes a component for managing user privileges. Privileges are managed from a common governance platform. When a privileged user requires access, the system will generate and set the password for the target resource, and then provide the password to the user. When the user is finished with the resource, the system will reset the password on the target resource. This helps with fraud detection by tracking access via group administrative user accounts down to individual users. The identity of the user can be passed along from one component of the architecture to another in order to authorize (grant or deny) requests and to identify users for auditing purposes. Each platform adds an additional layer of security, transparent to the end user.

b) Audit Management

The architecture includes a centralized audit management point that enables the tracking of information access and changes as well as administrative operations that could be used to compromise data security. This is facilitated by a robust audit management system. The system collects audit records and securely manages them in an audit database. Further, it supports the reporting and analysis of audit records across multiple databases.

c) Fraud Detection

The system has several components that are used to detect and prevent fraudulent activities from happening. The gateway component as described above detects fraud by examining inbound requests. An adaptive access control component examines the context of the authentication request. If conditions appear normal, then authentication will proceed as usual. However, if conditions are questionable, then a stronger authentication mechanism may automatically be triggered. Likewise if conditions are unacceptable, e.g. a blocked user id, then authentication is rejected entirely. Since all platforms provide access control, and access control is provided via a common enterprise service, adaptive access can be incorporated and managed across the enterprise from a single point in the architecture. Fraud detection is universally applied across all data sources and access channels. Fraudulent activity can be detected by

recognizing predictable patterns or through investigation and analysis. The architecture includes components to support both forms of fraud detection and to enable analysis and investigation of new and emerging threats. Patterns of behaviour that represent fraud can be correlated in an attempt to recognize when a problem is about to occur. Once a pattern has been identified it may be codified into an automated response.

4.4 Model Construction

The model prototype was constructed on ASP.NET platform. ASP.NET is a web platform that provides all the services required to build an enterprise-class server-based web application. This platform is built on the .NET Framework allowing applications to be written in any language that is compatible with the common language runtime (CLR). Visual Basic was used as the primary programming language for the prototype. Databases were created on MS SQL Server 2008R2, Oracle Express Edition 11g and MySQL version 5.6. Specifically, *birth registration database* was created on Oracle: *national registration and identification database* on MS SQL: *death registration database* on MySQL: and *virtual (federated) database* on MS SQL. The complete application was published on Internet Information Services (IIS) version 7.5.

4.4.1 System Architecture

The prototype was built on a 4-tier architecture comprising of a Presentation Tier, an Application Tier, a Federation Tier and a Data Management Tier as shown in figure 4- 31 below.

Presentation Tier

The Presentation Tier uses a web browser to provide the user with an interface for interacting with the backend databases through a web server. The web browser acts as a thin client which executes only a few of the application logic.

Application Tier

The Application Tier processes the various inputs and selections received by the web browser. It contains a web server (IIS Version 7.5) which hosts the server application and its supporting components. This tier implements the system's business logic (part of source code is found in **APPENDIX E**).

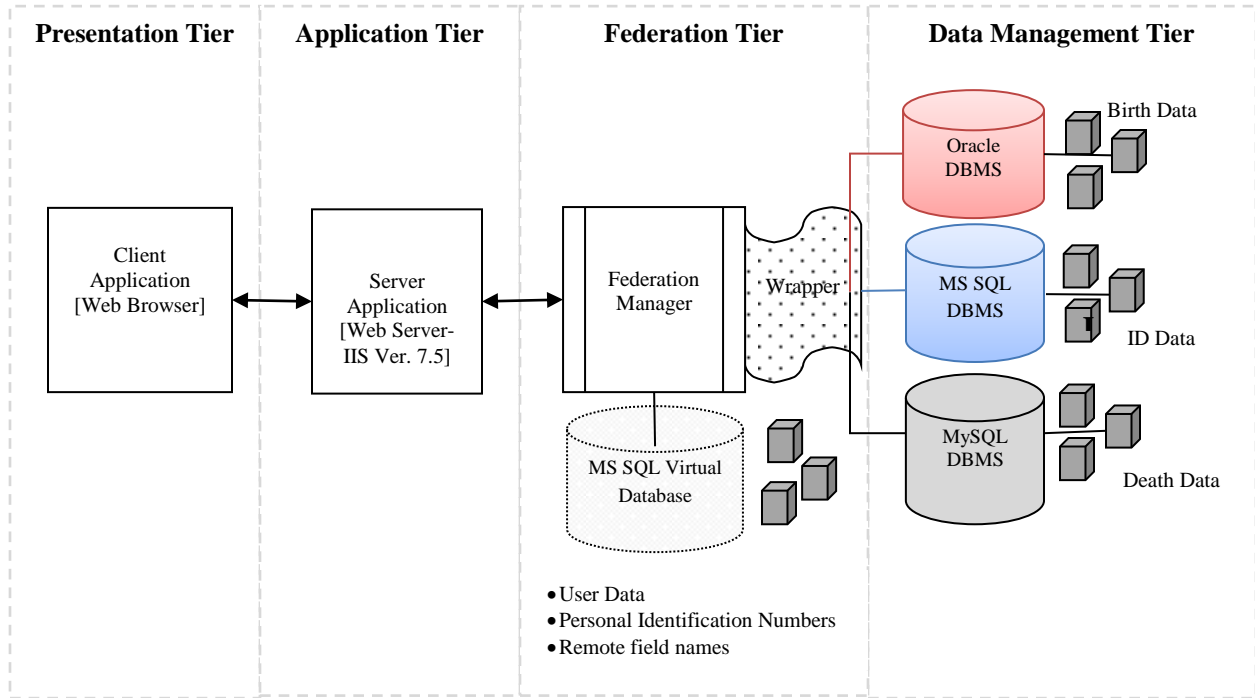


Figure 4. 30: ISPIS Prototype Architecture

Federation Tier

The Federation Tier comprises a virtual database through which the application accesses IdPs databases. This database contains user data, unique personal identifiers and remote table field names. These field names are used to create views to the IdPs databases. The field names are stored in a table called ‘RightsViews’ that was created through the following SQL script.

```

CREATETABLE [dbo].[RightsViews] (
    [Idxno] [numeric] (18, 0) IDENTITY (1,1) NOTNULL,
    [ViewDesc] [varchar] (100) NOTNULL,
    [ColumnName] [varchar] (100) NOTNULL,
    [ColumnDesc] [varchar] (100) NOTNULL,
    [Type] [varchar] (50) NOTNULL,
    [Priority] [int] NOTNULL
) ON [PRIMARY]

```

Table 4.21 below shows data entered into the ‘RightsViews’ table. The ViewDesc column contains names of IdPs database tables while the ColumnName column contains column names of the tables.

Table 4. 21: RightViews Table Data

ViewDesc	ColumnName	ColumnDesc	Type
National	Idno	Identity Card Number	string
National	Fname	Full Names	string
National	Dob	Date Of Birth	date
National	Sex	Gender	string
National	districtbirth	District Of Birth	String
National	dtissue	Date Of Issue	date
National	Photo	Photo	image
National	fingerprint	Finger Print	image
National	Signature	Signature	image
BirthDetails	Enumber	BirthCertificate Number	string
BirthDetails	Fnames	Full Names	string
BirthDetails	Dob	Date Of Birth	date
BirthDetails	Sex	Gender	string
BirthDetails	namefather	Name Of Father	string
BirthDetails	namemother	Name Of Mother	string
BirthDetails	nameinformant	Name Of Informant	string
BirthDetails	districtbirth	District Of Birth	string
BirthDetails	Regofficer	Registration Officer	string
BirthDetails	dtregistration	Date Of Registration	date
DeceasedDetails	Dno	Death Certificate Number	string
DeceasedDetails	Fnames	Full Names	string
DeceasedDetails	Dod	Date Of Death	date
DeceasedDetails	Sex	Gender	string
DeceasedDetails	Dplace	Place Of Death	string
DeceasedDetails	Nfather	Name Of Father	string
DeceasedDetails	nmother	Name Of Mother	string

Data Management Tier

The Data Management Tier comprises database management systems and IdPs databases. It provides data storage and access control functionality. Three databases: Birth Registration Database: National Registration and Identification Database: and Death Registration Database, were designed to simulate IdPs databases. They were created on different database management systems within the same computer.

The Birth Registration Database was created on Oracle DBMS with one table that was scripted as shown below.

```

CREATETABLE BIRTH.BIRTHDETAILS
(
  UPI          NUMBER (18) NOTNULL,
  FNAMES      VARCHAR2 (100BYTE) NOTNULL,
  DOB         DATENOTNULL,
  SEX         VARCHAR2 (10BYTE) NOTNULL,
  NAMEFATHER  VARCHAR2 (100BYTE) NOTNULL,
  NAMEMOTHER  VARCHAR2 (100BYTE) NOTNULL,
  NAMEINFORMANT VARCHAR2 (100BYTE) NOTNULL,
  DISTRICTBIRTH VARCHAR2 (100BYTE) NOTNULL,
  REGOFFICER  VARCHAR2 (100BYTE) NOTNULL,
  DTREGISTRATION DATENOTNULL
)

```

The National Registration & Identification Database was created on Microsoft SQL Server DBMS. It had one table that was scripted as shown below.

```
CREATETABLE [dbo].[IDDetails](
    [IDNo] [numeric](18, 0)NOTNULL,
    [FName] [varchar](100)NOTNULL,
    [DOB] [datetime] NOTNULL,
    [Sex] [varchar](10)NOTNULL,
    [DistrictBirth] [varchar](100)NOTNULL,
    [DTIssue] [datetime] NOTNULL,
    [Photo] [image] NULL,
    [FingerPrint] [image] NULL,
    [Signature] [image] NULL,
    [UPI] [numeric](18, 0)NOTNULL,
CONSTRAINT [PK_IDDetails] PRIMARYKEYCLUSTERED
)
```

The Death Registration Database was created on MySQL DBMS. It also had one table which was scripted as shown below.

```
CREATE TABLE `decdetails` (
  `dno` bigint(20) NOT NULL,
  `fnames` varchar(100) NOT NULL,
  `dod` datetime NOT NULL,
  `sex` varchar(10) NOT NULL,
  `dplace` varchar(200) NOT NULL,
  `nfather` varchar(100) NOT NULL,
  `nmother` varchar(100) NOT NULL,
  `UPI` int(11) NOT NULL,
  PRIMARY KEY (`dno`)
)
```

4.4.2 System Functionality

The application runs in any web browser. It has a login form that provides for inputting of user name and password. A user is required to enter a valid user name and password to be able to use the application.


The image shows a web-based login form. At the top left, there is a small yellow key icon. Below it, the form has two input fields: one labeled "UserName" and another labeled "Password". At the bottom of the form, there are two buttons: "Login" on the left and "Cancel" on the right. The form has a light blue background and rounded corners.

Figure 4. 31: Login Form

Every user has specific access rights which are assigned by a systems administrator. This is done through the form shown in Figure 4.32 below. The form shows the read rights assigned to a university in the Birth Registration database. A user from the university will have these rights.

