University of Fort Hare

Together in Excellence

INVESTIGATION OF THE NFC TECHNOLOGY FOR MOBILE PAYMENTS AND THE DEVELOPMENT OF A PROTOTYPE PAYMENT APPLICATION IN THE CONTEXT OF MARGINALIZED RURAL AREAS

A Dissertation Submitted In Fulfillment Of The
Requirements for the Degree
Of

MASTER OF SCIENCE
IN
COMPUTER SCIENCE

By

Caroline Gurajena

Supervisor

Prof Mamello Thinyane

July 2014

ABSTRACT

Both communication, and the methods and tools of commerce have evolved over time through the invention of new technologies. The latest of these technologies are mobile devices and electronic commerce respectively. The combination of these two technologies has resulted in the creation of electronic commerce which also enables mobile payments. Mobile payments (m-payments) are enabled by many technologies with Near Field Communication (NFC) being the most recent one. NFC is a wireless technology that enables mobile devices in close proximity to exchange data. The mobile device has already been enthusiastically accepted by the customers and they carry it with them wherever they go and this makes it a good device for providing a payment method alternative. This research looks at contactless mobile payment as a payment method. Customers in marginalized rural areas lack a payment alternative to cash hence in this research we are investigating and proposing the use of a NFC enabled mobile payment application for Marginalized Rural Areas. This research extensively evaluates and assesses the potential of using NFC enabled m-payments in Marginalized Rural Areas in South Africa by carrying out an investigation of the technology and its acceptance by customers. The investigation of the technology included implementation of a prototype application which was used to introduce the technology to the consumers. The customer acceptance of the NFC enabled mobile payments was evaluated using the Technology Acceptance model (TAM). The model was modified to suit the context of this study by adding more constructs. This research concluded that Near Field Communication enabled m-payments have great potential to be used and accepted by people in the marginalized rural areas.

DECLARATION

I, Caroline Gurajena, student number 200902544, do hereby declare that the work titled "INVESTIGATION OF THE NFC TECHNOLOGY FOR MOBILE PAYMENTS AND THE DEVELOPMENT OF A PROTOTYPE PAYMENT APPLICATION IN THE CONTEXT OF MARGINALIZED RURAL AREAS" is my own work and that, to the best of my knowledge, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any degree or diploma of the University or any other institution of higher learning except where due acknowledgement has been made in the text.

I hereby also declare that I am fully aware of the University of Fort Hare's policy on plagiarism and research ethics, and I have taken every necessary measure to comply with the regulations. I have obtained an ethical clearance certificate from the University of Fort Hare's Research Ethics Committee and the reference number is the following: THI021SGURO1

Signature.. ……………………………..

Caroline Gurajena Date

ACKNOWLEDGEMENTS

Above all I would like to thank God Almighty, if it was not for him I would not be here.

My deepest gratitude goes to my supervisor Prof Mamello Thinyane, I have learned a lot from you and you made it possible for me to finish this research. Thank you so much for your patience.

I am truly indebted and thankful to my parents Mr and Mrs N. A. Hahn, my sister Constance and my uncle Clemio Mushonga.

The financial assistance of the National Research Foundation (NRF) (UID: 90421) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the author and are not necessarily to be attributed to the NRF.

A special thank you goes to my friends Eddie, Daphy, Vongy, Wendy, Kudzie, Doiline, Munya, Vusi, Courage and Pride. You guys are the best; I always thank God for you.

This work is based on the research undertaken within the Telkom CoE in ICTD supported in part by Telkom SA, Tellabs, Saab Grintek Technologies, Easttel, Khula Holdings, THRIP and National Research Foundation of South Africa (UID : 84006). The opinions, findings and conclusions or recommendations expressed here are those of the authors and none of the above sponsors accepts no liability whatsoever in this regard.

DEDICATION

To the memory of my beloved, respected and greatly missed Grandmother Monica Nyashanu and uncle Collins Mushonga, thank you for your unconditional love and for believing in me.

Table of Contents

List of Tables

List of Figures

Table of Listings

ACRONYMS

NFC	Near Field Communication
RFID	Radio Frequency Identification
MRA	Marginalized Rural Area
SWOT	Strength, Weaknesses, Opportunities and Threats
TAM	Technology Acceptance Model
POS	Point of Sale
SMS	Short Message Services
SE	Secure Element
SEM	Structure Equation Modelling
PLS	Partial Least Squares
USSD	Unstructured Supplementary Service Data
GPRS	General Packet Radio Service
3G	Third Generation
UICC	Universal Integrated Circuit Card
SCH	Secure Channel Service
MNO	Mobile Network Operator
RF	Radio Frequency
PIN	Personal Identification Number
AES	Advanced Encryption Standard
SSE	Shared Service Secret
GSM	Global System for Mobile Communication
TSM	Trusted Service Manager
RTD	Record Type Definition
TNF	Type Name Definition
LLCP	Logical Link Control Protocol
SNEP	Simple NDEF Exchange Format
NDEF	NFC Data Exchange Format

1 INTRODUCTION

1.1 Introduction

Near Field Communication (NFC) is a wireless short range radio technology that enables communication between devices that either touch or are in close proximity of about 3 cm (ISO/IEC 18092, 2013). NFC was introduced in 2002 (ISO/IEC 18092, 2013). This technology evolved from existing contactless identification and interconnection technology called Radio Frequency Identification (RFID) (Aziza, 2010). This makes NFC to be compatible with RFID technology. The technology can be embedded in many different electronic devices including: smartphones, tablets and point of sale terminals. The NFC technology brings many advantages to mobile devices such as:

- no initial configuration requirement
- fast connection setup
- reliable communication
- improved user experience
- convenience (Raina, Pandey, & Makkad, 2011)
- security of contactless technology (Raina et al., 2011)
- bidirectional communication
- accessibility by third party applications installed on the mobile device
- short communication distance to reduce security threats such as man in the middle attacks and eavesdropping

This technology is becoming more prominent and this is seen through the number of NFC enabled applications that are being developed and the increase in the number of NFC enabled devices that are being released into the market each year since its introduction. Many NFC applications have been proposed and some of these have been developed. The domains of deployment of these applications typically include mobile payments (m-payments), access control, data transfer between NFC units, access to digital information and ticketing.

The most important emerging area for NFC technology that is offering potential growth is NFC-supported m-payments. M-payments have been around for some time now but their adoption have been limited (Dahlberg, Mallat, Ondrus, & Zmijewska, 2008a). The concept of m-payments enabled by the NFC technology is relatively new in Africa but not in other continents such as Asia and Europe. According to Dahlberg et al (2008), m-payments "are payments for goods, services, and bills with a mobile device (such as a mobile phone, smart-phone, or personal digital assistants) by taking advantage of wireless technologies and other communication technologies". Raina et al (2011) defined an m-payment as "the transfer of money from one party to another through the exchange of information". An NFC m-payment application is also known as contactless mobile payment application. In this research, the terms NFC enabled m-payment application and contactless payment application will be used interchangeably. The term contactless payment was first used to refer to payments carried out using credit cards which used the RFID technology. These cards are commonly known as contactless cards.

NFC m-payment applications have been deployed successfully in many Asian countries for a few years now (Ondrus & Pigneur, 2007; Smart Card Alliance, 2007). Japan started using NFC enabled m-payments in 2005 and these payment applications have been very successful (National Retail Federation, 2011). As NFC enabled m-payments are continuing to gain popularity; we are anticipating that soon this technology could and might become the mainstream payment method in Africa, with tangible benefits for the marginalized African communities. In the research done by Muriira and Kibua (2012), they noted that half of the Kenyan population would greatly benefit from the NFC technology if implemented by banks and the telecom companies – in this research we are anticipating that similar benefits and impact would be realized in the context of South Africa.

In contactless mobile payment transactions, the NFC technology does not make the actual payment but it is responsible for transferring the details that are required in carrying out a payment transaction. Since NFC technology is compatible with RFID, it enables credit cards or debit cards to be emulated and stored in a virtual wallet on the mobile device. These virtual cards will then be used to make m-payments. This is one way of carrying out NFC enabled m-payments. The other ways include using a virtual account that is created by the stakeholder offering the m-payment service and then use that virtual account for making payment transactions or by using an already existing bank account. In order to carry out an m-payment, the customer must have mobile money available in his/ her account. Mobile money is a form of electronic money. The next section covers mobile money and electronic money in detail.

1.2 Electronic Money and Mobile Money

M-payments can only be carried out using electronic money (e-money). E-money is defined in the National Payment System position paper published 2009 as monetary value that is stored electronically and represented by a claim on the issuer (South African Reserve Bank, 2009). E-money can either be issued out when the funds are received, accepted as payment of goods or services, redeemed as cash or deposited into a bank account. E-money leads us to the factor of mobile money (m-money). M-money is a form of e-money that enables both the banked and unbanked (i.e. people who do not have access to banking facilities) to deposit money into their mobile accounts and this is known as mobile banking. According to Jenkins (2008), m-money is monetary value that can be accessed and utilized via a mobile device (Jenkins, 2008).

Mobile banking is defined as "the use of a mobile device by a consumer to access and manage financial services provided by a bank, credit union, brokerage, or other financial services provider" (Smart Card Alliance, 2011). Mobile banking for the unbanked and underbanked (i.e. people who have limited access to banking services) has recently been on the increase in South Africa. The past few years have seen the introduction of mobile money transfer in Africa. This service insures the availability and accessibility of banking services both to the banked people (i.e. in terms of augmenting and supplementing the existing banking services) and also the unbanked (i.e. in terms of providing a new channel to banking services). M-money transfer is being offered by mobile network operators and banks. Examples of m-money transfer services in South Africa include cardless services for FNB and Standard Bank, M-PESA being offered by Vodacom in South Africa (Mas & Morawczynski, 2010) and MTN Mobile Money**.** M-money transfer service emerged from electronic payment and the banking industry.

M-money enables easy and cheap money transfer (mobile money transfers) among the mobile subscribers. M-money can also be used in m-payments or be converted back into cash by withdrawing from the appropriate agents, branches or ATMs. Mobile money transfer is usually used for sending remittances. The purpose of m-money is typically to bring financial services to the unbanked and also to supplement the banking service offering to the already banked individuals. Mobile money transfer can be classified as either m-payment or mobile banking. Mobile money transfer is based on person to person remittance service.

This research focuses on m-payments enabled by NFC technology. M-money provides one form of monetary value used to carry out m-payment transactions. The other form of the monetary value used in m-payment includes: existing bank accounts through mobile banking, payments cards, prepaid value stored in the mobile device or can be added on the mobile bill. In this research we are proposing an m-payment system that is coupled with a mobile money transfer service or mobile banking. It should be noted that there is a difference between mobile banking service and mobile banking. Mobile banking services are the services that are based on the existing bank's system of financial institution but mobile banking is a new method of banking created mainly to cater for the unbanked and the underbanked, by typically having the mobile operators providing a full-fledged banking service entirely focused around the use of cell phones (an example of this in the South African context is the MTN Mobile Money service).

1.3 Research Context

This research is framed under the domain of Information technology for Development (ICT4D) which seeks to improve the lives of people living in rural areas through technology. The majority of people staying in Marginalized Rural Areas (MRA) are either unbanked or underbanked. In 2013, a survey carried out by FinScope South Africa revealed that about 25 per cent of the South African adult population (16+) are unbanked most of whom are in rural areas (Ventures, 2013). Being unbanked includes the inadequacy of people to meet the bank's criteria to open a bank account (Afful, 2013) or their inability to have access to banking facilities. Since these people lack banking facilities, they also lack payment alternatives and have to always resort to cash which is difficult for them because they have to travel long distances in order to reach banks. This situation is made worse by the fact that most of their purchases are micro-payments in "spaza" shops (tuck-shops) where they also need to use cash only currently. Therefore there is a need to provide them with a safe, convenient and secure alternative way of carrying out monetary transactions which can be accepted by both formal and informal shops. One proposed way to provide the MRA with an alternative payment is to use an NFC enabled m-payment application - which is the focus of this research.