Define Role-Access Rights

Select System Role: 01 University ▼

Select Type Of Right To Configure: Read Rights ▼ Save Rights

Select Database To Configure Read Rights For: BirthDetails ▼

System Module	Allow?	Module Code	Update Code	Functional Area
Birth Certificate Number	<input type="checkbox"/>	ENUMBER	0	Reads/Views
Full Names	<input checked="" type="checkbox"/>	FNAMES	1	Reads/Views
Date Of Birth	<input checked="" type="checkbox"/>	DOB	1	Reads/Views
Gender	<input checked="" type="checkbox"/>	SEX	1	Reads/Views
Name Of Father	<input type="checkbox"/>	NAMEFATHER	0	Reads/Views
Name Of Mother	<input type="checkbox"/>	NAMEMOTHER	0	Reads/Views
Name Of Informant	<input type="checkbox"/>	NAMEINFORMANT	0	Reads/Views
District Of Birth	<input type="checkbox"/>	DISTRICTBIRTH	0	Reads/Views
Registration Officer	<input type="checkbox"/>	REGOFFICER	0	Reads/Views
Date Of Registration	<input type="checkbox"/>	DTREGISTRATION	0	Reads/Views

Figure 4. 32: User Access Rights Assignment Form

The prototype was designed to allow for the protection of a persons' private data. The system administrator is able to restrict the data to be accessed by each user. For example, a university user would have a different access profile from that of a night club user. Figure 4.33 shows the details seen by a university staff using the system while Figure 4.34 shows those that are seen by a night club staff. In this case, a bouncer at the night club is only interested in verifying the age and photo of the person intending to enter a club and nothing more.

Current User :	Date :	Institution Name :	InstitutionType :
Kabarak	2014-2-5 15:56:33	Kabarak	University

Enter Personal Identifier:

Birth Certificate Details	
Full Names :	John Njoroge Kamau
Date Of Birth :	09-Apr-1981
Gender :	Male
National Identity Card Details	
Identity Card Number :	23000119
Full Names :	John Njoroge Kamau
Date Of Birth :	09-Apr-1981
Gender :	Male




Figure 4. 33: University Profile

Current User :	Date :	Institution Name :	InstitutionType :
Samba	2014-2-5 16:1:28	Samba	Night Club

Enter Personal Identifier:

National Identity Card Details	
Date Of Birth :	09-Apr-1981




Figure 4. 34: Night Club Profile

The ISPIS model was conceptualized from the model of a federated identity management system. This model allows different identity data to be distributed among service providers but linked up centrally by identifiers which facilitate data flow among them. The central linkage was provided by a virtual (federated) database that enables disparate identity databases to connect with each other.

Though the ISPIS model was guided by identity federation during its development, it resulted into a hybrid of the ‘Centralized Identity System model’ and the ‘Federated Identity System model’ called ‘CHERUS ISPIS Model’. The centralized management of identity data ensures that one trusted institution becomes the sole custodian of the system. If this institution is government, then the level of system acceptance is expected to be high since citizens have more trust in their government managing personal information as compared to it being managed by a private organization. On the other hand, the federated part of the model ensures that the security and privacy of data is upheld.

The management of identities through a federation has been tested in some countries. The Austria’s e-card system allows electronic healthcare records to be stored in a distributed fashion across several systems which are managed by different parties. This implementation was necessitated by the existence of a strong data protection law in Austria which requires that systems handling patient’s data should be able to preserve privacy. Similarly, Gulf Cooperation Council countries (i.e. Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and United Arab Emirates) teamed up to interoperate their identification systems with the objective of easing the provision of common services to their citizens. The difference between these systems and ISPIS is that apart from facilitating service provision, ISPIS a secure system and assists in combating identity fraud.

4.5 Model Verification

The process of model verification was aimed at determining whether or not the ISPIS model fulfilled the established requirements. This was undertaken in two stages: (a) Verification of functional requirements and (b) Verification of non-functional requirements.

4.5.1 Verification of Functional Requirements

Enterprise Architect's Relationship Matrix was used to verify the functional requirements. The matrix enabled the tracing of requirements from the Requirements Model down to the Component Model. Each model element represented a system requirement. The matrix rows defined the source elements while its columns defined the target elements. Each row element and its corresponding column element were linked together to enable backward traceability.

i). Requirement to Use Case Realisation

The first verification step involved establishing a mapping of the *Requirements Model* to the *Use Case Model*. Requirements and Use Case Models were set as source and target packages respectively. Specifically, the Functional Requirements package of the Requirements Model was chosen as the source and the Use Case Model as the target as shown in Figure 4.35. This choice was informed by the fact that functional requirements of a system can alternatively be described by use cases. In the relationship matrix, functional requirements are listed horizontally while use cases are listed vertically. The arrows in the diagram define which functional requirements are realized by which use cases. For example, the "Access Control" functional requirement is realized by the use case "Login". It is clear from the matrix that all functional requirements have corresponding use cases that realize them.

Relationship Matrix					
Source:	Functional Requirements	Type:	Requirement	Link Type:	Realisation
Target:	Use Case Model	Type:	UseCase	Direction:	Source -> Target
			Use Cases::Connect		
			Use Cases::Identify a Person		
			Use Cases::Login		
			Use Cases::Validate a Person's Identity		
			Use Cases::Verify a Person's Identity		
	Access Control::The system shall allow access to authorized users only				↑
	Connectivity::The end user device shall connect to both wired and wireless data networks		↑		
	Identification::The system shall validate and verify an identity			↑	
	Identity Validation::The system shall check the existence of personal identifiers in a master identity database				↑
	Identity Verification::The system shall retrieve and display information details of an identity from the IdPs databases				↑

Figure 4. 35: Functional Requirement to Use Case Realisation

ii). Use Case to Class Realisation

The second verification step involved mapping the *Use Case Model's* Sequence diagrams to *Class Model*. Use Case Model was set as the source while Class Model was set as the target. Objects in the sequence diagrams were mapped to classes in the Class Model. This is because sequence diagram objects represent classes. Therefore, the use case object “Client Application: Login” is realized by the class “ClientApplicationLogin” and the use case “Federated Database” is realized by class “FederatedDatabase”, and so on, as shown in Figure 4.36 below.

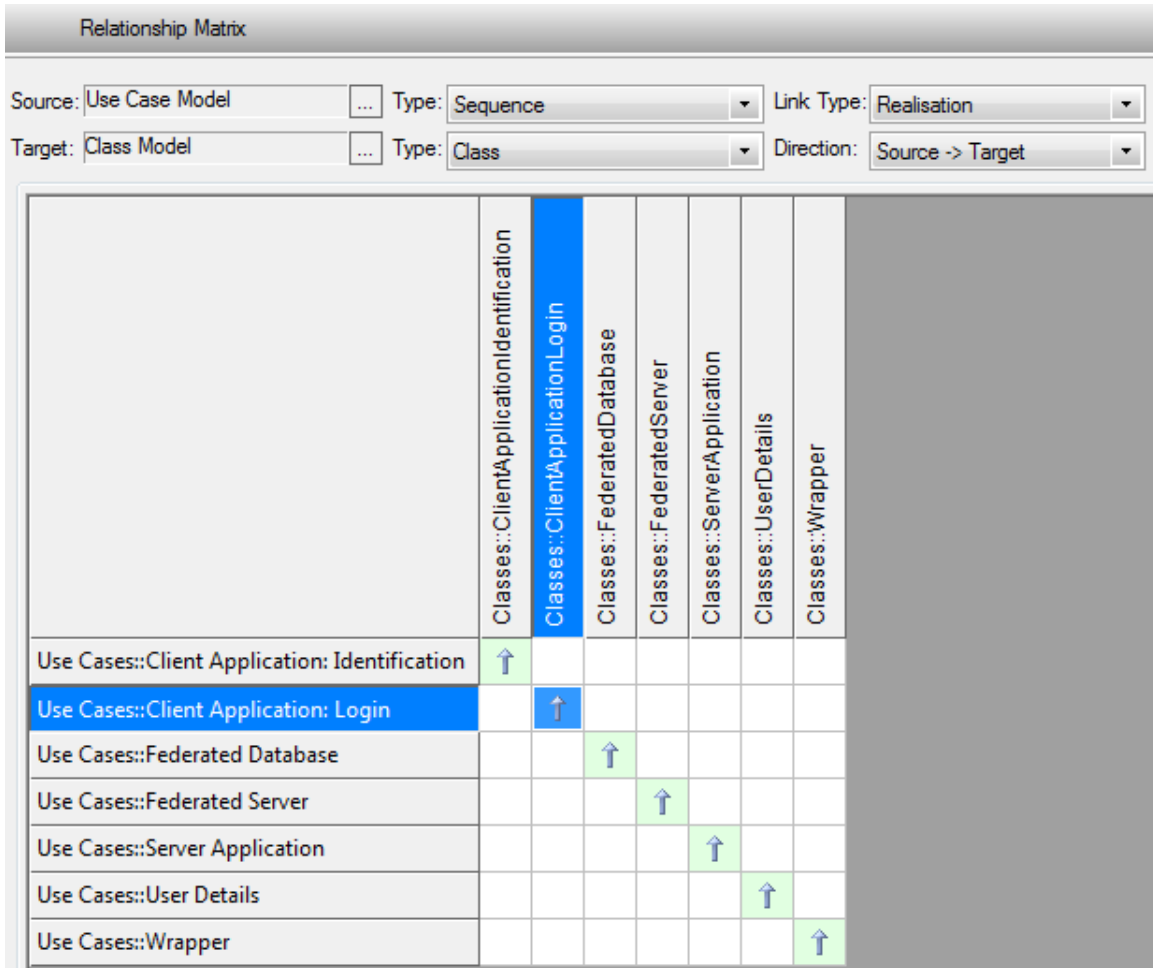


Figure 4. 36: Use Case to Class Realisation

iii). Class to Component Realisation

The third and final verification step of the functional requirements involved mapping the *Class Model* to *Component Model*. A Component Model has a higher level of abstraction than a Class Model. In most cases, a component is implemented by one or more Classes at runtime. Components are the building blocks, built up so that eventually a component can encompass a large portion of a system. In Figure 4.37, the two classes “ClientApplicationIdentification and ClientApplicationLogin” is realised by the component “ClientApplication”. The classes “FederatedServer, FederatedDatabase and Wrapper” is realized by the component “FederationManager”, and so on.

Relationship Matrix

Source: Class Model ... Type: Class Link Type: Realisation

Target: Components Model ... Type: Component Direction: Source -> Target

	Components Model::Client Application	Components Model::Federation Manager	Components Model::Server Application	Components Model::User Database
Classes::ClientApplicationIdentification	↑			
Classes::ClientApplicationLogin	↑			
Classes::FederatedDatabase		↑		
Classes::FederatedServer		↑		
Classes::ServerApplication			↑	
Classes::UserDetails				↑
Classes::Wrapper		↑		

Figure 4. 37: Class to Component Realisation

4.5.2 Verification of Non-Functional Requirements

Non-functional requirements were included at the stage of developing the component model. These requirements were performance, security, ubiquity and usability. Their verification involved identifying the specific components and technologies that would realize them.

i). Performance

The performance requirement specified that the system shall respond to all user requests in less than one second. One way of realizing this requirement may be through optimizing user queries. Literature on database performance suggests that query optimizers contribute a lot in improving the performance of a database system. ISPIS component model incorporates an

optimizer which determines the best way to execute queries. This component considers the various possible strategies and then chooses the one with the least cost in terms of system resources consumed. The other way is the fact that the system was designed in a multi-tiered architecture which allows the bulk of data processing work to be done at the identity federation side leaving the client side with virtually no work.

ii). Security

The security requirement aims to protect the confidentiality, integrity and availability of ISPIS from harm. This is addressed by the security architecture described in the Security View sub-section.

iii). Ubiquity

Ubiquity defines the ability to use the system anywhere at any time. Mobile devices, i.e. smart phone were proposed as one of the end-user devices. These devices are portable and thus can be carried by a user wherever he/she wants to go.

iv). Usability

Both token-based and biometric identifications are performed with limited manual intervention (No data entry required). Thus the system is easy to use and free of typing-errors.