NFC is a relatively new technology in South Africa. As far as we are aware, its applicability in MRAs of South Africa has not been thoroughly and extensively evaluated. Therefore, this research seeks to investigate the applicability of using NFC enabled m-payments in the MRAs of South Africa by carrying out a thorough feasibility study of the technology. Usage of NFC enabled m-payments has mostly been covered only in theory (Zea, Lekse, Smith, & Holstein, 2012) and lacks standardization and universality (Linck, Pousttchi, & Wiedemann, 2006). This has contributed to the slow adoption of m-payments and the failure of some of the applications that were deployed due to lack of understanding and technical knowledge which requires further research (Mallat, 2007). These challenges will be met by the feasibility study using a Strength, Weaknesses, Opportunities and Threats (SWOT) analysis of the NFC technology, developing a prototype payment application and exploring user adoption of the technology. Both the SWOT and feasibility study will facilitate analysis of usability aspects, social challenges, technical issues and also the user perception of the NFC Technology. The research also seeks to provide an exhaustive pre-emptive ground work for the implementation of a payment application that can be used in marginalized rural communities.

1.4 Research Motivation

This research looks at m-payments in the context of MRA where most of the unbanked and underbanked people are staying (Gillis & Pillay, 2012). Most of rural South Africa has an income that is erratic and predominantly reliant on government grants and thus cannot support the banking packages that have been offered by banks such as internet banking and telephone banking (Makina, 2013; Mkhumbuza, 2013). A study carried out by Mobility showed that 18 per cent of South Africans send remittances to unbanked family and friends regularly (Anong & Kunovskaya, 2013). Such packages have charges that are unaffordable to rural bankers and that has slowed or hampered their adoption. As such, banks have lost valuable customers and the customers lost the opportunity to transact and save money. The introduction of mobile banking has given these people an opportunity to gain access to banking services. Over the last few years

South Africa has experienced high levels of mobile network penetration and this has given more people access to mobile banking. Research shows that there are more people with mobile devices than bank accounts (Anong & Kunovskaya, 2013; Bankole, Bankole, Brown, & Cloete, 2012) even though South African banking system is well established (Kupukile & Ncube, 2011).

Based on these reasons we want to propose an m-payment application that is coupled together with mobile banking that is suitable for both the banked and underbanked staying in the rural areas. Not only will this benefit customers but also the government because through m-payment they can channel in the money in the informal sector to the formal sector and this will help them in economic development. The MRAs constitutes the majority of the unbanked population in South Africa (Coetzee, 2009).

1.5 Research Questions and Objectives

Table 1 gives a summary of the research questions, the research objective associated with the questions and the methodology that will be used to answer the question. The overall research question is: Is it feasible to use a contactless mobile payment application in the marginalized rural areas of South Africa and will the consumers accept this kind of payment method?

Table 1: Research Questions and objectives

Research Questions	Research Objectives		Chapter	Methodology
What are the strength, weaknesses, opportunities and threats of NFC enabled m-payments?	OBJ1	Undertake a SWOT analysis of the technology.	3, 4	• Literature Review
What are the security issues of NFC as a payment technology?	OBJ2	Evaluate security issues	3, 4	• Literature Review
What are the issues that affect the NFC mobile payment ecosystem and	8	Evaluate the NFC mobile payment ecosystem and the Secure Element	5	• Literature review

the Secure Element				
What are the consumer requirements for NFC enabled m-payments?	OB3a	Determine the knowledge of consumers on m-payments.	6, 8	• Interviews • Questionnaires
	OBJ3b	Determine user requirement for an NFC enabled m-payment application		
How feasible is it to implement an NFC enabled m-payment application?	OBJ4	Determine the practicality of implementing an NFC enabled payment application	7, 8	• System analysis, design and implementation
What are the factors that affect utilization of m-payments?	OBJ5	Deduce usability and user perception issues of m-payment applications	3	• Literature Review • Interviews
Will the users accept an NFC enabled payment application?	OBJ6a	Determine factors that affect consumer adoption of NFC m-payments.	6, 9	• Review literature of technology models that are used to test user acceptance of a technology and then select the appropriate model. • Draw factors that affect user acceptance of technology from the models suitable for mobile payment • Deduce hypotheses for factors that affect user acceptance and design a model to test user acceptance based on the hypotheses • Deduce the measurement items for each factor • Evaluate and validate the model and analyse the data qualitatively
	OBJ6b	Determine key determinants of the adoption of NFC enabled m-payment for MRA		
What are the NFC technology deployment strategies that can be adverted for MRA?	OBJ7	Give recommendation on the sustainable implementation framework for NFC applications in South Africa's marginalised rural communities.	10	• Data analysis and Literature review

1.6 Organization of Dissertation

The remaining part of this dissertation consists of nine chapters which are as follows:

- Chapter Two: Research Design – this chapter discusses the research design and the methodology used to conduct the research. The research design section outlines the techniques used. The methodology gives details of the methods used in the research.
- Chapter Three: Literature Review – the chapter reviews literature on m-payments, NFC technology and some of the related work.
- Chapter Four: SWOT Analysis – details the SWOT analysis and also looks at the security issues of the NFC technology.
- Chapter Five: NFC M-Payment Ecosystem and the Secure Element – discuss the NFC m-payment ecosystem and looks closely at major stakeholders. The Chapter also discusses the Secure Element used to store sensitive applications and data.
- Chapter Six: Theoretical Models Review – this chapter reviews literature on the relevant user technology acceptance models. Form the reviewed literature, one model will be chosen and will be modified to suit our research and hypotheses will be derived based on this model.
- Chapter Seven: System Analysis, Design and Implementation – this chapter looks at the analysis, design and implementation of the NFC payment application prototype.
- Chapter Eight: System Testing and Validation – this chapter tests and validates the developed application prototype.
- Chapter Nine: Data Analysis – the quantitative analysis will be used in the interpretation and analysis of the data collected for the technology acceptance model. To illustrate the results, tables, figures and graphs are used. Also, statistical analysis methods are used to test the relationship between the variables.
- Chapter Ten: Conclusion and Recommendation - gives the conclusion, recommendations and makes suggestions for further research.

1.7 Conclusion

In this research we intent to explore the feasibility of using NFC enabled m-payments in the MRAs of South Africa by carrying out a feasibility study of the technology. Perceived security and trust issues are some of the major barriers of electronic and m-payment (Siau, Sheng, Nah, & Davis, 2004). These issues can be overcome by educating the consumers about m-payments and the technology that the m-payment utilizes. Complexity of the mobile device has also hindered the adoption of m-payments (Laukkanen & Lauronen, 2005; Szmigig & Bourne, 1999). This has brought about usability problems and this makes the usability of mobile applications difficult to measure. This is one of the areas that will be greatly considered in this research and the main reason we are proposing the use of NFC technology. NFC enabled mobile payments offer consumers convenience and ease of use and also provide consumers with timely payments and convenience (Yang, Lu, Gupta, Cao, & Zhang, 2012). The relative advantages of m-payments include availability, remote purchases, time independence, place independence and queue avoidance (Mallat, 2007).

The acceptance of m-payments greatly depends on the following factors: interoperability, usability, simplicity, universality, security, privacy, cost and speed (Raina et al., 2011). These are some of the things that we will be discussed in this research. We also aim to assess and evaluate the potential of NFC enabled payments applications.

2 RESEARCH DESIGN AND METHODOLOGY

2.1 Introduction

Research design is the overall outline of the research work that connects the research problems to the empirical research. It defines the procedures that will be followed in order to answer the research questions. The research design links the design, data collection and the data analysis together in the research while ensuring that the research agenda is being addressed. The feasibility and validity of the research depends on the research design that was implemented. Feasibility in this context refers to whether the research design can be executed taking into consideration all the factors that are involved in undertaking the research: time and resources.

The credibility of the research validates the research. The research design must be modelled in such a way that it provides support for conclusions and desired recommendations and this will in turn provide the credibility of the research (Afanu, 2013). The research design needs to be usable. Usability of the research design ensures that all the research questions are answered. This chapter begins with broad assumptions that were made by the researchers and then moves on to more detailed methods about the prototype that was implemented and the methods that were used to collect and analyse data.

2.2 Research Design

Research philosophies are very important especially when undertaking a Social Science research. Even though this research cannot be categorized as a Social Science research, it took into consideration humanistic elements as it aimed at investigating the user adoption of NFC enabled m-payments. The research design adopted for this research was based on the research onion shown in Figure 2-1.

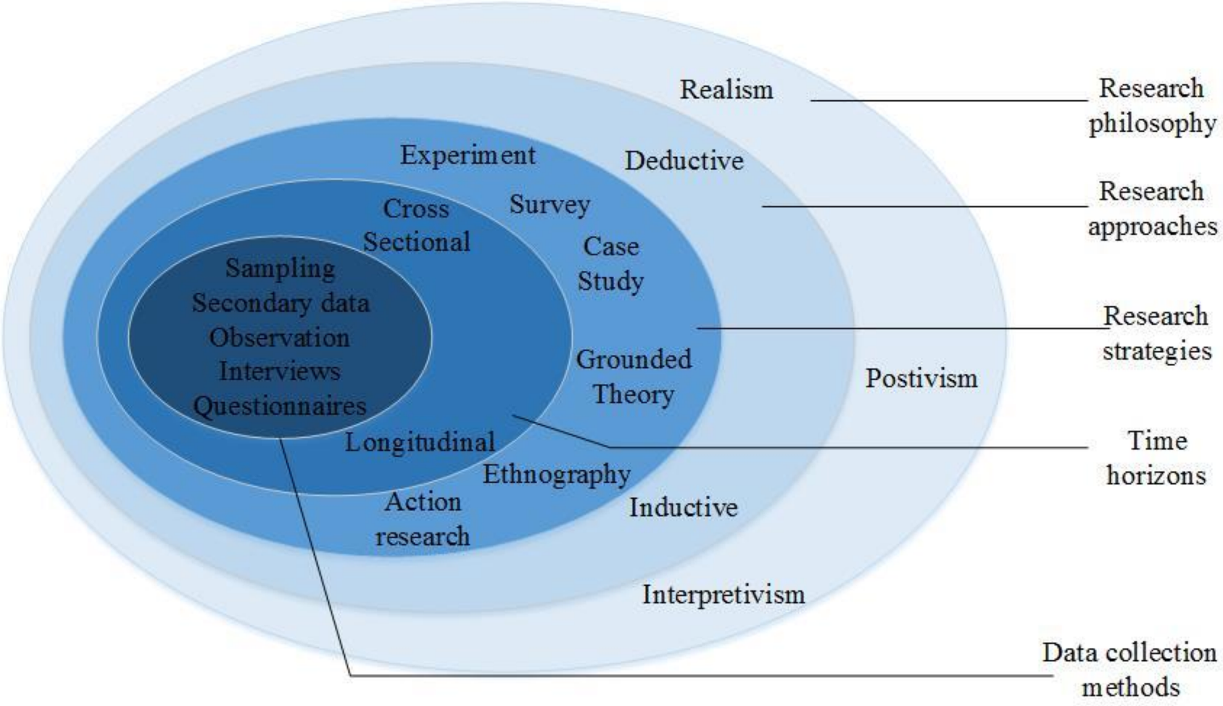


Figure 2-1: Research Onion (Saunders et al 2009)

In 1995 March and Smith argued that both design science and natural science (physical, biological, social and behavioural domains) activities are required "to ensure that IT research is both relevant and effective" (March & Smith, 1995). As we were seeking to give recommendation at the end of the research, it was very important to ensure that our research was relevant. To ensure the relevance of our research, we went through various literature on past research philosophies and activities on IT, design science and natural science.

According to Smith (2006) Information System research that adopts the positivism philosophies and the interpretivism philosophies suffers form, "persistent theory-practice inconsistencies" within the researcher's ontological assumptions and research practice (Smith, 2006) hence this research adopted the realism philosophy as its philosophical stance. Realism is a philosophical position that relates to scientific enquiry. The realism philosophy states that the results of the research will not be biased by the beliefs of the researcher since the researcher and the social reality exist independent of each other. Realism acknowledges that scientific methods are not perfect and that it is not possible to know for certain the reality without carrying out a research.

The realism philosophy enables the researcher to keep an open mind and explore new research methods.

There are two forms of realism: direct realism and critical realism. According to direct realism "what we experience through our senses portrays the world accurately" (Saunders, Lewis, & Thornhill, 2009). Critical realism is directly the opposite of direct realism; it argues that our sense deceive us. Of the two forms of realism the research adopted the critical realism. Critical realism asserts that the world is experienced through two steps. The first step consists of the object and the sensation it conveys and the second step is the mental processing that results when that sensation meets our senses. The first step is enough for direct realism.

Many business and management researchers agree with the views of critical research based on the argument that "as researchers we will only be able to understand what is going on in the social world if we understand the social structures that have given rise to the phenomena that we are trying to understand" (Saunders et al., 2009). In other words the knowledge of the researcher on reality which resulted from social conditioning is only understood through the social actors that take part in the derivation of the knowledge (Dobson, 2002; Saunders et al., 2009). Critical realism acknowledges that the world is always changing. A research carried out by Smith argues that critical realism, "through its novel ontological position, has the potential to advance information systems theory and research" (Smith, 2006). The major benefit of critical realism comes from reinterpretation of science activities (Smith, 2006). The reinterpretation of science activities helps to explain previous research (Smith, 2006).

The research was conducted using the deductive approach. Deductive simply means that the researcher initially has research questions which will then be answered by the research using the research design. This research conducted an exploratory, experimental, prediction, survey and evaluation of NFC enabled m-payment application for MRA. An exploratory study of previous research that has been done on m-payments was carried out throughout this research in order to gain understanding of the NFC technology and the adoption of m-payments. This was done with the aim to give recommendation on the implementation of m-payments for MRA which are supported by literature and practical experience of both the research participants and the researchers. Therefore a prototype payment application was development and used as an experimental payment application. The residents of Dwesa community were actively involved in the implementation and testing of the prototype and a survey was carried out after the residents had tested and approved the prototype.

The research used mixed methods in both data collection and analysis in order to grasp all the complex phenomena of m-payments. The purpose of this research was to conduct an investigation on the applicability of using NFC enabled mobile payments in MRA through literature review and an experimental prototype application. The remainder of this chapter discusses the methodology that was used to carry out this research. The methodology includes the methods used, the data collected and the analysis of the data.

2.3 Methodology

The research was carried out in four phases. The phases were adapted from a research done by Halaweh and the phases were modified to suit our research (Halaweh, 2012). Figure 2-2 shows the details of the four phases.

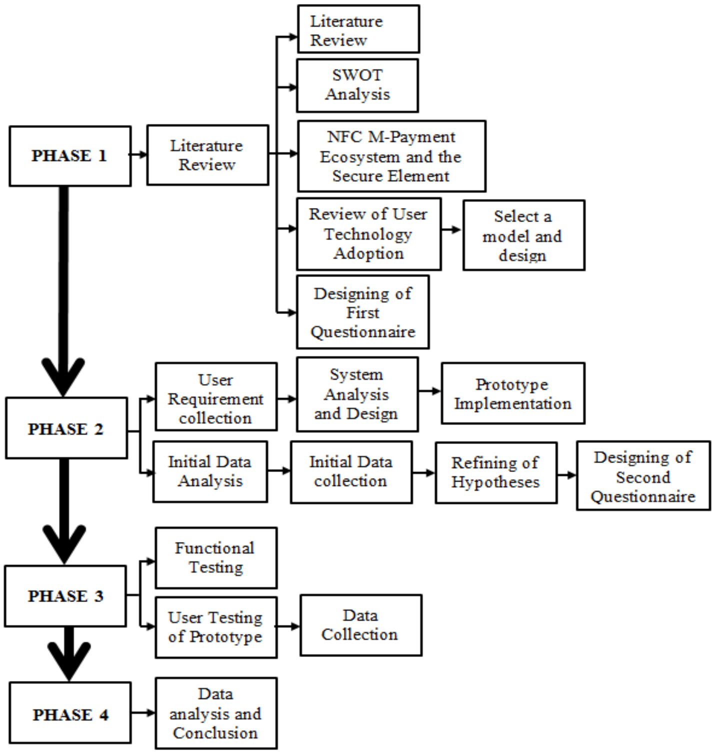

PHASE 1
Literature Review
Literature Review
SWOT Analysis
NFC M-Payment Ecosystem and the Secure Element
Review of User Technology Adoption
Select a model and design
Designing of First Questionnaire
PHASE 2
User Requirement collection
System Analysis and Design
Prototype Implementation
Initial Data Analysis
Initial Data collection
Refining of Hypotheses
Designing of Second Questionnaire
PHASE 3
Functional Testing
User Testing of Prototype
Data Collection
PHASE 4
Data analysis and Conclusion

Figure 2-2: Research Process

2.3.1 Phase 1

This phase focused on understanding the objectives of the research. The phase involved the review of related studies that have investigated the adoption of mobile payments in general and speculated the adoption of m-payments that are enabled by NFC in other countries in great detail. It also involved the study of literatures that explains and explores the NFC technology. This phase is the most important phase because it provides some of the expected results of the research and highlights the originality and contribution of the research.

2.3.1.1 Literature Review

Since NFC is a new technology as far as South Africa is concerned, there was also a need to carry out an overview study of the technology. This was carried out through the review of journals and white papers, and also through the NFC Forum website (http://nfc-forum.org/). White papers were used because of the limited amount of published journals about the NFC technology and NFC m-payment application.

2.3.1.2 SWOT Analysis

Apart from the review of m-payments, this phase also included a thorough SWOT (Strength, Weakness, Opportunity, Threats) analysis of the NFC technology in terms of m-payments. The SWOT analysis was based on the related literature and also on the prototype application.

2.3.1.3 Review of User Technology Adoption Models

This phase also involved the review of different theoretical models that explains "the relationship between user attitudes, perceptions, beliefs, and eventual system use" (Amoako-Gyampah & Salam, 2004). After the review of the models, one model was chosen and modified to suit the research. A set of hypotheses were then drawn based on the relevant literature reviewed and the chosen model.

2.3.2 Phase 2

This phase involved the implementation of a prototype payment application. The first part of the phase involved gathering user requirement from the users and relevant journals and books. The implementation was done using software prototyping. The implementation included the implementation of the mobile phone payment application, the simulated back-end banking system and the payment terminal application. Once the prototype payment application had been finalized, the system was taken to Dwesa for the participants to test it for the last time. Due to the limited number of NFC enabled Android mobile phones among the users, the users were be presented with two NFC enabled mobile devices and a point of sale terminal to use in experimenting with the system.

2.3.2.1 System Prototyping

Evolutionary prototyping was used to implement the application. Evolutionary prototyping is when the initial prototype undergoes a series of refinement. The evolutionary prototyping was the best choice for the m-payment application implementation because it enables each identified user issue to be covered and thoroughly tested.

2.3.2.2 Questionnaire Design

This phase also included the design of the questionnaire. The questionnaire was developed for the TAM based on the hypotheses that were developed in Chapter 6. The responses to the survey questions were designed according the Five-point Likert-type scale with points from 1 to five as follows: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree and 5 = Strongly Agree. Besides the questions based on the hypotheses, the questionnaire also includes the participants' profile information. The profile information did not include the participant's name and surname. As mentioned earlier the population that was targeted was the residents of the Dwesa community which is a MRA in the Eastern Cape. Validity of the data was a major concern when it came to data collection. To ensure validity of the data that was going to be collected, the questionnaire underwent a series of refinement with the help of other academics.

2.3.3 Phase 3

This phase included the testing of the prototype application by the participants and also the testing and validation of the application. The initial part of this phase was to test the functionality of the application and to validate it. The second part was to allow the participants to play around with the application. Usability issues were tested through the prototype system after the users had tested the application. The phase also included carrying out interviews with the participants. The questions used in the interview included structured questions and open-ended questions.

2.3.3.1 System Testing

System testing included user testing and functional testing. Functional testing tested the technological efficiency of NFC as an enabling technology for m-payment applications. User testing included usability testing. Due to lack of hardware security issues were not tested in great depth.

2.3.3.2 Data Collection

Both questionnaire and interviews were used in collecting data. Data for the TAM was collected using the questionnaire. Data collected using the questionnaire was analysed qualitatively using a statistical tool.

Interviews

Besides questionnaires, interviews were also conducted. An interview is a method of gathering data through asking the participant a bunch of questions. These interviews enabled the researchers to understand the opinions of the consumers and have the consumers explain their answers in detail. Interviews were used to get the opinion of the merchants Dwesa. We decided to use unstructured interviews because they allow the interviewees to freely express themselves.

Interview consideration

The following factors were taken into consideration before the interviews were conducted:

- Explaining the purpose of interview

- Duration of interview
- Types of interviews to be conducted
- Language issues

2.3.4 Phase 4

This was the final phase. In this phase the report was compiled that included challenges, barriers and all the factors that affect the adoption and acceptance of the technology. Also the data that was collected in phase 4 was analysed in this phase. In the end recommendation / guidelines for subsequent implementations of mobile payment application for marginalized rural areas will be provided in this phase.

2.3.5 Methodology summary

The phases were designed in such was that each phase was to be completed before another one was begun. The data for the TAM theory was analysed qualitatively using the warpPLS4.0 statistical tool. The data analysis is covered in great depth in chapter 9. Since we were collecting data from people, we had to take ethical principles into consideration. The following Section covers the ethical principles that were taken into consideration for this research.

2.4 Ethical Considerations

An ethical clearance was obtained from the research committee before any data was collected (see APPENDIX E - Ethical Clearance). The following ethical principles were taken into consideration throughout this research: voluntary participation, no harm, informed consent and, confidentiality and anonymity. Data collection was confidential as no personal information about the participants was collected. The participants who were involved had no pressure to comply with that data collection. It was clearly emphasised to each participating individual that participation was voluntary and that they could pull out any time they felt they could not continue.

Both a verbal and written explanation of the research was given to the participants in person. The explanation provided information about the purpose of the project and the role of the participants in it. The participants were also invited to ask questions on any aspect of either the research or their participation they didn’t understand. The participants were also proved with consent forms which clearly stated that their participation was voluntary.

The interviews were conducted in such a way that no participant felt embarrassed or uncomfortable during and after the interviews. The mobile devices that were used were devices that were already available on the market that supported NFC technology; hence no harm was foreseen emanating from mobile devices.

2.5 Summary

This research follows an objective research assumption, a realism approach and used both the quantitative and qualitative methods for data collection. Both questionnaire and interviews were used to collect data. The research design was based on the research onion and was modified to suit the research. The research combines both the social sciences methods and computer sciences methods to ensure validity of the adoption results obtained through the research. The Research was not only investigating the adoption of the NFC technology but was also aimed at testing the technical feasibility of the technology use through the development of the prototype.