Verification of functional requirements allowed the tracing of requirements from the Requirements Model to the Deployment Model. This was done using a module within Enterprise Architect software. However, verification of non-functional requirements was based on logic. This may have compromised the expected outcome since logic is prone to subjectivity.

4.6 Model Validation

Data for validating the system was entered into the three databases. Table 4.22 shows the data that was entered into the Birth Registration database.

Table 4. 22: Birth Details Data

PI	Full Names	DOB	Sex	Father's Name	Mother's Name	Informant Name	District of Birth	Registration Officers	Date of Registration
100102	Jane Juma	05/23/1967	Female	Mike Roger Juma	Susan Juma	Fred Wanyonyi	Mombasa	David Baridi	05/31/1967
100103	Daniel K. Kipkorir	05/07/1981	Male	Willy Korir	Rebby Korir	Ronald Choge	Uasin Gishu	Alice Mutai	05/08/1981
100104	Nancy Getao Thomas	02/01/1966	Female	Clinton Thomas	Faith Getao	Kamau Karanja	Nakuru	Abraham Esokon	02/28/1966
100101	Lily Zain Kimla	08/12/1979	Female	Jack Kimla	Jude Kimla	Caroline Wambui	Kericho	Muigai Kamau	06/02/1980
100100	John Njoroge Kamau	04/09/1981	Male	Anthony Maina Kamau	Elizabeth Wambui Kamau	Simon Kinyajui	Kiambu	Catherine Atieno	05/06/1981

Table 4.23 shows the data that was entered into the death registration database.

Table 4. 23: Death Details Data

Death No.	Full names	Date of Death	Gender	Death Place	Father's Name	Mother's Name	PI
1002765	Lil Zain Kimla	2013-02-13	Female	Kisumu	Jack Kimla	Jude Kimla	100101
2837378	Daniel K. Kipkorir	2014-01-02	Male	Mombasa	Willy Korir	Rebby Korir	100103

Table 4.24 shows the data that was entered into the national registration and identification database.

Table 4. 24: National ID Data

IDNo	Full Names	DOB	Sex	District of Birth	Date of Issue	Photo	FingerPrint	Signature	PI
13564232	Daniel K. Kipkorir	9/9/1999	Male	Uasin Gishu	9/9/1999				100103
18225363	Nancy Getao Thomas	2/1/1966	Female	Nakuru	8/5/1985				100104
22111121	Lily Zain Kimla	8/12/1979	Female	Kericho	2/12/1998				100101
23000119	John Njoroge Kamau	4/9/1981	Male	Kiambu	3/5/2000				100100
24536636	Jane Juma	5/23/1967	Female	Mombasa	1/5/1990				100102

A set of identity fraud scenarios were developed from the results of the identity fraud survey to validate the model as described below.

4.6.1 Identity Theft

Scenario 1: Use of stolen/lost personal documents to apply for a loan

Let us assume that the fraudster went to open a bank account in Kenya Commercial Bank. After presenting the required documents, the bank employee searches the national identity card number (UPI) from ISPIS system. The search result is displayed in Figure 4.38 below.

Current User :	Date :	Institution Name :	InstitutionType :
Kcb	2014-3-8 14:39:49	Kenya Commercial Bank	Bank

Enter Personal Identifier:



National Identity Card Details	
Identity Card Number :	23000119
Full Names :	John Njoroge Kamau
 	

Figure 4. 38: Identity Search by a Bank Employee

This information would allow the bank employee to clearly compare the photo and signature of the fraudster with that in the system.

Scenario 2: Use of look-alike passport to travel or Use of stolen/lost breeder documents to apply for a passport

In this case, the immigration officer verifies the identity of the traveller with other identification databases (birth and national ID). The passport UPI is searched as shown in Figure 4.39.

Current User :	Date :	Institution Name :	InstitutionType :
Immigration	2014-5-16 10:26:59	Doi	Immigration

Enter Personal Identifier: Search

Birth Certificate Details	
Birth Certificate Number :	100100
Full Names :	John Njoroge Kamau
Date Of Birth :	09-Apr-1981
Gender :	Male
Name Of Father :	Anthony Maina Kamau
Name Of Mother :	Elizabeth Wambui Kamau
Name Of Informant :	Simon Kinyajui
District Of Birth :	Kiambu
Registration Officer :	Catherine Atieno
Date Of Registration :	06-May-1981
National Identity Card Details	
Identity Card Number :	23000119
Full Names :	John Njoroge Kamau
Date Of Birth :	09-Apr-1981








Figure 4. 39: Identity Search by an Immigration Officer

This allows the immigration officer to confirm the identity of the traveller or the person applying for a passport from the retrieved information.

Scenario 3: Impersonating and NHIF member

In this scenario, a patient visits a hospital seeking for medical services. The hospital employee at the reception requests his/her NHIF card and national identity card. The identity

card number (UPI) is first searched from ISPIS database. If the card is valid, the details shown in Figure 4.40 below will be displayed.

Current User :	Date :	Institution Name :	Institution Type :
Knh	2014-5-16 11:56:35	Knh	Hospital

Enter Personal Identifier:

Birth Certificate Details	
Birth Certificate Number :	100100
Full Names :	John Njoroge Kamau
Date Of Birth :	09-Apr-1981
Gender :	Male
National Identity Card Details	
Identity Card Number :	23000119
Full Names :	John Njoroge Kamau
Date Of Birth :	09-Apr-1981
Gender :	Male
Date Of Issue :	05-Mar-2000




Figure 4. 40: Identity Search by a Hospital Employee

This search enables the hospital employee to verify the identity of the patient before allowing him or her to access medical services.

4.6.2 Identity Fabrication

Scenario: Registration of M-PESA accounts using forged identity documents

The fraudster pretending to be a KWS officer is used to demonstrate how the system will prevent the fraud. The fraudster is assumed to have faked a military card and used it to register for MPESA service.

Current User :	Date :	Institution Name :	InstitutionType :
Safaricom	2014-3-9 11:2:20	Safaricom	Mobile Service Operator

Personal Identifier: 1001005 Was Not Found!

Enter Personal Identifier:

Figure 4. 41: Identity Search by a National Registration Bureau Employee

The system would have informed the MPESA registration agent that the presented military card was fictitious (Figure 4.41).

4.6.3 Identity Manipulation

Scenario 1: Use of forged NHIF member's card

If it is assumed that the fraudster altered the photo of a genuine NHIF card, a search of the card's UPI would reveal the real owner of the card as shown in Figure 4.42.

Current User :	Date :	Institution Name :	InstitutionType :
Nhif	2014-5-16 11:30:1	Nhif	Health Insurance

Enter Personal Identifier:

Birth Certificate Details	
Birth Certificate Number :	100102
Full Names :	Jane Juma
Date Of Birth :	23-May-1967
Gender :	Female
National Identity Card Details	
Identity Card Number :	24536636
Full Names :	Jane Juma
Date Of Birth :	23-May-1967
Gender :	Female
Date Of Issue :	05-Jan-1990




Figure 4. 42: Identity Search by a Hospital Employee

The search results would have assisted the hospital employee in verifying the patient’s identity.

Scenario 2: Use of altered passport to travel

Just like in **Scenario 1** above, a search of the passport’s UPI would reveal the real owner of the passport as shown in Figure 4.43 below.

Current User :	Date :	Institution Name :	Institution Type :
Immigration	2014-5-16 11:15:45	Doi	Immigration

Enter Personal Identifier:

Birth Certificate Details	
Birth Certificate Number :	100103
Full Names :	Daniel K. Kipkorir
Date Of Birth :	07-May-1981
Gender :	Male
Name Of Father :	Willy Korir
Name Of Mother :	Rebby Korir
Name Of Informant :	Ronald Choge
District Of Birth :	Uasin Gishu
Registration Officer :	Alice Mutai
Date Of Registration :	08-May-1981
National Identity Card Details	
Identity Card Number :	13564232
Full Names :	Daniel K. Kipkorir
Date Of Birth :	07-May-1981




Figure 4. 43: Identity Search by an Immigration Officer

4.6.4 Data Manipulation

Scenario: Backdating of NHIF member's registration date

The security architecture proposed for ISPIS is able to combat data manipulation in the database. This feature was not incorporated in the prototype.

4.6.5 Phishing

Scenario: Use of skimmed ATM cards to carry out illegitimate cash withdrawals

ISPIS was not designed to incorporate the use of Automatic Teller machines. It may therefore not prevent card skimming. However, other solutions such as the use of EMV (chip-based) ATM cards may prevent skimming.

4.6.6 Social Engineering

Scenario: Using fake M-PESA messages to defraud agents/customers

ISPIS may not be applicable in curbing this kind of fraud directly. However, if one falls into this trap, the ISPIS system would assist in tracing the perpetrator. Because registration of MPESA service requires a prior registration with ISPIS. Therefore the fraudster's identity details would be available in the ISPIS system.

Validation was performed through a model prototype. The prototype incorporated only the key functionalities that were expected of the model. For example, the biometric and NFC components were not included in the prototype. Their functionality was only described in theory. However, these components have been tested with other systems that are similar to ISPIS and have proven to work. The survey revealed that existing government registration and identification databases did not have data of the entire population. It also showed that the databases contained duplicate and invalid records. The effectiveness of ISPIS would be affected greatly if the system operates with such problem laden data. In addition, phishing (card skimming) and social engineering were not explicitly curbed by the proposed model. However, other solutions for these types of fraud have been proposed elsewhere. For example, banks are now turning to EMV (chip-based) ATM cards since they are difficult to skim. Social engineering is being addressed through education and legal frameworks.

CHAPTER 5

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the study findings (5.2) and also provides the conclusions (5.3) and recommendations (5.4).

5.2 Summary of Findings

This study was intended to develop a model for a personal identification system that is resilient, secure and capable of curbing identity fraud. This initiative was in reaction to a growing trend in identity fraud perpetration and lack of reliable tools for combating the crime. The study specifically sought to identify the methods used to perpetrate identity fraud, determine the challenges that make Kenya's personal identification system vulnerable to identity fraud, and thirdly develop a model of a personal identification system that addresses these challenges and (4) verify and validate the model.

A survey was undertaken to establish the methods used by criminals to perpetrate identity fraud and the challenges facing Kenya's primary registration and identification systems. The identity fraud survey was undertaken at the Banking Fraud Investigations Department, Department of Immigration, Safaricom Limited and the National Hospital Insurance Fund. The study established that *identity theft*, *identity fabrication*, *identity manipulation*, *data manipulation*, *phishing* and *social engineering* were the main methods used in Kenya. The survey on Kenya's Registration and Identification Systems on the other hand was carried out at the Civil Registration Department and the National Registration Bureau. The results showed that the main contributors to inability to combat identity fraud were: four fold namely the existence of incomplete and unclean data, the use of paper documents, lack of interoperability among the systems and inadequate system security architecture.