3 LITERATURE REVIEW

3.1 Introduction

The journey towards a cashless society started with the introduction of credit and debit cards. Later on contactless cards were introduced. Now the focus is on m-payments. This chapter seeks to give an in-depth knowledge of m-payments and the NFC technology. The chapter is divided into five sections: Mobile Payments, NFC Technology Overview, NFC Mobile Payment Applications, Related works and Conclusion. The section on M-Payments focuses on the different types of mobile payments and their associated technologies. The remaining sections will focus on NFC as a payment technology and some of the related work that has been done by other researchers. Literature shows that a number of m-payments have failed (Mallat, 2007). It is important to understand what previous studies have discovered about these failed services and about the mobile market in general including all unanswered issues (Dahlberg et al., 2008a).

3.2 Mobile Payments

In the past few years there has been a great evolution of both the commerce and the communication industries and their associated technologies. The most recent technologies from these industries are e-commerce and mobile phones respectively. Over the past ten years, these technologies have been gaining attention especially among researchers. The researchers were focusing on combining these two technologies and this combination resulted in a new product called m-payments. M-payments have provided new capabilities of carrying out business. In simple terms an m-payment is when a mobile device is functionally used in executing and confirming payment for goods or services. Zang and Dodgson (2007) defined mobile payments as any type of payment that involves the convergence of a telecommunication network, a bank network and a credit card (Zang & Dodgson, 2007). Ever since their introduction, m-payments have been gaining popularity all over the world including in Africa. Kenya is one of the African countries that has the most success in terms of m-payments (Muriira & Kibua, 2012). According to a research done by Visa International; 89 per cent of consumers who tried m-payments found them to be more convenient compared to other payment methods (Innovision Research &

Technology, 2007). M-payments are not only limited to two parties exchanging financial value in return for goods or services but also includes the transfer of money through the exchange of information (Raina et al., 2011).

3.2.1 Categories of Mobile Payments

Mobile payments can be categorized using location, transaction size or transaction technology. When m-payments are categorized using location, the payments can either be remote payments or proximity payments. A remote payment is a payment that is made without interacting directly with the merchant’s point of sale (POS) (Smart Card Alliance, 2011). Remote payments can further be divided into two types: mobile money transfer transactions and purchase payment transactions. A proximity payment can be defined as a payment in which the mobile phone interacts in some way with a physical POS device to transfer the consumer’s payment information and perform the transaction (Smart Card Alliance, 2011).

In 2007 KPMG categorized m-payment based on transaction into five categories: business-to-business (B2B), business-to-consumer (C2B), consumer-to-consumer (C2C), person-to-person (P2P) and remittance (KPMG International, 2007). In this context the NFC enabled m-payment application we are proposing falls in the C2B category and the NFC enabled peer-to-peer money transfer is a P2P transaction.

The m-payments can also be categorized into two categories based on transaction size: macro payments and micro payment. Micro payments are typically for paying small bills and they limit the amount of money that a customer can spend, in America a user who is using micro payment can spent a total amount of $25 and in UK the total amount is £20 (Smart Card Alliance, 2011). There is no limit to the amount of money that can be spent by a user who is using macro payments. Figure 3-1 shows the different types of mobile payments and some of the technologies that support them.

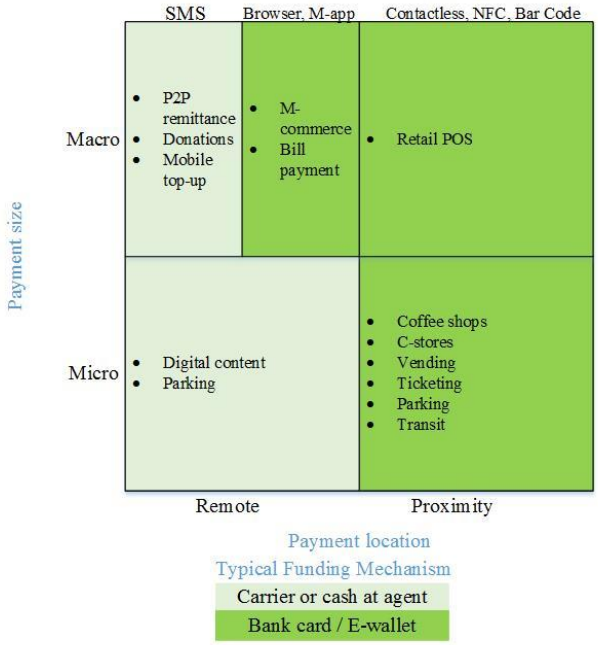


Figure 3-1: Mobile Payment Differentiators (Smart Card Alliance, 2011)

The sources of funds that are used in m-payments include traditional bank account, credit card, debit card, a prepaid card or the bill can be included in the mobile phone bill. Another option of getting funds for carrying out m-payments is by using an agent who will provide the user with a virtual account and the user will then load cash into that account.

3.2.1.1 Remote Mobile Payments

The technologies that support remote payments include SMS, secure mobile browsers and mobile payment applications. Two types of remote mobile payments that will be looked at in this section are Peer-to-Peer or Person-to-Person (P2P) mobile payments and mobile commerce (m-commerce).

3.2.1.1.1 P2P Mobile Payments

This type of payment allows mobile device users to pay one another using a payment application provided by third parties or banks. This is also known as m-money transfer. P2P has become very popular in developing countries where the number of the unbanked and underbanked people is very high. It is based on the Short Message Services (SMS) feature of the mobile device. An example of a P2P money transfer application is M-PESA in Kenya and South Africa (Jack &

Suri, 2011). M-PESA enables consumers to make personal money transfers, ATM withdrawals, pay bills, make point-of-sale purchases and top-up their mobile phone account. M-PESA aims to reduce the costs of transferring money. P2P payment services are also used by business owners to carry out their own payment activities.

3.2.1.1.2 M-Commerce

M-commerce is the use of a mobile device to perform a commercial transaction (Smart Card Alliance, 2011). M-Commerce involves searching or paying for goods and services using a mobile device's web browser.

3.2.1.2 Proximity Mobile Payments

Proximity payments are used when paying for goods or services in stores that are equipped with the appropriate POS or on vending machines. This type of payment usually relies on the financial industry payment infrastructure. Proximity payments can be implemented using NFC or Bar codes technologies. In Bar code-enabled proximity mobile payment, a two-dimensional (2D) barcode is displayed on a smartphone screen and read by an optical scanner at a retail POS, or the smartphone's camera is used as an optical scanner to read a bar code displayed on a POS terminal (Smart Card Alliance, 2011).

3.2.2 Successful Mobile Payment Systems in South Africa

Technologies that support mobile payments can be grouped into three: message based technologies, mobile internet and contactless payments. This section will look at the mobile payment systems that are currently being used in South Africa.

3.2.2.1 Message based technologies

Short Message Services (SMS) and Unstructured Supplementary Service Data (USSD) are the two main message based technologies. Some applications make use of both of them to carry out transactions.

3.2.2.1.1 Short Message Services (SMS)

SMS messages are handled by an SMS service centre that is maintained by the Mobile Network Operator (MNO). The MNO provides its subscribers with a centre number that will be used in sending and receiving messages. Payments are initiated by sending a message from the mobile phone. In South Africa SMS mobile payments are commonly used to pay for digital content such data bundles, ringing tones or games. The services are charged by using premium SMS rates which are more expensive than standard rates. Some banks use SMSs to enable their customers to carry out financial transactions.

The SMS based mobile payments application are currently the most popular applications. SMS based application have the following disadvantages:

- They can only support a limited number of characters
- The messages are complicated and slow to key in (Amoroso & Magnier-Watanabe, 2012; Niina Mallat, 2007; Massoth & Bingel, 2009)
- They are unreliable (Amoroso & Magnier-Watanabe, 2012)
- There is a risk of making a mistake when typing
- They lack encryption and authentication of users
- Can be affected by viruses. In 2006 Bose and Shin discovered that the SMS services were susceptible to denial of service and malware (Bose & Shin, 2006)

3.2.2.1.2 Unstructured Supplementary Service Data (USSD)

The most popular m-payments in South Africa are based on USSD. USSD provides an additional channel for transmitting data and this is different from GSM networks (Chidembo, 2009). An example of a USSD string is *111*444#. USSD transactions are faster than SMS transactions because they are session based. A transaction is cancelled if the session runs out of time before the transaction is complete. USSD are linked to the MNO internal network and therefore they are usually provided the MNO. USSD are complicated to use because the user has to remember the USSD string that is related to the transaction they want to carry out.

3.2.2.2 Mobile internet

The mobile internet provides a way of accessing the internet and payments are made similar to transactions from a personal computer. The m-payments supported by the mobile internet make use of inbuilt internet connections such as General Packet Radio Service (GPRS), 3G (Third Generation) and EDGE. The mobile internet allows the users to enter their credit or debit card information in order to make a purchase. Most of the web based applications are supported by the Wireless Application Protocol (WAP). WAP defines standards for accessing data over a wireless network.

3.2.3 Contactless Payments

A Contactless Payment application is defined as a payment application residing in the Universal Integrated Circuit Card (UICC) or Secure Element (SE) of a mobile phone that employs NFC Technology. Contactless payments are carried out by bringing an NFC enabled mobile phone into close proximity with an NFC enabled terminal point. The transactions are carried out through radio frequencies.

3.2.4 Acceptance of M-Payments

The acceptance of m-payments are affected by (Tomi Dahlberg, Mallat, Ondrus, & Zmijewska, 2008b):

- The technology and the standard
- Regulation and legislation imposed by the government
- Existing purchase and payments habits
- The infrastructure of the national economy

Mobile payments have many unique features that make the more desirable than other payments methods. Some of the major features are (Pihlajamäki, 2004):

- Ubiquity
- Reachability
- Localization
- Personalization
- dissemination

The adoption of m-payments by consumers mainly depends on: security (Bamasak, 2011; Paul Gerhardt Schierz, Schilke, & Wirtz, 2010), cost (Lu, Yang, Chau, & Cao, 2011) and convenience (Kim, Mirusmonov, & Lee, 2010; Mobey Forum, 2011a).

- Cost – the costs for carrying out transaction and for application usage should not be too high otherwise the consumers will be reluctant to use the application. Consumers adopt a new payment method if it is not more expensive than the current payment method.
- Security – includes integrity, authentication and confidentiality. A payment application should also include non-repudiation of transactions. Customers prefer payment methods that offer security that is based on their own understanding and this makes authorization very important.
- Convenience – This includes ease of use, portability, flexibility, speed, ease of setting up and learning to use the payment application. According to Chau (1996) ease of use directly affects the user attitude, intention, actual use and the usefulness of a technology (Chau, 1996). Davis (1993) defined ease of use as the degree to which an individual believes that the use of a system would be free of mental and physical effort (Davis, 1993).

3.2.5 Summary

Rather than replacing credit and debit cards, m-payments represent a transformative digital application that will benefit not only the banked and merchants but also the unbanked and underbanked. For example in Africa’s developing countries remote banking is being carried out using mobile phones through SMSs (Granelli, 2011).

Most of the literature that was reviewed in this section showed that the major barrier to adoption and usability of m-payments is due to the complexity of the m-payment application or the technology that supports the application. Companies and the stakeholders of m-payments are now adopting NFC technology as a new m-payment technology because it is easy to use (Ondrus & Pigneur, 2007). A survey done in USA and Canada in 2012 by Lightspeed research revealed that getting the consumers to use a technology for the first time was a biggest challenge (Lightspeed Research, 2012). The survey also revealed that most consumers were not using mobile devices for payments because they were concerned about the security of the application and their privacy. Therefore it is very important to educate the consumers about the technology before launching its applications. Hence this research seeks to introduce NFC technology to the consumers. The next section discusses the standards and regulation for e-money in South Africa in order to understand the legal regulations and standards that govern m-payments in South Africa.

3.3 Standards and Regulation for e-money in South Africa

This section looks at the standards and regulation for e-money in South Africa in order for us to also consider them in our recommendations mainly based on literature findings. "A fundamental requirement for a stable and secure payment system is that it should operate in a well-defined legal environment, setting out the rights and obligations of each party involved in effecting a payment through the system" (Lawack-Davids, 2012). In South Africa the National Payment System (NPS) covers the whole payment process from the payer to the beneficiary. It also includes the settlement among banks. NPS defines e-money as electronically stored monetary value "represented by a claim on the issuer" (South African Reserve Bank, 2009). The NPS paper also states that e-money can be redeemed for physical cash or be deposited into a bank account. According to the NPS position paper (South African Reserve Bank, 2009) e-money includes internet banking, m-payments and mobile banking. The NPS is also concerned with the interoperability of e-money. If defines the interoperability of e-money as the integration of e-money systems using agreed standards and specifications. According to the NPS interoperable systems "lead to the development of large network externalities which will, in the longer term, reduce operational cost and complexity for all customers" (South African Reserve Bank, 2009).

The Reserve Bank of South Africa welcomes new technological innovative developments and it takes the responsibility of familiarizing itself with any new innovation and investigates its effects on the economy. The Bank acknowledges that new e-money products might require intervention or adjustment that can arise due to the need to (Lawack-Davids, 2012):

- Maintain the integrity, confidence and limit the risk in the NPS
- Assist other regulatory authorities in providing consumers with adequate protection from unfair practices, fraud and financial loss

- Assist law enforcement agencies in the prevention of criminal activity

The Reserve Bank of South Africa regards e-money as a supplement to hard cash and supports the development of e-money products by (South African Reserve Bank, 2009):

- “Supporting the development of a banking industry vision for electronic substitutes for physical banknotes and coin”
- “Supporting the development of national standards to enable interoperability of e-money products and devices”
- “Participating in initiatives aimed at providing secure payment instruments for the general public, including the unbanked and rural communities of South Africa and the Southern African region”

In South Africa the ‘business of a bank’ is only conducted by a bank (Act No. 94 of 1990 – the Banks Act). The ‘business of a bank’ is defined as “the soliciting or advertising for or the acceptance of ‘deposits’ from the general public as a regular feature of the business in question” (Act No. 94 of 1990 – the Banks Act). This research realises the challenge that the Bank Act imposes to m-payment as it makes taking deposits by non-banks an offence in South Africa. Furthermore the Banks Act causes the Banking Sector to monopolize the m-payments and this will not benefit the unbanked. South Africa has a good market opportunity for NFC enabled m-payments. The only challenge that might hinder the implementation and adoption of the m-payment is that of lack of regulations and also the limiting of the issuing of e-money to banks only by the NPS. The regulation by the NPS that only the banks can issue e-money can cause the banks to monopolize m-payments of which the banks currently have been unsuccessful at offering m-payments including contactless payments. FNB and ABSA launched trials applications which were not successful since the application just ended on trial basis.

3.4 Near Field Communication Overview

NFC offers a simple communication way which is touch based. It can be used to complement other wireless technology for example NFC can be used to set-up Bluetooth or wireless connection. NFC hardware can either be installed in a mobile device or can be embedded in a SIM (Subscriber Identity Module) card or Micro SD card (Muriira & Kibua, 2012).

NFC evolved from a combination of earlier RFID contactless identification and interconnection technologies (ISO14443A/MIFARE/FeliCa) and it is based on inductive coupling (Ailisto et al., 2007). This makes it compatible with the ISO 14443 infrastructure. The specification details of NFC are found in ISO 18092 (ISO/IEC 18092, 2013). While NFC builds on the strengths of RFID technology, it also addresses some of the weaknesses of the technology, like security by restricting the physical distance between the devices and offering a two way communication between two devices. Table 2 shows the comparison of NFC with other commonly existing technologies. As shown in the table by usability, consume experience and selectivity, the advantages of NFC over other technologies include ease of use more security. The short range of NFC also provides more security.

Table 2: Comparison of NFC with other existing technologies

	NFC	RFID	Bluetooth
Set-up time	<0.1ms	<0.1ms	~6sec
Range	Approximately 3cm	Up to 3m	Up to 50m
Usability	Human centric, easy, intuitive and fast	Item centric and easy	Data centric medium
Selectivity	High given security	Partially given	Requires pairing (identification)
Use cases	m-payment, authentication, service initiation and mobile wallet	Item tracking and authentication	Data exchange, m-payments, device connection
Consumer experience	Touch or wave to connect	Get information	Configuration required

Figure 3-2 shows NFC- related standards. The top layer defines the mechanism of selecting the communication mode on the lower layer (Ailisto et al., 2007). ECMA-340 defines the peer-to-peer mode of NFC which is the NFCIP-1 mode (ECMA International, 2013b). This is the mode that allows peer to peer exchange of data. ECMA-352 defines the NFCIP-2 which defines how to automatically select the correct mode of operation when initiating communication (ECMA

International, 2013c). Both ISO/IEC 14443 and ISO/IEC 15693 are standards for contactless cards that can be emulated by an NFC enabled device. We are not going to go into detail of these standards because they are not in our focus of study.

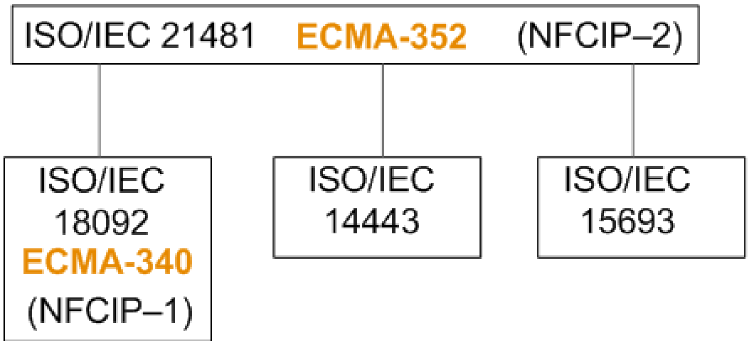
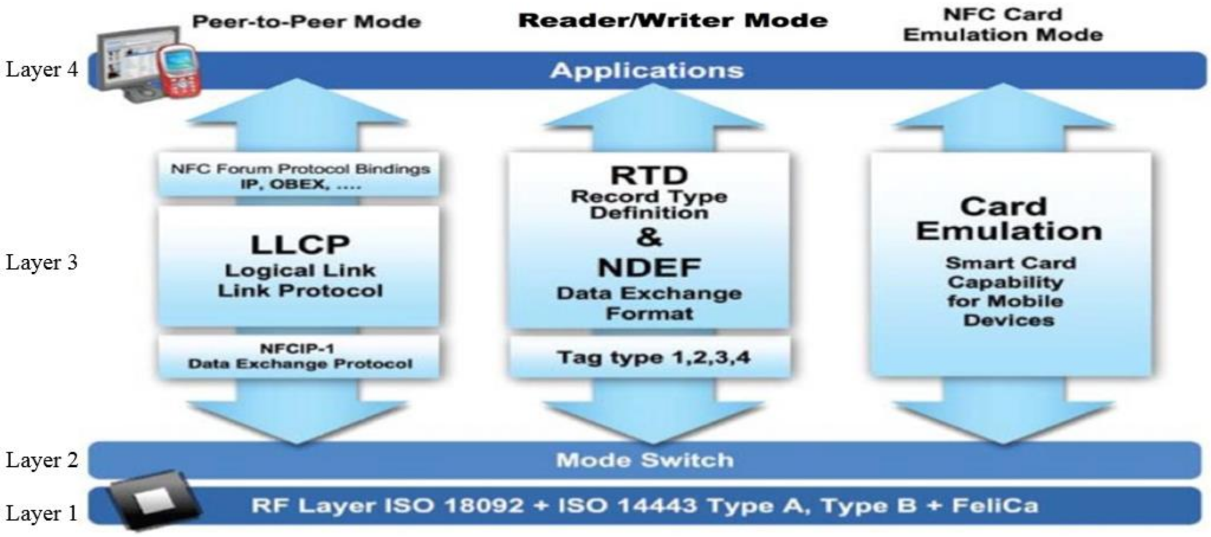

ISO/IEC 21481 ECMA-352 (NFCIP–2)
ISO/IEC 18092 ECMA-340 (NFCIP–1)
ISO/IEC 14443
ISO/IEC 15693

Figure 3-2: NFC Related Standard (Ailisto et al., 2007)

Basically there are three uses of NFC devices and these depend on the operation mode:

- Card Emulation mode: in this mode the NFC device emulates the contactless card. The benefit of this mode is that it eliminates the carrying of a physical object such as cash or credit card and also offers the benefits of m-payments. This mode can also be used to provide authentication mechanism.
- Reader/Writer mode: here an active NFC device can read/write data to/from a passive device such as NFC compatible tags. According to the applications and prototypes that have been developed this is currently the most widely used mode. Currently smart poster applications are one of the most important applications of this mode. The Reader/Writer mode can be easily adapted by many scenarios such as universities, bus stations, hospitals, museums and shops and is easy to implement (Ozdenizci, Aydin, Coskun, & Ok, 2010).
- Peer-To-Peer: Peer-To-Peer communication involves bi-directional communication. In this mode two NFC devices communicate and exchange information at link-level. The data speed of NFC technology is up to 424Kbit/sec and is standardized in the ISO/IEC 18092 standard (ISO/IEC 18092, 2013). Peer -to-peer data transfer occurs between two NFC enabled mobile devices or between an NFC enabled mobile device and an NFC equipped computer. This mode provides easy data exchange between devices compared to other technologies such as Bluetooth.

Figure 3-3 shows the operation modes of NFC as defined by the NFC Forum. The Layer 1 of Figure 3-3 is the analog specifications which define the RF that is used by an NFC Forum device. The specifications also define the strength and the shape of the RF field and also determine the operating range of the device.



Peer-to-Peer Mode
Reader/Writer Mode
NFC Card Emulation Mode
Layer 4
Applications
Layer 3
NFC Forum Protocol Bindings IP, OBEX, ...
LLCP Logical Link Link Protocol
NFCIP-1 Data Exchange Protocol
RTD Record Type Definition & NDEF Data Exchange Format
Tag type 1,2,3,4
Card Emulation
Smart Card Capability for Mobile Devices
Layer 2
Mode Switch
Layer 1
RF Layer ISO 18092 + ISO 14443 Type A, Type B + FeliCa

Figure 3-3: NFC Forum Specification Architecture (Keen, 2009)

Layer 2 consists of the digital protocol specifications. The digital protocol specifications define the implementation specifications of the digital aspects of NFC standards (i.e. ISO/IEC 18092 and ISO/IEC 14443). Its purpose is to define building blocks that are needed to ensure that communication is interoperable among different devices. Layer 2 also specifies when to carry out collision detection.

Layer 3 specifies the communication modes and channels for all NFC devices. It also includes the message coding format for the applications. NFC Data Exchange Format (NDEF) is used when creating NFC messages to ensure interoperability. Record Type Definition is used to construct records in NDEF messages. The use of both RTD and NDEF messages will be covered in chapter 7 under implementation.

Layer 4 consists of the applications for different that uses the NFC technology. The applications can either be peer-To-peer applications, read/write application which allows a device to read/write from another NFC device or they enable an NFC device to be used as a contactless smart card.

There are two communication modes of operation that are supported by the NFC technology: passive and active mode. In active mode both devices are active and in passive mode one device is active and the other one is passive. During communication a device can either be passive or active. An active device generates its own RF while a passive device uses the RF that was generated by the active device. The initiator (the device that starts the communication) initiates communication at a specific speed (106, 212 or 424kbs) using a particular mode. The target (the device that the initiator will be communicating with) replies the initiator using the same speed. Termination takes place when either the two devices move out of range or when the application issues a termination command (Al-ofeishat & Rababah, 2012). Usually a passive device does not have its own power source or its battery powered and will use the power generated by modulating the RF from the active device. During communication the devices cannot change the mode of communication (Al-ofeishat & Rababah, 2012).