The findings of the study assisted in developing, constructing and validating the ISPIS model. The model has the ability to detect and prevent incidences of identity fraud. It is accessible through ubiquitous devices such as smartphones and can therefore be used in a wide range of scenarios where identity checks are routinely done. Additionally, it is easy to use and

free of typing-errors since users have limited manual intervention (e.g. there is no data entry required when searching for an identity). Its security architecture has advantages as it ensures confidentiality, integrity, availability and privacy of identity data.

There were however a number of challenges experienced during the development and construction of ISPIS. First, the model's security requirements were complex considering the many potential kinds of attacks that could be mounted. Further, it was designed to operate on multiple networks such as the internet, where such attacks are more pronounced. Secondly, the performance/response time which is a critical parameter for its adoption had complex requirements.

5.3 Conclusion

This study developed a model for an integrated and secure personal identification system. The model was meant to guide in designing national identification systems that are capable of curbing identity fraud. This was in reaction to a growing trend in the perpetration of identity fraud and lack of reliable tools for curbing the crime. The outcome of the surveys together with a review of literature on similar systems assisted in developing the model. This was done from the perspective of the service provider, the identity provider and the security architect. The modelling of the service provider view commenced with capturing the user requirements into a Requirements Model. This model was then translated into a Use Case Model to define the exact system functionality. The details of the Use Case Model were converted into sequence diagrams so as to describe the processes in the system and the interface a user would use to execute the Use Case. This led to the creation of a class model to specify the objects in the system, as well as their data and operations. A Data Model was then constructed to describe the data to be stored and retrieved from the system. This was followed by the construction of a component model to define the logical packaging of classes. A Deployment Model was finally developed to define the physical architecture of the system.

The identity provider view represented the processes that take place at the back-end of ISPIS. The model provided for two types of Identity Providers, i.e. Primary and Secondary. The Primary IdP was defined as the principal identity registration entity responsible for authenticating secondary identity registrations. The modelling process involved the construction of workflow diagrams and a description of technologies that would be incorporated.

The security view presented an architecture which comprised a series of (1) platforms and infrastructure that apply and enforce security controls, (2) an enterprise security framework that manages security, and (3) a set of security interfaces that enable communication between security components. The architecture provided for secure computing platforms and inter-communications throughout the processing chain enabling each node in the chain to inject security controls in order to protect data in use, in transit, and at rest. This would ensure that data is protected from end-to-end, starting from the end user devices through all processing nodes, networks and databases, all the way to offline backup media.

The prototype of the model was constructed on an ASP.NET platform. The front-end was built with Microsoft Visual Studio 2010 Ultimate software suite. The back-end databases (identity provider databases) were created on MS SQL Server 2008R2, Oracle Express Edition 11g and MySQL version 5.6. The application was finally published on Internet Information Services (IIS) version 7.5.

The model was verified with the assistance of a requirements traceability matrix. This was meant to test whether or not the proposed system satisfies the requirements of its intended users. It was then validated through the constructed system prototype in order to check the degree to which the model accurately represented the real world from the perspective of its usage. The prototype was subjected to a set of identity fraud scenarios that had been developed from the survey.

The test results revealed that identity fraud would be reduced significantly if countries such as Kenya implement ISPIS.

5.4 Recommendations

It is generally recommended that countries that experience incidences of identity fraud such as Kenya should consider implementing ISPIS as an alternative tool for curbing the crime. However, the following areas may need to be looked at:

- i). *Registration of all residents in the country:* The government can undertake a national digitization drive to capture digital and biometric identities of citizens of all ages using technology-based registration equipment. This would ensure that ISPIS is able to identify any resident in the country in real-time.

- ii). *Legal and policy Issues:* Kenya should review its legal and policy frameworks to ensure that they support the implementation of personal identification systems.
- iii). *ICT infrastructure:* ISPIS is meant to identify a person anywhere anytime. Therefore data network and any other supporting infrastructure should be put in place so as to allow global identification.
- iv). *Identity fraud awareness:* This may reduce socially engineered frauds.
- v). *Improve accessibility to registration offices:* Many people living in remote parts of a country seldom get to identity registration offices. Proper access to infrastructure should be put in place.

5.5 Suggestions for Further Research

Findings from the study revealed a number of areas that call for further investigations. The following areas are therefore suggested for further research:

- i). *Development of a framework for testing vulnerabilities and measuring the strength of identity registration systems:* This is needed so as to address the weaknesses found in the identity registration process.
- ii). *Development of a global personal identification system:* Integrating identification systems at a national level may not provide a complete solution to identity fraud. While one country can implement a very secure identification system, the integrity of that system is affected by the integrity of other external systems.
- iii). *Expanding integration of persons' databases to include land, assets and establishment:* This is required to enable the provision of a complete source of truth about an individual.
- iv). *Establishing the potential of NFC-technology in personal identification:* NFC technology was proposed for automatic reading of identifiers from identity card to the client application. This technology was however not tested with the prototype.
- v). *Development of a universal data source wrapper:* The data source wrapper within the federation manager is an important component for linking identity providers' databases. The current design utilized the native data source connectors. Configuring these connectors for

many different data sources may be cumbersome. Research on the development of a universal data source wrapper should be considered.

- vi). *Solutions for mobile identity fraud:* Mobile technology was found to be a key facilitator to identity fraud. Researchers should come up with potential technologies to address this problem.
- vii). *Identity fraud research from legal perspective:* ISPIS connects to autonomous identity databases. There may be need to carry out research on the legal implications of connecting identity databases at national and international levels.

REFERENCES

- Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Cognitive Computation*, 2(3), 242-253.
- Acoca, B. (2009). Online Identity Theft Retrieved 8 September, 2012, from www.oecd.org/publishing/corrigenda
- Al-Khoury, A. M., & Bal, J. (2007). Digital Identities and the Promise of the Technology Trio: PKI, Smart Cards, and Biometrics. *Journal of Computer Science*, 5(3), 361-367.
- Aly, G., & Roth, K. H. (2004). The Nazi Census – Identification and Control in the Third Reich
- Baechler, S., Fivaz, E., Ribaux, O., & Margot, P. (2011). False identity documents profiling: A promising forensic intelligence method to fight identity document fraud. *Le profilage forensique des fausses pièces d'identité: Une méthode de renseignement prometteuse pour lutter contre la fraude documentaire*, 64(4), 467-480.
- Bang, Y., Lee, D.-J., Bae, Y.-S., & Ahn, J.-H. (2012). Improving information security management: An analysis of ID–password usage and a new login vulnerability measure. *International Journal of Information Management*, 32(5), 409-418.
- Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud detection in telecommunications: History and lessons learned. *Technometrics*, 52(1), 20-33.
- Borcea-Pfutzmann, K., Hansen, M., Liesebach, K., Pfutzmann, A., & Steinbrecher, S. (2006). What user-controlled identity management should learn from communities. *Information Security Technical Report*, 11(3), 119-128.

- Brisis, K. d., Mansfield, N., & Rundle, M. (2009). The Role of Digital Identity Management in the Internet Economy. *A Primer for Policy Makers* Retrieved 11 November, 2013, from <http://www.oecd.org/internet/ieconomy/43091476.pdf>
- Carson, J. S. (1986). Convincing Users of Model's Validity Is Challenging Aspect of Modeler's Job. *Industrial Engineering*, 18(6), 74-85.
- Castro, D. (2011). Explaining International IT Application Leadership: Electronic Identification Systems *The Information Technology & Innovation Foundation*.
- Chappelle, D. (2013). Security in Depth Reference Architecture. Retrieved from <http://www.oracle.com/technetwork/topics/entarch/oracle-wp-security-ref-arch-1918345.pdf>
- Chollet, G., Perrot, P., Karam, W., Mokbel, C., Kanade, S., & Petrovska-Delacrétaz, D. (2012). Identities, forgeries and disguises. *International Journal of Information Technology and Management*, 11(1-2), 138-152.
- Clarke, R. (1994). Human Identification in Information Systems: Management Challenges and Public Policy Issues. *Information Technology & People*, 7(4), 6-37.
- Cofta, P. (2008). Towards a better citizen identification system. *Identity in the Information Society*, 1(1), 39-53.
- Das, R. (2006). An introduction to biometrics. *Keesing Journal of Documents & Identity* Retrieved 10 July, 2013, from http://biometricnews.net/test/Articles/Biometrics_Article_Introduction_To_Biometrics.pdf
- Davis, P. K. (1992). Generalizing Concepts and Methods of Verification, Validation, and Accreditation (VV&A) for Military Simulations *RAND Report*.

- De Hert, P. (2008). Identity management of e-ID, privacy and security in Europe. A human rights view. *Information Security Technical Report*, 13(2), 71-75.
- Deswarte, Y., & Gamba, S. (2010). A proposal for a privacy-preserving national identity card. *Transactions on Data Privacy*, 3(3), 253-276.
- Dettmer, R. (2004). Safety in numbers [biometric identification cards and database]. *IEE Review*, 50(11), 26-29.
- Dong, X., Clark, J. A., & Jacob, J. L. (2010). Defending the weakest link: Phishing websites detection by analysing user behaviours. *Telecommunication Systems*, 45(2-3), 215-226.
- Douglas, B. A. D., Leonardo; Christopher, K. Tucker. (2011). "Napoleonic Know-How" in an Age of Persistent Engagement. *Small World Journal*.
- Eisen, O. (2009). In-session phishing and knowing your enemy. *Network Security*, 2009(3), 8-11.
- Encinas-Franco, J. (2005). National Identification System: Do we Need One? *Policy Insights* Retrieved July 09 2012, from <http://www.senate.gov.ph/publications/PI%202005-12%20-%20National%20Identification%20System%20-%20Do%20We%20Need%20One.pdf>
- Florence, J., Hassan, A., Carole, A., Ezra, C., James, M., Akademia, N., . . . Moses, K. (2007). An Identity Crisis? A Study on the Issuance of National Identity Cards In Kenya. Nairobi: Kenya National Commission on Human Rights.
- Furnell, S. M. (2010). Online identity: Giving it all away? *Information Security Technical Report*, 15(2), 42-46.
- Giannasi, F., Lovett, P., & Godwin, A. N. (2001). Enhancing confidence in discrete event simulations. *Computers in Industry*, 4(2), 141-154.
- Gitonga, A. (2013). Imposter PPO was a tout. *Standard Digital* Retrieved January 4, 2013, from <http://www.standardmedia.co.ke/?articleID=2000074171>

- Gordon, G. R., & Willox, N. A. (2003). Identity Fraud: A Critical National and Global Threat. *White Paper* Retrieved October 28, 2013, from http://www.utica.edu/academic/institutes/ecii/publications/media/identity_fraud.pdf
- Greenleaf, G. (2010). India's national ID system: Danger grows in a privacy vacuum. *Computer Law and Security Review*, 26(5), 479-491.
- Grijpink, J. (2004). Identity fraud as a challenge to the constitutional state. *Computer Law & Security Review*, 20(1), 29-36.
- Grijpink, J. (2005). Biometrics and identity fraud protection: Two barriers to realizing the benefits of biometrics – A chain perspective on biometrics, and identity fraud – Part II. *Computer Law & Security Review*, 21(3), 249-256.
- Heichlinger, A., & Gallego, P. (2010). A new e-ID card and online authentication in Spain. *Identity in the Information Society*, 3(1), 43-64.
- Heimbigner, D. (1985). A federated Architecture for Information management. *ACM Transactions on Office Information Systems*, 3(3), 253-278.
- Hernandez-Ardieta, J. L., Gonzalez-Tablas, A. I., de Fuentes, J. M., & Ramos, B. (2013). A taxonomy and survey of attacks on digital signatures. *Computers & Security*, 34(0), 67-112.
- Hopkins, L. (2005). Identity synthesis: Creating an identity from scratch Retrieved 24 January 2013, from <http://hinari-gw.who.int/whalecomwww.scopus.com/whalecom0/inward/record.url?eid=2-s2.0-84864546809&partnerID=40&md5=5dc3c9544f2862cc71e62760102adbac>
- Hsu, M.-H., Yeh, Y.-T., Chen, C.-Y., Liu, C.-H., & Liu, C.-T. (2011). Online detection of potential duplicate medications and changes of physician behavior for outpatients visiting multiple hospitals using national health insurance smart cards in Taiwan. *International Journal of Medical Informatics*, 80(3), 181-189.