During the initialization of communication between two NFC devices a Shared Secret Service is initiated to enable the sharing of a secret between the devices. This secret will then be used by the Secure Cannel Service (SCH) to "standardise the secure channel service to protect all subsequent communication in either direction according to the mechanisms specified by the cryptography standard" (Jovanovic & Organero, 2011).

NFC and other Radio Frequency (RF) wireless communication are differentiated by the RF signal transmission between the initiator and the target (Al-ofeishat & Rababah, 2012). NFC does not freely broadcast radio waves; it uses straight magnetic/electrostatic coupling between devices (Al-ofeishat & Rababah, 2012).

3.4.1 Coding and Modulation

NFC technology uses two type of coding for data transmission: Modified Miller and Manchester coding. The transmission of data depends on whether the device is either passive or active. For active devices the data is coded using either the modified Miller coding or the Manchester coding depending on the baud rate. Passive devices only use the Manchester coding. Table 3 shows the coding and modulation that is used at different transfer speeds. Amplitude-Shift

Keying (ASK) is a form of modulation that represents digital data as variations in amplitude of a carrier wave (ISO/IEC 18092, 2013).

Table 3: Mode of Communication and Data Rates Supported (A. Kumar, 2010)

Baud	Active Device	Passive Device
424 kBd	Manchester, 10%ASK	Manchester, 10%ASK
212 kBd	Manchester, 10%ASK	Manchester, 10%ASK
106 kBd	Modified Miller, 100% ASK	Manchester, 10%ASK

Both coding schemes uses a fixed time slot which is divided into two halves called half bits to transmit a single data bit (Haselsteiner & Breitfuß, 2006). A zero is encoded differently from a one. The Miller coding encodes a zero with a pause in the first half bit and one is encoded with a pause in the second half bit (Haselsteiner & Breitfuß, 2006). The Modified Miller coding has additional rules for encoding zero (Haselsteiner & Breitfuß, 2006). Miller coding causes two subsequent half bits to have a pause if a one is followed by a zero and the Modified Miller coding avoid this by encoding the zero without a pause. In Manchester coding a half bit is either a pause or is modulated (Haselsteiner & Breitfuß, 2006). 100% modulation means that no signal is sent in a pause and 10% means about 82% of the level of a non-paused signal is sent in a pause (Haselsteiner & Breitfuß, 2006). These modulation strengths affect the security of the transmission.

3.4.1.1 Power Transmission and Data Transmission from a Polling Device

As mentioned above NFC technology uses a signal carrier of 13.56MHz for data transmission. A passive device such as an NFC phone in passive mode uses the carrier signal of the polling device as energy source; this means the phone will work even if it is off. The Modulation scheme of the polling device is ASK. If the NFC devices are communicating using the peer-to-peer mode both directions will be modulated and coded like a polling device. In the peer-to-peer mode less power is used because both devices uses their own power supply and the carrier signal is switched off after transmission has ended.

3.4.1.2 Data transmission from a listening Device

A passive listening device also affects the active polling device because of the coupling of the coils and a listening device. "A variation in the impedance of the listening device causes amplitude or phase changes to the antenna voltage of the polling device, detected by the polling device", and this is called load modulation (Minihold, 2011).

3.4.2 NFC Service Categories

The NFC technology can support different types of services which can be grouped into three categories:

- Service Initiation and Configuration – NFC is used to launch another service such as setting up Bluetooth connectivity or opening a website.
- Peer-To-Peer Communication – here the technology is used to transfer data between two devices. NFC technology can only be used to transfer small amount of data because it supports a maximum speed of 424 kbps (ISO/IEC 18092, 2013).
- Payment and Ticketing – NFC technology can be used to support m-payments applications. NFC reduces the cost of maintaining issuing tickets.

3.4.3 NFC Architecture

An NFC enabled mobile device is integrated with circuits for NFC interface and a secure element (SE). The NFC interface consist of an integrated circuit called an NFC controller, an NFC antenna and an NFC Contactless Front-end which is a contactless analog/digital front-end (D. Kumar, Gonsalves, Jhunjhunwala, & Raina, 2010; Raina et al., 2011). The NFC controller enables NFC transactions. Each NFC enabled device must have at least one SE which enables it to carry out secure proximity transactions with other NFC enabled devices. The SE is connected to the NFC controller. The SE provides secure storage for NFC applications and also for data that is used by the applications. The following are the common interfaces that are supported between the controller and the SE: the Single Wire Protocol (SWP) and the NFC wired interface. As shown in Figure 3-4, the SE can be accessed and controlled either internally from the host controller or externally from the RF field externally.

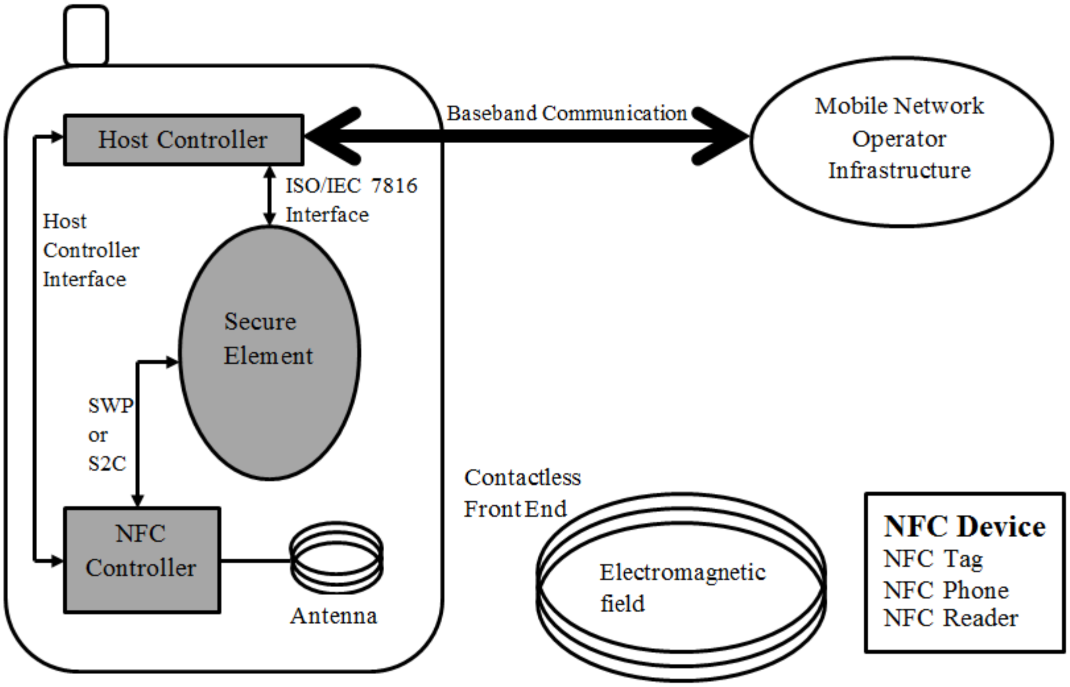


Figure 3-4: Architecture of NFC technology integrated in a mobile device

The operating mode of the device is set by the host controller through the Host Controller Interface which connects the host controller and the NFC controller. The host controller also establishes a connection between the NFC controller and the SE and processes the data that is send or received (Raina et al., 2011).

3.4.4 Advantages of NFC

NFC offers the following advantages (Patel & Kothari, 2013):

- Intuitive – interaction between devices occurs by just bringing two devices into close proximity.
- Interoperable – NFC is backward compatible with RFID.
- Ready Secure – Communication distance is reduced to few centimetres and this reduces security risks.

3.4.5 NFC Forum

The NFC Forum was formed in 2004. The purpose of the forum is to advance the use of NFC through developing specifications, that ensures interoperability among devices and services, and educating the market about NFC. The forum was founded by NXP, Sony and Nokia. The NFC Forum is now made up of over 170 members who include mobile device manufacturers, applications developers, and financial services institutions. All these members work together to promote the use of the technology. The mission of the NFC Forum is to advance the use of NFC technology by:

- Developing standards based specifications that ensure interoperability between devices and services
- Encouraging the development of products using NFC Forum specifications
- Educating the market globally about NFC technology
- Ensuring that products claiming NFC capabilities comply with NFC Forum specifications

3.4.6 Summary

According Raina et al (2011) NFC technology brings user experience, convenience and security of contactless technology to the mobile devices, and is enabling quick transactions and services in our day-to-day lives (Raina et al., 2011). NFC technology is desirable because it does not require the user to perform complex manual configurations.

3.5 NFC Mobile Payments

The complexity of SMS based m-payments gave rise to the need of an alternative m-payment which is simple and faster in biometrics and keystrokes (Raina et al., 2011). NFC technology m-payment method also known as contactless payment method can overcome the weaknesses of SMS based mobile payments methods. Currently there are many mobile contactless payment applications in use all over the world and these include Discover Zip, American Express ExpressPay, MasterCard PayPass, Visa PayWave and Google Wallet. Many contactless mobile payment applications have been successfully implemented and deployed in Japan and South

Korea as well. In 2009 17 million citizens of Japan and approximately 4 million people in South Korea were already using contactless m-payments (Ezell, 2009). A research on the types of wireless technologies used for mobile payments done by Zmijewska highlighted that NFC shows promise for payments and ticketing because of its ease of use (A Zmijewska, 2005).

There are different types of technologies that enable m-payments and these include Bluetooth, GPS, and Geolocation. Table 4 shows a comparison of some of the technologies that are supporting m-payments and mobile money transfer. Geolocation payments make use of an application that detects the location of all the other users who have the same application on their mobile devices within a given area using WIFI, GPS or Bluetooth. This technology enables users of the application to pay each other without the need of transferring banking details. An example of Geolocation payment in South Africa is the GEO Payments on the FNB Banking App.

Table 4: Comparison of m-payments technology

	NFC Payments	Geo Payments	Mobile money Transfer services e.g. M-PESA, MTN Money
Technology	NFC chip Application	GPS/WIFI Application	At least 2G SMS and/or USSD
Compatibility	NFC devices	Any smartphone	Smartphones and feature phones
Operating Range	Approximately 3cm	Restricted by network signal	Restricted by network signal
Power consumption	Low - Medium	Medium - High	Low
Interference Hazard	Low	Medium - High	Low

Geo payments heavily depend on the quality of the network signal. They also have the issue of the privacy of the users since the users can be easily detected with anyone who has the same application on their mobile devices.

For a contactless application to work, it must be personalized with an account which is issued by the stakeholder which is in charge of the payment application. Mobile contactless payment applications provide lucrative opportunities for all the stakeholders involved in the payment application. One of the barriers that was affecting the adoption of m-payments was usability and this issue is overcome by NFC technology through its simplicity. NFC technology supports all five m-payments transaction categories: C2P, P2P, B2B, C2C and remittance. Only two NFC m-payments applications that are globally recognized are going to be reviewed in this section.

3.5.1 Examples of NFC Mobile Payments Applications in Use

This section discusses two NFC enabled mobile payments applications that have been successfully deployed and are currently in use. The two examples were chosen mainly because they are successful and are being used globally.

3.5.1.1 Google Wallet

Currently Google is the major player in m-commerce with the Google Wallet application (Du, 2013). The Google Wallet is a mobile payment system that has a service which allows users to purchase goods using their NFC enabled smartphones. Google wallet was launched on the 26th of May 2011. The Google Wallet is an example of a C2B transaction application. Currently the financial intermediaries for the Google Wallet are MasterCard and Citigroup (Aamoth, 2011). Google meets both of the companies' security requirements.

The Google Wallet replaces physical credit and loyalty cards. Google is the one that provides the merchants with the mobile payment terminals and the downloadable Google Wallet application (Du, 2013). Consumers with NFC enabled phones can download and install the application into their phones. The consumers can then set up a virtual credit card or pre-paid card using any of the two financial intermediaries (Du, 2013). After this the consumers can then use their mobile phones to pay at any participating merchants by tapping their phones on the Google payment terminal. Information about the shoppers buying habits can be instantly collected and used for marketing purposes. Basically the consumers just have to tap their smartphones on the terminal to make a payment and the payment will be processed and the details of the payment will be stored on the phone.

Google was aiming at building an ecosystem around Google Wallet (STRATEGY ANALYTICS INSIGHT, 2012). The payment credentials are encrypted and stored on a Secure Element chip that is separate from the Android device memory and can only be accessed by authorized programs. Figure 3-5 shows the payment process for the Google Wallet.

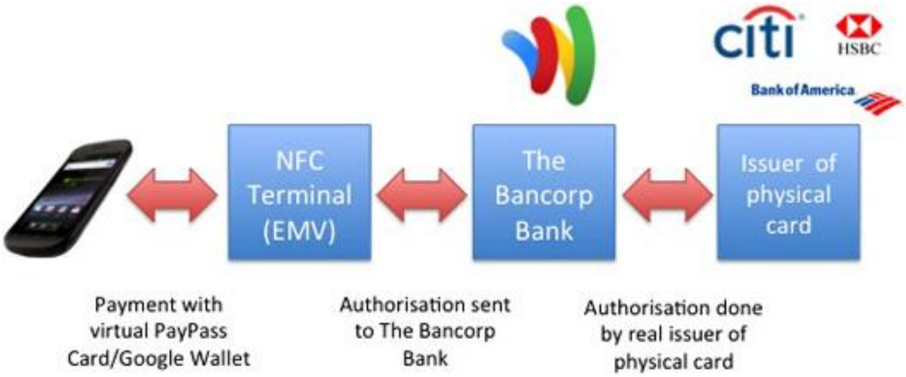

citi
HSBC
Bank of America
NFC Terminal (EMV)
The Bancorp Bank
Issuer of physical card
Payment with virtual PayPass Card/Google Wallet
Authorisation sent to The Bancorp Bank
Authorisation done by real issuer of physical card

Figure 3-5: Google Wallet payment process

One of the challenges that Google Wallet has faced is that for a customer to be able to use the application, the customer has to own an account with one of the issuing bank such as Citi Bank or register to use Google's prepaid payment card. Another limitation of Google Wallet is that it is limited to Android phones.

3.5.1.2 Osaifu- Keitai (Japan)

Different m-payment applications have been successfully deployed in Japan and many consumers are using them to make payments at convenient stores, transit fares, and many other goods (Ondrus & Pigneur, 2007). A leading MNO in Japan called NTT DoCoMo launched a mobile wallet called Osaifu-Keitai in 2004. “The Osaifu- Keitai platform enables mobile phones to be used for proximity payments in shops via a dedicated reader device, and it also supports remote (online) payments” (NTT DOMOCO, 2011). Some of its applications include credit cards, identity cards, pass keys, loyalty cards and mass transit passes (NTT DOMOCO, 2011). In 2011 at least 1.4 million merchants in Japan were already accepting Osaifu-Keitai (NTT DOMOCO, 2011).

The executive director of NFC Services and Innovation for NTT DoCoMo Norio Nakamura said that the benefits of Mobile NFC include increased speed for transaction processing, simplicity and data collection. He also said NFC makes it easy for merchants to track the effectiveness of their promotions and collect data on customer behaviour. All these benefits make NFC a powerful marketing tool. NTT DoCoMo has managed to keep expanding its NFC m-payment through collaboration with other influential stakeholders which include leading companies in a number of industries (NTT DOMOCO, 2011). NTT DoCoMo succeeded by "effectively explaining the NFC concept and its many merits, as well as making strategic investment alliances to accelerate the deployment of reader/writer terminals in proprietorships" (NTT DOMOCO, 2011). In 2012 NTT DoCoMo took Osaifu-Keitai global through signing a deal with MasterCard that enabled 17 million ID mobile card holders to use their mobile phones to make payments at MasterCard PayPass in 41 countries and on the 560, 000 Osaifu-Keitai POS in Japan (Clark, 2012).

3.5.2 NFC Payment Applications Adoption Challenges

Jovanovic and Organero identified the following as some of the most important factors which are preventing the faster adoption of NFC technology as a mobile device payment technology (Jovanovic & Organero, 2011):

- Lack of clearly defined standards across the industry.
- Stakeholders who are collaborating to adopt the technology are more concerned about making profit regardless of the possibility of technical inferiority of the solution they are offering.
- Merchants are waiting for critical mass of consumers before they can accept NFC m-payments and the consumers are waiting for the merchants to accept NFC m-payments before they can purchase NFC enabled devices and adopt NFC m-payments. Hence in most countries the merchants and the consumers are caught in a deadlock.
- Some consumers are concerned about the battery life of their device, receiving a call or other mobile network action while a payment transaction is in progress.

3.5.3 Advantages of NFC mobile payment over traditional methods

The following are advantages of the NFC Mobile Phone that will widen the opportunities for NFC services (NFC Forum, 2008):

- Interactivity – the mobile device has a user interface that will enable the user to interact with the payment application. The application can keep purchase records including receipts. The user can activate or deactivate any of the payment using the user interface.
- Remote Multi-Application Management – NFC mobile phones can support more than one payment application. Mobile network operators enables the mobile phone to support application management functions such as dynamic provision to a trusted execution environment, assignment of trusted areas, application download, personalization and locking/unlocking. Execution of these functions is done remotely in real time on the mobile device. This allows the user to be in control of their accounts all the time.
- Remote User Management – NFC technology enables the use of a user-centric model because the user can remotely manage all the payment application on the mobile device. Customers and service providers are able to use the User management function by communicating through the mobile network which is always on. “For example, service providers, with users’ consent, can retrieve NFC service usage records and send users customized information during transactions or on other occasions. In another example, users can access their personal data in real time and can be more proactive about the information they would like to receive” (NFC Forum, 2008).

3.5.4 Summary

Merchants who have employed contactless m-payment have experienced faster transaction time, increased spending and increased customer loyalty (Smart Card Alliance, 2007). Contactless payments were easy for merchants to adopt because the payments used existing financial networks. NFC technology can support Person-to-Person financial exchange (Du, 2013). This enables a user who owns an NFC enabled device to transfer money to another user.

An m-payment can either be an application connected directly to an account offered by bank or a TSM or virtual wallet. A virtual wallet offers various services which include virtual cards, loyalty cards, vouchers, coupons and transport ticketing. The consumer will choose the card to use when making a payment transaction. In this research an application connected to an account offered by a bank was be considered for the prototype m-payment. A simulated banking system was used for the bank.

A research done by Ondrus and Pigneur (2007) showed that the contactless payment method is more efficient than the traditional cash payment method (Ondrus & Pigneur, 2007). Most merchants did not adopt the current m-payments previously because the process for a transaction is long and tedious but NFC technology will enable the development of applications that are more user-friendly and quick to use since they will not be menu based.

3.6 Related Work

This section will consider some of the work that has been done on the adoption and feasibility of using NFC technology for mobile payment in different countries. The following researches were considered: The Future Mobile Money Service for Kenya, Exploring Consumer Adoption of NFC-Enabled Mobile Payments in South Africa, Exploring consumer adoption of m-payments – a qualitative study. The first two were chosen because they consider m-payments in the context of Africa. The second was also chosen because it covers a survey of the adoption of NFC enabled m-payments in South Africa. The last research was chosen because it explores the determinants of the adoption of m-payments which will also be considered in this research.

3.6.1 NFC Technology: The Future Mobile Money Service for Kenya

In this paper, Muriira and Kibua (2012) discusses the feasibility of m-payments and the future opportunities of NFC in Kenya (Muriira & Kibua, 2012). Kenya is one of the few African countries with a high adoption of m-payments. M-payments are currently carried out in Kenya through: the premium SMS based transactional payments, direct mobile billing, and mobile web payments. The authors of this research paper identified that the existing technologies that were being used in Kenya had challenges that affected customers, banks as well as to the Mobile Network Operators (MNO). The current technologies supported applications that were menu based and this led to usability issues and also made the development of the application complex.

The research purpose of this research was to investigate the opportunities of NFC technology as an m-payment application technology to consumers, banks and telecom companies.

From the review the researchers found that the adoption of NFC technology will eliminate the process and cost of transferring money from a mobile account such as an M-PESA account into a bank account and vice versa. According to this research, the number of people who have mobile phones doubles the number of people who have bank accounts and gives the MNO an upper hand over the banks. For the telecom companies the researchers found that NFC technology gives a good business opportunity for MNO to have a competitive advantage over banks. For the banks the researchers found out that since the banks were already issuing out credit and debit cards to their customers so they can use the NFC enabled device to replace the bank cards with an NFC payment application that stores virtual cards and the new payment application will use the same infrastructure that was used by the cards. This means that the banks can develop the application independent of the MNO. The researchers concluded that more than half of the population of Kenya will benefit from NFC payment application.

3.6.2 Exploring Consumer Adoption of NFC-Enabled Mobile Payments in SA

In this research, Chidembo's (2009) goal was to investigate the feasibility of the South African consumers adopting NFC enabled m-payment. This research was only limited to the Gauteng province of South Africa which is an urban area. The research did not "analyse in detail the strengths and weaknesses of the NFC Technology" (Chidembo, 2009). This research showed that payment needs of consumers in South Africa can be met by the adoption of NFC enabled mobile payment. Contactless mobile payments can be successfully implemented and deployed in the South African retail industries. The research also showed that consumers failed to identify the advantage of using contactless mobile payments over traditional methods. In summary, based on this research the author provided the following recommendations to any potential stakeholder that would want to provide NFC enabled mobile payment service to their customers: the number of steps for a payment transaction should be less than 4, reputation of the stakeholder should be taken into consideration and the transaction should be cheap. "This research has proved the important role that certain NFC enabled mobile payment adoption characteristics such as cost, relative advantage, complexity, compatibility, trust and security has in the future adoption of this mobile payment method by South African consumers" (Chidembo, 2009).

3.6.3 Exploring consumer adoption of m-payments – a qualitative study

In this research, Mallat (2007) examines the willingness of consumers to use m-payments. The objective of the paper was to investigate the adoption of mobile payment by consumers through "empirically examining the adoption determinants that are specific for the mobile payment context". This research identified the following as the characteristics of mobile payments which increase the complexity of m-payments adoption environment:

- several competing providers which includes financial institutions and MNO
- two groups of adopters which are different (merchants and consumers)
- lack of standardization and compatibility

Table 5 shows some of the factors that affect the adoption of mobile payments.

Table 5: Factors affecting consumer adoption of m-payments (Niina Mallat, 2007)

Adoption determinant	Contributing factors	Effect	depends on situation use
Relative Advantage	• Time and place independent purchases • Queue avoidance • Enhance payment instrument availability • Complement cash	+ + + +	yes
Compatibility	• High with digital content and services • High with small value purchase at POS • Low with large value purchases	+ + –	yes
Complexity	• Complex SMS formats, codes, service numbers • Management of separate accounts burdensome • Complex registration procedures	- - -	no
Costs	• Premium pricing & high transactions costs	-	no
Network extension	• Lack of wide merchant adoption • Proprietary devices / services	- -	no
Trust	• In merchants • In telecom operators • In financial Institutions	+ + +	no

Perceived security risks	• Unauthorized use	-	no
	• Transaction errors	-	
	• Lack of transaction record and documentation	-	
	• Vague transactions	-	
	• Concerns on device and network reliability	-	
	• Concerns on privacy	-	

The researcher used diffusion innovation theory to do the analysis. According to Laukkanen and Lauronen (2005) mobile banking gives the consumers the freedom of location free access and from this Mallat concluded that m-payments gives the consumers " a timely access to financial assets and an alternative to cash payments.