- Hussain, A. (2002). *General principles and commercial law in Kenya* Nairobi EAEP: East African Educational Publishers.
- Jain, A. K., Hong, L., & Pankanti, S. (2000). Biometric Identification. *Communications of ACM*, 43(2), pp. 91-98.
- Jain, A. K. J. F. N., K. (2010). Fingerprint Matching. *Computer Communications*, 43(2), 36-44.
- Jamieson, R., Wee Land, L. P., Winchester, D., Stephens, G., Steel, A., Maurushat, A., & Sarre, R. (2012). Addressing identity crime in crime management information systems: Definitions, classification, and empirics. *Computer Law and Security Review*, 28(4), 381-395.
- Jones, A. (2005). How much information do organizations throw away? *Computer Fraud & Security*, 2005(3), 4-9.
- Kardas, G., & Tunali, E. T. (2006). Design and implementation of a smart card based healthcare information system. *Computer Methods and Programs in Biomedicine*, 81(1), 66-78.
- Kemp, G. (2010). Fighting public sector fraud in the 21st century. *Computer Fraud and Security*, 2010(11), 16-18.
- Koops, B. J., Leenes, R., Meints, M., Van Der Meulen, N., & Jaquet-Chiffelle, D. O. (2009). A typology of identity-related crime. *Information Communication and Society*, 12(1), 1-24.
- Kosta, E., Zibuschka, J., Scherner, T., & Dumortier, J. (2008). Legal considerations on privacy-enhancing Location Based Services using PRIME technology. *Computer Law & Security Review*, 24(2), 139-146.
- Li, J., Wang, G. A., & Chen, H. (2011). Identity matching using personal and social identity features. *Information Systems Frontiers*, 13(1), 101-113.
- Lincoln, A. (2004). Electronic Signature Laws and the Need for Uniformity in the Global Market. *The Journal of Small and Emerging Business Law*, 8, 67-71.

- Loo, W. H., Yeow, P. H. P., & Chong, S. C. (2009). User acceptance of Malaysian government multipurpose smartcard applications. *Government Information Quarterly*, 26(2), 358-367.
- Mannan, M., & Van Oorschot, P. C. (2009). Localization of credential information to address increasingly inevitable data breaches Retrieved 24 January, 2013, from <http://hinari-gw.who.int/whalecomwww.scopus.com/whalecom0/inward/record.url?eid=2-s2.0-77950574163&partnerID=40&md5=ec0108bba541c81043a1c35e49c68178>
- McCarty, B. (2003). Automated identity theft. *Security & Privacy, IEEE*, 1(5), 89-92.
- Mills, G. (2007). *Identity Theft*. 46 West St, Chichester, West Sussex County PO19 1RP, United Kingdom: Summersdale Publishers Ltd.
- Ministry of Information and Registration of Persons, K. (2013a). Civil Registration Department Retrieved 20 December, 2013, from <http://www.crd.go.ke/>
- Ministry of Information and Registration of Persons, K. (2013b). Historical Background Retrieved 22 December, 2013, from <http://www.crd.go.ke/index.php/about-crd/historical-background>
- Mumo, M. (2012, July 31, 2012). East African banks lose US\$48.3 million to fraud, *Daily Nation*.
- Munene, F. M. (1994). The Current Status of Vital Statistics and Civil Registration Systems in Kenya Retrieved 27 April, 2014, from http://unstats.un.org/unsd/demographic/meetings/wshops/1994_Ethiopia_CRVS/docs/Doc.10_Kenya.pdf
- Noore, A. (2000). Highly Robust Biometric Smart Card Design. *IEEE Transactions on Consumer Electronics*, 46(4).
- Olabode, O. (2011). Smart card identification management over a distributed database model. *Journal of Computer Science*, 7(12), 1770-1777.

- Oxford University Press. (2014). Oxford Dictionaries *Language Matters*, from <http://www.oxforddictionaries.com/>
- Pan, J. A., Winchester, D., Land, L., & Watters, P. (2010). Descriptive data mining on fraudulent online dating profiles Retrieved 24 January 2013, from <http://hinari-gw.who.int/whalecomwww.scopus.com/whalecom0/inward/record.url?eid=2-s2.0-84870636418&partnerID=40&md5=eca08c081053faf0a6ae169ac7c74a7f>
- Peyravi, N. J., S. (2010). *Optimization and integration of electronic identity authentication using a biometric indicator and RFID*. Paper presented at the Cybernetics and Intelligent Systems (CIS), 2010 IEEE Conference on. <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5518565>
- Rebovich, D. J. (2009). Examining identity theft: Empirical explorations of the offense and the offender. *Victims and Offenders*, 4(4), 357-364.
- Record, M. (2008). *Protecting Your Identity A Practical Guide to Preventing Identity Theft and Its Damaging Consequences* Retrieved from www.howtobooks.co.uk
- Rissanen, T. (2010). Electronic identity in Finland: ID cards vs. bank IDs. *Identity in the Information Society*, 3(1), 175-194.
- Robinson, S. (1997, December 07 - 10). *Simulation Model Verification and Validation: Increasing the Users' Confidence*. Paper presented at the Winter Simulation Conference, Atlanta, GA, USA
- Rössler, T. (2008). Giving an interoperable e-ID solution: Using foreign e-IDs in Austrian e-Government. *Computer Law & Security Review*, 24(5), 447-453.
- Sargent, R. G. (2007). *Verification and Validation of Simulation Models*. Paper presented at the Proceedings of the 2007 Winter Simulation Conference.


- Sauveron, D. (2009). Multiapplication smart card: Towards an open smart card? *Information Security Technical Report*, 14(2), 70-78.
- Shaw, V. N. (1996). Social Control in China: A Study of Chinese Work Units
- Smedinghoff, T. J. (2012). Solving the legal challenges of trustworthy online identity. *Computer Law & Security Review*, 28(5), 532-541.
- Sproule, S., & Archer, N. (2006). Defining Identity Theft – A Discussion Paper: McMaster University.
- Sproule, S., & Archer, N. (2010). Measuring identity theft and identity fraud. *International Journal of Business Governance and Ethics*, 5(1-2), 51-63.
- Such, J. M., Espinosa, A., Garcia-Fornes, A., & Botti, V. (2011). Partial identities as a foundation for trust and reputation. *Engineering Applications of Artificial Intelligence*, 24(7), 1128-1136.
- Sullivan, C. (2009). Digital identity – The legal person? *Computer Law & Security Review*, 25(3), 227-236.
- Warren, A., & Mavroudi, E. (2011). Surveillance and identity management: Migrant perspectives on UK Biometric Residence Permits. *Computer Law & Security Review*, 27(3), 245-249.
- Wayman, J. L. (2008). Biometrics in identity management systems. *IEEE Security and Privacy*, 6(2), 30-37.
- Wilcox, N. A., & Regan, T. M. (2002). Identity Fraud: Providing a Solution. *Journal of Economic Crime Management*, 1(1). Retrieved from http://www.popcenter.org/problems/identity_theft/PDFs/wilcox.pdf
- Yeow, P. H. P., Yuen, Y. Y., & Loo, W. H. (2012). Ergonomics issues in national identity card for homeland security. *Applied Ergonomics*(0).

Ying, X., Wu, X., & Barbará, D. (2010). *Spectrum based fraud detection in social networks*.

Zezeza, T. (1992). *The Colonial Labour System in Kenya*: East African Educational Publishers.

APPENDIX A:

LETTER OF INTRODUCTION


Kabarak University
INSTITUTE OF POST GRADUATE STUDIES & RESEARCH

Private Bag - 20157
KABARAK, KENYA
E-mail: directorpostgraduate@kabarak.ac.ke

Tel: 0203511275
Fax: 254-51-343012
www.kabarak.ac.ke

6th May, 2013

TO WHOM IT MAY CONCERN

Dear Sir/ Madam,


RE: JOEL KIMELI CHERUS - GDI/M/1113/09/11


The above named is a Doctoral Student at Kabarak University in the School of Science, Engineering and Technology undertaking PhD in Information Technology. He is carrying out research entitled "*A Model of an Integrated and Secure Personal Identification System.*" The supervisors: Prof. Jason Githeko and Dr. Joseph Siror.

He has successfully defended his proposal and is collecting data.

Kindly provide the necessary assistance. Thank you for your continued support.

Yours faithfully,





Dr. Kageni Njagi
DIRECTOR - (POST-GRADUATE STUDIES & RESEARCH)

Kabarak University Moral Code
As members of Kabarak University family, we purpose at all times and in all places, to set apart in our heart, Jesus as Lord. (1 Peter 3:15)

APPENDIX B:

LETTER OF RESEARCH AUTHORIZATION



NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone: +254-20-2213471,
2241349, 310571, 2219420
Fax: +254-20-318245, 318249
Email: secretary@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

9th Floor, Utalii House
Uhuru Highway
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No.

Date:

27th November, 2013

NACOSTI/P/13/0382/278

Joel Kimeli Cherus
Kabarak University
Private Bag-20157
KABARAK.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on "*A model of an integrated and secure personal identification system,*" I am pleased to inform you that you have been authorized to undertake research in **Nairobi County** for a period ending **31st December, 2013.**

You are advised to report to **the County Commissioner and the County Director of Education, Nairobi County** before embarking on the research project.

On completion of the research, you are expected to submit **two hard copies and one soft copy in pdf** of the research report/thesis to our office.


SAID HUSSEIN
FOR: SECRETARY/CEO
NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Copy to:

The County Commissioner
The County Director of Education
Nairobi County.

APPENDIX C:

QUESTIONNAIRE FOR IDENTITY FRAUD SURVEY

This questionnaire seeks to collect information about the methods used by criminals to perpetrate identity fraud. The findings are expected to assist in developing the right model. Kindly provide the information frankly and honestly. All information received will be treated in confidence and used for academic purposes only.

SECTION A: BACKGROUND INFORMATION

1. Name of your Institution.....
2. What is the institution’s core business?
.....
3. What services does your institution offer to the public?
 - (i)
 - (ii)
 - (iii).....
 - (iv).....
4. Which of these services requires prove of identity in order to access?
 - (i)
 - (ii)
5. What does your institution use for identification (Choose all that apply)?
 - a. PIN/User Name/Password
 - b. Biometric
 - c. Identity Card/Document
 - d. Other.....

SECTION B: IDENTITY FRAUD

Identity fraud is where a client/customer uses someone else’s identity or a fictitious one to illegally access services

6. Have there been incidences of identity fraud in your institution?

Yes [] No [] If yes, List some of them.

- (i)
- (ii)
- (iii).....

7. In each case, describe how the fraud was carried out and how it was discovered. Check the frequency of occurrence.

4.12
.....
.....
.....

Very Frequently Frequently Occasionally Rarely Very Rarely Never

4.13
.....
.....

Very Frequently Frequently Occasionally Rarely Very Rarely Never

4.14
.....
.....

Very Frequently Frequently Occasionally Rarely Very Rarely Never

8. In your own opinion, what do you think should be done to prevent such incidences of identity fraud from happening in future?

.....
.....
.....
.....

Thank you for taking your time to answer this questionnaire.

APPENDIX D:

INTERVIEW SCHEDULE FOR ID SYSTEM SURVEY

PART I: BACKGROUND OF THE SYSTEM

1. What is the system's name?
2. When was it implemented?
3. Why was it implemented?
4. Were there other previous versions of the system? Yes No If "Yes", which ones?

PART II: SYSTEM FUNCTIONALITY

A. Registration

5. What are the requirements needed for one to register into the identification system?
6. How is the registration done?
7. Who does the registration?
8. Where is the registration?
9. When is the registration?
10. How often is the registration?
11. What is the current registered population?

B. Data Transmission

12. Is there any transmission of registration data to some other site? If yes, proceed to ask questions 11 and 12.
13. How is it transmitted?
14. How long does it take the data to reach its final destination?

C. Data Processing

15. What is involved during processing of registration data?

16. Who does the processing?
17. Where is it done?
18. What is the product of the processed data?
19. Who are the consumers of this product?
20. How do the consumers get the product?

D. Data Storage

21. What stores the processed and the unprocessed data?
22. Where is the storage area located?
23. Who does the storage of the data?
24. Is there a secondary storage facility? If yes, how frequently is data backed up?

E. Verification and Validation

25. Can the system identify incorrect registration data? If yes, explain how?

PART III: TECHNOLOGY

26. What are the components of the identification system?
27. What kind of technology is used for data registration, transmission and storage?
28. Is the system networked? If yes, under what topology?
29. What Operating System(s) is/are in use?
30. What application software is/are running?
31. How are electronic documents managed?

PART IV: SYSTEM ARCHITECTURE

32. How are the components of the system connected?
33. Does the system interact with other external systems? If so, how?

34. How does data flow within the system?

PART V: SYSTEM SECURITY

35. What kind of security has been implemented on:-

- a. Equipment.
- b. Gateway.
- c. Platform.
- d. Database.

36. Who is in charge of system security in your department?

APPENDIX E:

SAMPLE SOURCE CODE FOR THE PROTOTYPE

```
'Check if Unique Personal Identifier exists in virtual/federated database
'-----
    Dim TmpData As New Data.DataTable
    '
    TmpData = MyDbQuery.ExecuteRecords(1, "SELECT Idxno, upi FROM UPI WHERE upi = " &
    Val(txtUIP.Text) & "", "", Nothing)
    If Object.ReferenceEquals(TmpData, Nothing) Then
        lblErrorMsg.Text = "Personal Identifier: " & txtUIP.Text & " Was Not Found!"
        Exit Sub
    End If
    If TmpData.Rows.Count <= 0 Then
        lblErrorMsg.Text = "Personal Identifier: " & txtUIP.Text & " Was Not Found!"
        Exit Sub
    End If

'Load all data into the grids
'-----
    Dim BirthData As New Data.DataTable
    Dim NationalData As New Data.DataTable
    Dim DeceasedData As New Data.DataTable
    '
    'Module Codes For The Data
    '05 View ID Details
    '06 View Birth Details
    '07 View Deceased Details

    BirthData = LoadBirthDetails(Session("CurrentUserRoleCode"), "06", Val(txtUIP.Text.Trim))
    NationalData = LoadNationalIDDetails(Session("CurrentUserRoleCode"), "05", Val(txtUIP.Text.Trim))
    DeceasedData = LoadDeceasedDetails(Session("CurrentUserRoleCode"), "07", Val(txtUIP.Text.Trim))

'Load personal details into main grid
'-----
    Dim i, j As Integer
    Dim y As New Data.DataTable
    y.Clear()
    y.Columns.Add("item")
    y.Columns.Add("itemvalue")
    '
    If Not Object.ReferenceEquals(BirthData, Nothing) Then
        If BirthData.Rows.Count > 0 Then
            y.Rows.Add()
            y.Rows(y.Rows.Count - 1).Item("item") = "    Birth Certificate Details"
            y.Rows(y.Rows.Count - 1).Item("itemvalue") = ""
            '
            j = BirthData.Rows.Count
            For i = 0 To j - 1
                y.Rows.Add()
                If Not IsDBNull(BirthData.Rows(i).Item("item")) Then
                    y.Rows(y.Rows.Count - 1).Item("item") =
                    BirthData.Rows(i).Item("item").ToString.Trim
                End If
                If Not IsDBNull(BirthData.Rows(i).Item("itemvalue")) Then
                    y.Rows(y.Rows.Count - 1).Item("itemvalue") =
                    BirthData.Rows(i).Item("itemvalue").ToString.Trim
                End If
            Next i
        End If
    End If
```

```

        y.Rows.Add()
        y.Rows(y.Rows.Count - 1).Item("item") = ""
        y.Rows(y.Rows.Count - 1).Item("itemvalue") = ""
    End If 'If BirthData.Rows.Count > 0 Then
End If 'If Not Object.ReferenceEquals(BirthData, Nothing) Then
If Not Object.ReferenceEquals(NationalData, Nothing) Then
    If NationalData.Rows.Count > 0 Then
        y.Rows.Add()
        y.Rows(y.Rows.Count - 1).Item("item") = "    National Identity Card Details"
        y.Rows(y.Rows.Count - 1).Item("itemvalue") = ""

        j = NationalData.Rows.Count
        For i = 0 To j - 1
            y.Rows.Add()
            If Not IsDBNull(NationalData.Rows(i).Item("item")) Then
                y.Rows(y.Rows.Count - 1).Item("item") =
                    NationalData.Rows(i).Item("item").ToString.Trim
            End If
            If Not IsDBNull(NationalData.Rows(i).Item("itemvalue")) Then
                y.Rows(y.Rows.Count - 1).Item("itemvalue") =
                    NationalData.Rows(i).Item("itemvalue").ToString.Trim
            End If
        Next i

        y.Rows.Add()
        y.Rows(y.Rows.Count - 1).Item("item") = ""
        y.Rows(y.Rows.Count - 1).Item("itemvalue") = ""

        End If 'If NationalData.Rows.Count > 0 Then
End If 'If Not Object.ReferenceEquals(NationalData, Nothing) Then
If Not Object.ReferenceEquals(DeceasedData, Nothing) Then
    If DeceasedData.Rows.Count > 0 Then
        y.Rows.Add()
        y.Rows(y.Rows.Count - 1).Item("item") = "    Death Certificate Details"
        y.Rows(y.Rows.Count - 1).Item("itemvalue") = ""

        j = DeceasedData.Rows.Count
        For i = 0 To j - 1
            y.Rows.Add()
            If Not IsDBNull(DeceasedData.Rows(i).Item("item")) Then
                y.Rows(y.Rows.Count - 1).Item("item") =
                    DeceasedData.Rows(i).Item("item").ToString.Trim
            End If
            If Not IsDBNull(DeceasedData.Rows(i).Item("itemvalue")) Then
                y.Rows(y.Rows.Count - 1).Item("itemvalue") =
                    DeceasedData.Rows(i).Item("itemvalue").ToString.Trim
            End If
        Next i

        y.Rows.Add()
        y.Rows(y.Rows.Count - 1).Item("item") = ""
        y.Rows(y.Rows.Count - 1).Item("itemvalue") = ""

        End If 'If DeceasedData.Rows.Count > 0 Then
End If 'If Not Object.ReferenceEquals(DeceasedData, Nothing) Then

If Not Object.ReferenceEquals(y, Nothing) Then
    If y.Rows.Count > 0 Then

```



```

        dtgrdmodules.DataSource = y
        dtgrdmodules.DataBind()
        dtgrdmodules.Visible = True
    End If
End If

End Sub 'END: Load personal details into main grid

```

'Function to retrieve death details

```

Private Function LoadDeceasedDetails(ByVal CurrentUserRoleCode As String, ByVal ModuleCode As String,
    ByVal IDNo As String) As Data.DataTable
    LoadDeceasedDetails = Nothing

    Dim i, j, m, n, z As Integer
    Dim CmdObj As Data.SqlClient.SqlCommand
    Dim ViewFields As String = ""
    Dim ViewDescrType As String = ""
    Dim ViewDescr As String = ""
    Dim ViewData As String = ""
    Dim SqlSearch As String = ""
    Dim ColData As New Data.DataTable
    Dim TempDate As DateTime
    Dim DeceasedLoaded As Boolean = False
    '
    '
    Dim x As New Data.DataTable
    x.Clear()
    x.Columns.Add("item")
    x.Columns.Add("itemvalue")
    '
    lblErrorMsg.Text = ""
    Try
        'get column descriptions
        CmdObj = New Data.SqlClient.SqlCommand
        CmdObj = APII.DbProcess(0, "RightsViews", "ColumnName,ColumnDesc,Type", "", "ViewDesc =
            'DeceasedDetails'", "")
        If Not Object.ReferenceEquals(CmdObj, Nothing) Then
            If Not Object.ReferenceEquals(ColData, Nothing) Then
                ColData.Clear()
                ColData.Rows.Clear()
                ColData.Columns.Clear()
            End If
            ColData = MyDbQuery.ExecuteRecords(7, "", "", CmdObj)
        End If

        CmdObj = New Data.SqlClient.SqlCommand
        CmdObj = APII.DbProcess(0, "Rights", "ViewFields", "", "ModuleCode='" & ModuleCode & "' And
            RoleCode='" & CurrentUserRoleCode & "'", "")
        If Not Object.ReferenceEquals(CmdObj, Nothing) Then
            If Not Object.ReferenceEquals(DaTable, Nothing) Then
                DaTable.Clear()
                DaTable.Rows.Clear()
                DaTable.Columns.Clear()
            End If
            DaTable = MyDbQuery.ExecuteRecords(7, "", "", CmdObj)
            j = DaTable.Rows.Count
            If j > 0 And ColData.Rows.Count > 0 Then
                ViewFields = DaTable.Rows(0).Item(0).ToString.Trim
                '
                If ViewFields.Trim.Length > 1 Then
                    If ViewFields.Trim.Contains("\") Then
                        '*****begin split
                        Dim MyItmArray() As String
                        MyItmArray = ViewFields.Split("\")
                    End If
                End If
            End If
        End If
    Catch
    End Try
End Function

```

```

For z = 0 To MyItmArray.Count - 1
ViewFields = ""
If Not Object.ReferenceEquals(MyItmArray(z), Nothing) Then
ViewFields = MyItmArray(z).ToString.Trim
End If
If ViewFields.Trim.Length > 1 Then
'
'*****Process each db column
ViewDescr = ""
ViewDescrType = ""
ViewData = ""
n = ColData.Rows.Count
For m = 0 To n - 1
If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
IsDBNull(ColData.Rows(m).Item(1)) Then
If ColData.Rows(m).Item(0).ToString.Trim.ToLower =
ViewFields.Trim.ToLower Then
ViewDescr = ColData.Rows(m).Item(1).ToString.Trim
ViewDescrType = IIf(IsDBNull(ColData.Rows(m).Item(2)), "",
ColData.Rows(m).Item(2).ToString.Trim)
Exit For
End If
End If 'If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
IsDBNull(ColData.Rows(m).Item(1)) Then
Next m
SqlSearch = "Select " & ViewFields & " From deceased.decdetails Where
Enumber=" & Val(IDNo) & ""
If Not Object.ReferenceEquals(DaTable, Nothing) Then
DaTable.Clear()
DaTable.Rows.Clear()
DaTable.Columns.Clear()
End If
DaTable = MyDbQuerry.ExecuteRecordsDeceased(1, SqlSearch, "", Nothing)
j = DaTable.Rows.Count
If j > 0 Then
For i = 0 To j - 1
ViewData = IIf(IsDBNull(DaTable.Rows(i).Item(0)), "",
DaTable.Rows(i).Item(0))
'
Next i

End If 'If j > 0 Then
'
If ViewDescr.Trim.Length > 1 And ViewData.Trim.Length > 0 Then
If ViewDescrType.Trim.ToLower = "image" Then
'no images are in the db for death details at the moment
ElseIf ViewDescrType.Trim.ToLower = "date" Then
If Date.TryParse(ViewData, TempDate) Then
ViewData = TempDate.ToString("dd-MMM-yyyy")
x.Rows.Add()
x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
Else
x.Rows.Add()
x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
End If 'If Date.TryParse(ViewData, TempDate) Then
Else
x.Rows.Add()
x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
End If 'If ViewDescrType.Trim.ToLower = "image" Then
'
End If 'If ViewDescr.Trim.Length > 1 Then
'
'*****End Of Process each db column
'

```

```

        End If 'If ViewFields.Trim.Length > 1 Then
    ,
Next z
,
'*****end split
Else 'If ViewFields.Trim.Contains("\") Then
'its only a single Row
'get the column dedcription
,
ViewDescr = ""
ViewDescrType = ""
ViewData = ""
n = ColData.Rows.Count
For m = 0 To n - 1
    If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
        IsDBNull(ColData.Rows(m).Item(1)) Then
        If ColData.Rows(m).Item(0).ToString.Trim.ToLower =
            ViewFields.Trim.ToLower Then
            ViewDescr = ColData.Rows(m).Item(1).ToString.Trim
            ViewDescrType = IIf(IsDBNull(ColData.Rows(m).Item(2)), "",
                ColData.Rows(m).Item(2).ToString.Trim)
            Exit For
        End If
    End If 'If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
        IsDBNull(ColData.Rows(m).Item(1)) Then
    ,
Next m
,
SqlSearch = "Select " & ViewFields & " From deceased.decdetails Where
    Number=" & Val(IDNo) & ""
If Not Object.ReferenceEquals(DaTable, Nothing) Then
    DaTable.Clear()
    DaTable.Rows.Clear()
    DaTable.Columns.Clear()
End If
DaTable = MyDbQuery.ExecuteRecordsDeceased(1, SqlSearch, "", Nothing)
j = DaTable.Rows.Count
If j > 0 Then
    For i = 0 To j - 1
        ViewData = IIf(IsDBNull(DaTable.Rows(i).Item(0)), "",
            DaTable.Rows(i).Item(0))
    Next i
End If 'If j > 0 Then
,
If ViewDescr.Trim.Length > 1 And ViewData.Trim.Length > 0 Then
    If ViewDescrType.Trim.ToLower = "image" Then
        'no images are in the db for death details at the moment
        ,
    ElseIf ViewDescrType.Trim.ToLower = "date" Then
        If Date.TryParse(ViewData, TempDate) Then
            ViewData = TempDate.ToString("dd-MMM-yyyy")
            x.Rows.Add()
            x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
            x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
        Else
            x.Rows.Add()
            x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
            x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
        End If 'If Date.TryParse(ViewData, TempDate) Then
    Else
        x.Rows.Add()
        x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
        x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
    End If 'If ViewDescrType.Trim.ToLower = "image" Then
    ,
End If 'If ViewDescr.Trim.Length > 1 Then

```

```

        End If 'If ViewFields.Trim.Contains("\") Then
    End If 'If ViewFields.Trim.Length > 1 Then
    End If 'If j > 0 Then
    End If 'If Not Object.ReferenceEquals(CmdObj, Nothing) Then
    CmdObj = Nothing
    LoadDeceasedDetails = x
Catch ex As Exception
    lblErrorMsg.Text = "***Errors Occurred While Fetching Details!"
End Try

End Function 'End: Function to retrieve death details

```

'Function to retrieve birth details

```

-----
Private Function LoadBirthDetails(ByVal CurrentUserRoleCode As String, ByVal ModuleCode As String,
    ByVal IDNo As String) As Data.DataTable
    LoadBirthDetails = Nothing
    Dim i, j, m, n, z As Integer
    Dim CmdObj As Data.SqlClient.SqlCommand
    Dim ViewFields As String = ""
    Dim ViewDescrType As String = ""
    Dim ViewDescr As String = ""
    Dim ViewData As String = ""
    Dim SqlSearch As String = ""
    Dim ColData As New Data.DataTable
    Dim TempData As DateTime
    Dim x As New Data.DataTable
    x.Clear()
    x.Columns.Add("item")
    x.Columns.Add("itemvalue")
    lblErrorMsg.Text = ""
    Try
        'get column descriptions
        CmdObj = New Data.SqlClient.SqlCommand
        CmdObj = APII.DbProcess(0, "RightsViews", "ColumnName,ColumnDesc,Type", "", "ViewDesc =
            'BirthDetails'", "")
        If Not Object.ReferenceEquals(CmdObj, Nothing) Then
            If Not Object.ReferenceEquals(ColData, Nothing) Then
                ColData.Clear()
                ColData.Rows.Clear()
                ColData.Columns.Clear()
            End If
            ColData = MyDbQuery.ExecuteRecords(7, "", "", CmdObj)
        End If

        CmdObj = New Data.SqlClient.SqlCommand
        CmdObj = APII.DbProcess(0, "Rights", "ViewFields", "", "ModuleCode='" & ModuleCode & "' And
            RoleCode='" & CurrentUserRoleCode & "'", "")
        If Not Object.ReferenceEquals(CmdObj, Nothing) Then
            If Not Object.ReferenceEquals(DaTable, Nothing) Then
                DaTable.Clear()
                DaTable.Rows.Clear()
                DaTable.Columns.Clear()
            End If
            DaTable = MyDbQuery.ExecuteRecords(7, "", "", CmdObj)
            j = DaTable.Rows.Count
            If j > 0 And ColData.Rows.Count > 0 Then

```

```

ViewFields = DaTable.Rows(0).Item(0).ToString.Trim
,
If ViewFields.Trim.Length > 1 Then
    If ViewFields.Trim.Contains("\") Then
        '*****begin split
        Dim MyItmArray() As String
        MyItmArray = ViewFields.Split("\")
        For z = 0 To MyItmArray.Count - 1
            ViewFields = ""
            If Not Object.ReferenceEquals(MyItmArray(z), Nothing) Then
                ViewFields = MyItmArray(z).ToString.Trim
            End If
            If ViewFields.Trim.Length > 1 Then
                ,
                '*****Process each db column
                ViewDescr = ""
                ViewDescrType = ""
                ViewData = ""
                n = ColData.Rows.Count
                For m = 0 To n - 1
                    If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
                        IsDBNull(ColData.Rows(m).Item(1)) Then
                        If ColData.Rows(m).Item(0).ToString.Trim.ToLower =
                            ViewFields.Trim.ToLower Then
                            ViewDescr = ColData.Rows(m).Item(1).ToString.Trim
                            ViewDescrType = IIf(IsDBNull(ColData.Rows(m).Item(2)), "",
                                ColData.Rows(m).Item(2).ToString.Trim)
                            Exit For
                        End If
                    End If 'If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
                        IsDBNull(ColData.Rows(m).Item(1)) Then
                ,
                Next m
                ,
                ,
                SqlSearch = "Select " & ViewFields & " From BIRTH.BirthDetails Where
                    ENUMBER=" & Val(IDNo) & ""
                If Not Object.ReferenceEquals(DaTable, Nothing) Then
                    DaTable.Clear()
                    DaTable.Rows.Clear()
                    DaTable.Columns.Clear()
                End If
                DaTable = MyDbQuery.ExecuteRecordsBirth(1, SqlSearch, "", Nothing)
                j = DaTable.Rows.Count
                If j > 0 Then
                    For i = 0 To j - 1
                        ViewData = IIf(IsDBNull(DaTable.Rows(i).Item(0)), "",
                            DaTable.Rows(i).Item(0))
                    Next i
                End If 'If j > 0 Then
                ,
                If ViewDescr.Trim.Length > 1 And ViewData.Trim.Length > 0 Then
                    If ViewDescrType.Trim.ToLower = "image" Then
                        'no images are in the db for birth details at the moment
                    ElseIf ViewDescrType.Trim.ToLower = "date" Then
                        If Date.TryParse(ViewData, TempDate) Then
                            ViewData = TempDate.ToString("dd-MMM-yyyy")
                            x.Rows.Add()
                            x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
                            x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
                        Else
                            x.Rows.Add()
                            x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
                            x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
                        End If 'If Date.TryParse(ViewData, TempDate) Then
                    Else

```

```

        x.Rows.Add()
        x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
        x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
    End If 'If ViewDescrType.Trim.ToLower = "image" Then
    ,
    End If 'If ViewDescr.Trim.Length > 1 Then
    ,
    '*****End Of Process each db column
    ,
    End If 'If ViewFields.Trim.Length > 1 Then
    ,
Next z
,
'*****end split
Else 'If ViewFields.Trim.Contains("\") Then
'its only a single Row
'get the column dedcription
,
ViewDescr = ""
ViewDescrType = ""
ViewData = ""
n = ColData.Rows.Count
For m = 0 To n - 1
    If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
        IsDBNull(ColData.Rows(m).Item(1)) Then
        If ColData.Rows(m).Item(0).ToString.Trim.ToLower =
            ViewFields.Trim.ToLower Then
            ViewDescr = ColData.Rows(m).Item(1).ToString.Trim
            ViewDescrType = IIf(IsDBNull(ColData.Rows(m).Item(2)), "",
                ColData.Rows(m).Item(2).ToString.Trim)
            Exit For
        End If
    End If 'If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
        IsDBNull(ColData.Rows(m).Item(1)) Then
    ,
Next m
,
SqlSearch = "Select " & ViewFields & " From BIRTH.BirthDetails Where ENUMBER="
    & Val(IDNo) & ""
If Not Object.ReferenceEquals(DaTable, Nothing) Then
    DaTable.Clear()
    DaTable.Rows.Clear()
    DaTable.Columns.Clear()
End If
DaTable = MyDbQuery.ExecuteRecordsBirth(1, SqlSearch, "", Nothing)
j = DaTable.Rows.Count
If j > 0 Then
    For i = 0 To j - 1
        ViewData = IIf(IsDBNull(DaTable.Rows(i).Item(0)), "",
            DaTable.Rows(i).Item(0))
    Next i

End If 'If j > 0 Then
,
If ViewDescr.Trim.Length > 1 And ViewData.Trim.Length > 0 Then
    If ViewDescrType.Trim.ToLower = "image" Then
        'no images are in the db for birth details at the moment
        ,
    ElseIf ViewDescrType.Trim.ToLower = "date" Then
        If Date.TryParse(ViewData, TempDate) Then
            ViewData = TempDate.ToString("dd-MMM-yyyy")
            x.Rows.Add()
            x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
            x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
        Else
            x.Rows.Add()
            x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "

```

```

        x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
    End If 'If Date.TryParse(ViewData, TempData) Then
Else
    x.Rows.Add()
    x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
    x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
End If 'If ViewDescrType.Trim.ToLower = "image" Then
'
    End If 'If ViewDescr.Trim.Length > 1 Then
'
    End If 'If ViewFields.Trim.Contains("\") Then
'
    End If 'If ViewFields.Trim.Length > 1 Then
End If 'If j > 0 Then
End If 'If Not Object.ReferenceEquals(CmdObj, Nothing) Then
CmdObj = Nothing
'
    LoadBirthDetails = x
'
Catch ex As Exception
    lblErrorMsg.Text = "***Errors Occurred While Fetching Details!"
End Try

End Function 'Function to retrieve birth details

'Function to retrieve national identity card details
'-----
Private Function LoadNationalIDDetails(ByVal CurrentUserRoleCode As String, ByVal ModuleCode As
String, ByVal IDNo As String) As Data.DataTable
    LoadNationalIDDetails = Nothing
'
    Dim i, j, m, n, z As Integer
    Dim CmdObj As Data.SqlClient.SqlCommand
    Dim ViewFields As String = ""
    Dim ViewDescrType As String = ""
    Dim ViewDescr As String = ""
    Dim ViewData As String = ""
    Dim SqlSearch As String = ""
    Dim ColData As New Data.DataTable
    Dim TempData As DateTime
    Dim Image1 As Byte()
    Dim Image1L, Image2L, Image3L As Boolean
'
'
    Dim x As New Data.DataTable
    x.Clear()
    x.Columns.Add("item")
    x.Columns.Add("itemvalue")
'
    Image1 = Nothing
    Image1L = False
    Image2L = False
    Image3L = False
'
    lblErrorMsg.Text = ""
    Try
        'get column descriptions
        CmdObj = New Data.SqlClient.SqlCommand
        CmdObj = APII.DbProcess(0, "RightsViews", "ColumnName,ColumnDesc,Type", "", "ViewDesc =
'National'", "")
        If Not Object.ReferenceEquals(CmdObj, Nothing) Then
            If Not Object.ReferenceEquals(ColData, Nothing) Then
                ColData.Clear()
                ColData.Rows.Clear()
                ColData.Columns.Clear()

```

```

    End If
    ColData = MyDbQuery.ExecuteRecords(7, "", "", CmdObj)
End If

CmdObj = New Data.SqlClient.SqlCommand
CmdObj = APII.DbProcess(0, "Rights", "ViewFields", "", "ModuleCode='" & ModuleCode & "' And
RoleCode='" & CurrentUserRoleCode & "'", "")
If Not Object.ReferenceEquals(CmdObj, Nothing) Then
    If Not Object.ReferenceEquals(DaTable, Nothing) Then
        DaTable.Clear()
        DaTable.Rows.Clear()
        DaTable.Columns.Clear()
    End If
    DaTable = MyDbQuery.ExecuteRecords(7, "", "", CmdObj)
    j = DaTable.Rows.Count
    If j > 0 And ColData.Rows.Count > 0 Then
        ViewFields = DaTable.Rows(0).Item(0).ToString.Trim
        '
        If ViewFields.Trim.Length > 1 Then
            If ViewFields.Trim.Contains("\") Then
                '*****begin split
                Dim MyItmArray() As String
                MyItmArray = ViewFields.Split("\")
                For z = 0 To MyItmArray.Count - 1
                    ViewFields = ""
                    If Not Object.ReferenceEquals(MyItmArray(z), Nothing) Then
                        ViewFields = MyItmArray(z).ToString.Trim
                    End If
                    If ViewFields.Trim.Length > 1 Then
                        '
                        '*****Process each db column
                        ViewDescr = ""
                        ViewDescrType = ""
                        ViewData = ""
                        n = ColData.Rows.Count
                        For m = 0 To n - 1
                            If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
                                IsDBNull(ColData.Rows(m).Item(1)) Then
                                If ColData.Rows(m).Item(0).ToString.Trim.ToLower =
                                    ViewFields.Trim.ToLower Then
                                    ViewDescr = ColData.Rows(m).Item(1).ToString.Trim
                                    ViewDescrType = IIf(IsDBNull(ColData.Rows(m).Item(2)), "",
                                        ColData.Rows(m).Item(2).ToString.Trim)
                                    Exit For
                                End If
                            End If
                            If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
                                IsDBNull(ColData.Rows(m).Item(1)) Then
                                '
                            End If
                        Next m
                        '
                        SqlSearch = "Select " & ViewFields & " From dbo.IDDetails Where
                            Enumer=" & Val(IDNo) & ";"
                        If Not Object.ReferenceEquals(DaTable, Nothing) Then
                            DaTable.Clear()
                            DaTable.Rows.Clear()
                            DaTable.Columns.Clear()
                        End If
                        DaTable = MyDbQuery.ExecuteRecordsNational(1, SqlSearch, "", Nothing)
                        j = DaTable.Rows.Count
                        If j > 0 Then
                            For i = 0 To j - 1
                                Image1 = Nothing
                                If ViewDescrType.Trim.ToLower = "image" Then
                                    Image1 = IIf(IsDBNull(DaTable.Rows(i).Item(0)), Nothing,
                                        DaTable.Rows(i).Item(0))
                                Else
                                    ViewData = IIf(IsDBNull(DaTable.Rows(i).Item(0)), "",

```



```

        DaTable.Rows(i).Item(0))
    End If
    Next i

End If 'If j > 0 Then
If ViewDescr.Trim.Length > 1 Then
    If ViewDescrType.Trim.ToLower = "image" Then
        'go on
        If Not Object.ReferenceEquals(Image1, Nothing) Then
            If Image1.Length > 0 Then
                If Image1L = False And Image2L = False And Image3L =
                    False Then
                    'lblPhoto0.Text = ViewDescr.Trim
                    If UploadFromDb(Image1, imgPhotograph0) = True
                        Then
                        Image1L = True
                        'lblPhoto0.Visible = True
                        imgPhotograph0.Visible = True
                    End If

                    ElseIf Image1L = True And Image2L = False And Image3L
                        = False Then
                    'lblPhoto1.Text = ViewDescr.Trim
                    If UploadFromDb(Image1, imgPhotograph1) = True
                        Then
                        Image2L = True
                        'lblPhoto1.Visible = True
                        imgPhotograph1.Visible = True
                    End If

                    ElseIf Image1L = True And Image2L = True And Image3L =
                        False Then
                    'lblPhoto2.Text = ViewDescr.Trim
                    If UploadFromDb(Image1, imgPhotograph2) = True
                        Then
                        Image3L = True
                        'lblPhoto2.Visible = True
                        imgPhotograph2.Visible = True
                    End If

                    End If
                End If 'If Image1.Length > 0 Then
            End If 'If Not Object.ReferenceEquals(Image1, Nothing) Then
        End If

        ElseIf ViewDescrType.Trim.ToLower = "date" And
            ViewData.Trim.Length > 0 Then
            If Date.TryParse(ViewData, TempData) Then
                ViewData = TempData.ToString("dd-MMM-yyyy")
                x.Rows.Add()
                x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
                x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
            Else
                x.Rows.Add()
                x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
                x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
            End If 'If Date.TryParse(ViewData, TempData) Then
        Else
            If ViewData.Trim.Length > 0 Then
                x.Rows.Add()
                x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
                x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
            End If
        End If 'If ViewDescrType.Trim.ToLower = "image" Then
    End If 'If ViewDescr.Trim.Length > 1 Then
End If

```

```

        ,
        '*****End Of Process each db column
        ,
        End If 'If ViewFields.Trim.Length > 1 Then
        ,
    Next z
    ,
    '*****end split
Else 'If ViewFields.Trim.Contains("\") Then
    'its only a single Row
    'get the column dedcription
    ,
    ViewDescr = ""
    ViewDescrType = ""
    ViewData = ""
    n = ColData.Rows.Count
    For m = 0 To n - 1
        If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
            IsDBNull(ColData.Rows(m).Item(1)) Then
            If ColData.Rows(m).Item(0).ToString.Trim.ToLower =
                ViewFields.Trim.ToLower Then
                ViewDescr = ColData.Rows(m).Item(1).ToString.Trim
                ViewDescrType = IIf(IsDBNull(ColData.Rows(m).Item(2)), "",
                    ColData.Rows(m).Item(2).ToString.Trim)
                Exit For
            End If
        End If 'If Not IsDBNull(ColData.Rows(m).Item(0)) And Not
            IsDBNull(ColData.Rows(m).Item(1)) Then
        ,
    Next m
    ,
    SqlSearch = "Select " & ViewFields & " From dbo.IDDetails Where Enumber=" &
        Val(IDNo) & ";"
    If Not Object.ReferenceEquals(DaTable, Nothing) Then
        DaTable.Clear()
        DaTable.Rows.Clear()
        DaTable.Columns.Clear()
    End If
    DaTable = MyDbQuery.ExecuteRecordsNational(1, SqlSearch, "", Nothing)
    j = DaTable.Rows.Count
    If j > 0 Then
        For i = 0 To j - 1
            Image1 = Nothing
            If ViewDescrType.Trim.ToLower = "image" Then
                Image1 = IIf(IsDBNull(DaTable.Rows(i).Item(0)), Nothing,
                    DaTable.Rows(i).Item(0))
            Else
                ViewData = IIf(IsDBNull(DaTable.Rows(i).Item(0)), "",
                    DaTable.Rows(i).Item(0))
            End If
        Next i
    End If 'If j > 0 Then
    ,
    If ViewDescr.Trim.Length > 1 Then
        If ViewDescrType.Trim.ToLower = "image" Then
            'lblPhoto0.Text = ViewDescr.Trim
            If UploadFromDb(Image1, imgPhotograph0) = True Then
                'go on
                'lblPhoto0.Visible = True
                imgPhotograph0.Visible = True
            End If
        ,
        ElseIf ViewDescrType.Trim.ToLower = "date" And ViewData.Trim.Length > 0
            Then
                If Date.TryParse(ViewData, TempDate) Then
                    ViewData = TempDate.ToString("dd-MMM-yyyy")
                End If
            End If
        End If
    End If
    ,

```

```

        x.Rows.Add()
        x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
        x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
    Else
        x.Rows.Add()
        x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
        x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
    End If 'If Date.TryParse(ViewData, TempData) Then
Else
    If ViewData.Trim.Length > 0 Then
        x.Rows.Add()
        x.Rows(x.Rows.Count - 1).Item("item") = ViewDescr.Trim & " : "
        x.Rows(x.Rows.Count - 1).Item("itemvalue") = ViewData.Trim
    End If
    End If 'If ViewDescrType.Trim.ToLower = "image" Then
    End If 'If ViewDescr.Trim.Length > 1 Then
    End If 'If ViewFields.Trim.Contains("\") Then
    End If 'If ViewFields.Trim.Length > 1 Then
    End If 'If j > 0 Then
    End If 'If Not Object.ReferenceEquals(CmdObj, Nothing) Then
    CmdObj = Nothing
    LoadNationalIDDetails = x
Catch ex As Exception
    lblErrorMsg.Text = "***Errors Occurred While Fetching Details!"
End Try

End Function 'Function to retrieve national identity card details

```