3.6.4 Discussion of the findings of related work

All the papers that were reviewed in this section agree that the customers can immensely benefit from contactless m-payments application. According to the first papers reviewed, m-payments will enable the unbanked and underbanked to have access to banking services because the MNOs have penetrated marginalized areas better than the banks in terms of network coverage (Adkins, 2013; Aker & Mbiti, 2010; Ondiege, 2010). Like most researchers who have researched the feasibility of the adoption of m-payments, the above researchers focused mainly on consumers and merchants in urban areas. The unbanked and underbanked usually reside in the marginalized rural areas. At the moment these are the consumers that are making use of the SMS based P2P money transfer like M-PESA a success. Clearly these consumers need to be included in all the feasibility studies on the adoption of NFC especially in developing countries. This thesis seeks to carry out a feasibility study of the adoption of NFC in these in these areas. The last paper that was reviewed in this section provided a comparison platform for this research. Instead of just carrying out an empirical study on the adoption of NFC enabled m-payments on people who have probably never used m-payments, in this research a prototype NFC payment application will be designed and developed and it will be used to help introduce NFC technology in the proposed area of study.

3.7 Conclusion

Various literatures were reviewed in this chapter. Even though NFC technology faces many strong competition there is no doubt that its simplicity will be a major determining factor in deterring popularity amongst users (Du, 2013). Most of the researchers who have done some work on NFC agree that the technology eliminates connection complications.

Interoperability, Usability, Simplicity, Universality, Security, Privacy, Cost, Speed and Cross border Payments are some of the most important challenges that needs to be overcome for m-payment to be accepted (Raina et al., 2011). The success of mobile payments depends on many factors which include: security factors, stakeholders, consumer knowledge and the mobile devices themselves. Consumers are mostly concerned about convenience, security and ease of use. Consumers are most likely to adopt a technology if they know that they will benefit from it, understand how it works and if it is not expensive.

The addition of NFC does not increase the cost of the mobile device with a huge margin. “The incremental cost of equipping a mobile phone with NFC capability is relatively small, adding perhaps $10 to $15 to the cost of a phone” (Mccarthy & Data, 2008). In 2012 the incremental cost of an NFC enabled device was estimated to be around &$3 - $5 (Deloitte, 2012). Lack of mobile phones that are equipped with NFC among the customers might hinder the adoption of NFC payment applications. This could be overcome by using SIM cards or Micro SD that are equipped with the NFC hardware. Alternatively the consumers can simply add an NFC sticker at the back of their mobile phones (Jovanovic & Organero, 2011). The only problem with these alternatives is that the NFC hardware will be lying under multiple layers of metal and plastic and this might affect the quality of the antenna’s signal (Muriira & Kibua, 2012). More still needs to be done to prevent NFC from failing the same way the other technologies have failed. There is need to analyse and understand the requirements that are needed to make NFC succeed (Ondrus & Pigneur, 2007).

There is clearly no doubt that NFC will bring about better performance such as speed compared to other m-payment technologies and traditional payment methods such as cards. Even though countries like Japan have successfully implemented NFC mobile payments, they are not without flaws. Most of the mobile payments applications that have been deployed in Japan lacks interoperability and has caused the retailer merchants to have up to four POS reader terminals (Ezell, 2009). This can be overcome by the collaboration of all the stakeholders in the country. The stakeholders do not necessarily have to come up with a single application but they can define standards that will enable their application to be interoperable. Mallat (2007), concluded that for m-payments to be widely adopted the applications must be integrated with the existing FIs and MNOs. In conclusion most researchers agree that cashless payments methods offer speed and convenience, and any mobile application must demonstrate these advantages over traditional payment methods. For a successful implementation of a mobile payment application there is need to have a thorough understanding of the country's market characteristics and their effects weather positive or negative on m-payment adoption (Pope et al., 2011).

4 SWOT ANALYSIS FOR NFC TECHNOLOGY

4.1 Introduction

This chapter provides part of the answers to questions that are associated with objectives OBJ1 and OBJ2. SWOT analysis is the identification of strengths, weaknesses, opportunities and threats (SWOT) to yield strategic insights (Valentin, 2001). The SWOT analysis helps in the understanding of the strengths and weaknesses of the technology and also in identifying the opportunities that are open to the technology and the threats that might be faced (He, 2012).

The numbers of people who are using smartphones are increasing every day. The smartphones are equipped with innovations targeted at making the life of users easier. These innovations include technologies such as NFC technology and Bluetooth which makes it easier for the users to perform different kinds of tasks. In 2013 Jandebeur & Schaeufele carried out a SWOT analysis of NFC technology to show weather NFC enabled smartphones can be used to increase purchase efficiency to merchants and consumers when used as a replacement for credit and debit cards (Jandebeur & Schaeufele, 2013). Besides what was covered by Jandebeur & Schaeufele (2013), in this research we are considering NFC technology as a payment solution to the unbanked and underbanked as well. This chapter details a SWOT analysis of the NFC technology. NFC technology is believed to have great potential by service companies and mobile device manufacturers (Strommer, Hillukkala, & Ylisaukko-oja, 2007). This potential will be explored in detail in the following sections.

4.2 Strengths

"NFC is compatible with almost all existing RFID solutions, increasing its potential use with already installed commercial deployments; it is considered an open technology; and it is recognized by ISO/IEC, ETSI, and ECMA" (Sammarco, 2010). NFC can use the already existing infrastructure of RFID. It has the advantage of providing a two way communication over RFID; this means it is more secure than RFID. Its short range of communication enables automatic coupling and reduces security risks. One of the main advantages of NFC technology as a mobile technology is that it is simple to use. It is easy to connect two devices using NFC because there is no need of exchange of data between the devices before connection as is the case with Bluetooth - the devices only need to be brought close together and connection is automatic.

NFC can also act as a complimentary technology to other technologies such as Bluetooth where it can be used to carry out initialization of connection. In this case NFC is user to transmit connection messages between the devices. This will help consumers to understand and accept the technology quickly. The technology can also be used in user authentication through card emulation. In this case the device can store the identity card of the user which can be used in authenticating even during m-payments.

Smartphones have enough processing power and memory for NFC applications. When performing a mobile payment using an NFC enabled phone, all that the user has to do is "wave their mobile phone in front of the NFC reader to complete the transaction and this is extremely fast and simple" (He, 2012). Besides the fact that mobile phones especially smartphones can be erased remotely if the phone is lost or stolen, the mobile phone also provides two-factor authentication (Jandebeur & Schaeufele, 2013). NFC enabled mobile devices can be password protected and the m-payment application can also be password protected and this makes NFC to be more secure than credit cards and debit cards; and other payment methods as well. NFC can make financial transactions faster, more convenient, and more accessible. It also has the following advantages: ubiquitous purchase, queue avoidance and a payment alternative for cash. For other stakeholders other than merchants and customers, NFC enabled m-payments provides new revenue channel. Also since the users are familiar with their devices, NFC provides quick transaction which will be advantageous to the merchants as this will reduce queues in their shops.

NFC technology can be used in a wide range of industries and service. In this research we have already identified two: peer-to-peer money transfer and m-payments. NFC can also be used in the transport industry and in marketing. Because NFC is a new technology, industries that adopt NFC technology would provide better services to their consumers and would be viewed by consumers as up to date and progressive. This would help these companies to retain their consumers and also to gain new customers. The younger generation wants to be identified with dynamic and progressive companies; companies which adopt new technology are viewed as dynamic and appealing to the younger generation.

4.3 Weaknesses

The weaknesses of NFC technology for m-payments include lack of NFC enabled devices among the customers despite their availability on the market. We have observed that most people in the MRA of South Africa do not own NFC enabled devices which mean that they have to buy the devices or the m-payment service providers have to provide the people with mobile devices. Also merchants who decide to adopt NFC enabled m-payments would need to buy the appropriate readers.

Most of the devices that have NFC technology are smart phones and the battery life of these devices is already constrained for most users who use many applications (Ghag & Hedge, 2012). With NFC being powered by battery, the life of the phone’s battery will also be reduced by m-payments enabled by NFC. Depending on the m-payment application that was developed, both the CPU and storage memory might also be affected.

Since mobile devices are small, adding the NFC antenna and other NFC parts might require the mobile device manufacturers to redesign older cheaper models and this will make their new version more expensive (Jandebeur & Schaeufele, 2013). Worldwide the NFC market is still significantly small and NFC enabled devices are not yet sufficiently widely deployed.

For NFC enabled m-payment, there is still more that needs to be done to convince customers and other stakeholders that NFC is a secure technology that they can benefit from. Since NFC is still a new technology in the m-payment sector, stakeholders needs to invest in it, before they can start reaping the benefits of using. Stakeholders who invest in NFC at the moment will be taking a risk and most small companies will not be able to invest because it is expensive investment. This is because there is still more that needs to be done in terms of marketing and educating the customers and the merchants also in terms of hardware and software requirements. Merchants may decide not to adopt m-payments due to the following reasons: high costs, lack of relative advantage, complexity and lack of standardization of applications (low compatibility) (Tomi

Dahlberg et al., 2008a). The stakeholders offering an NFC enabled m-payments need to ensure that these reasons will not affect their payment application.

The other weakness of NFC are its communication range of 3 cm or less and its data transfer rate which is up to 424kpbs (ISO/IEC 18092, 2013). The low rate data limit causes NFC to be used to transfer small amounts of data. The payment application and its data need to be stored in a secure element but some NFC devices lack the secure element. This affects stakeholders other than the MNOs because they have to provide the secure element to the customers.

4.4 Opportunities

With time the weaknesses of the NFC technology will be insignificant compared to its strength and the opportunities it offers. There is more that can be done by NFC enabled devices other than performing contactless mobile payments. The applications that can be developed for NFC can be grouped into three categories: Peer-to-Peer, Service Initiation and Payment and Ticketing (Cavoukian, 2012). Service initiation includes marketing and information retrieval applications. This section gives details of some of the most popular applications that can be enabled by the NFC technology.

4.4.1 Mobile Payment

NFC provides a way for carrying out efficient payments and this can be achieved either through card emulation or the read/write mode. In card emulation the NFC enabled device will be used in place of traditional credits and debit card. Card emulation is the easiest method to adopt because it uses the already existing infrastructure and smart card readers. Card emulation reduces the number of cards that a user carries around.

A mobile wallet that is enabled by NFC is another example of the use of an NFC enabled mobile phone in read/write mode. This mode usually constitute of an NFC tag that contains the banking information of the store and a mobile device that has an application that uses this information to carry out a banking transaction (Nambi, Prabhakar, & Jamadagni, 2012). This is method does not require a reader or a POS terminal. Another method for the mobile wallet will be to use a reader as in the case of the Google wallet. The ability of the NFC technology to run on mobile devices is an added advantage to the NFC enabled m-payments over other form of payments because customers carry their mobile devices everywhere they go. M-payment offers new revenue channel to both MNOs and banks.

4.4.2 Ticketing

NFC technology can also be used to provide mobile ticketing (m-ticketing). M-ticketing can be used in the transport sector, sports sector and the entrainment sector. When a customer buys a ticket electronically using m-payments or using cash, the ticket is stored in the mobile device. The user will use the ticket by swiping his/her phone. M-Ticketing improves access to ticketed services and offers convenience to customers.

4.4.3 Marketing

NFC technology can also be used for advertising; tags can be put in busy areas such as shopping malls and stations that provide detailed information about a certain product. The users can obtain the adverts by swiping their phones.

4.4.4 Loyalty and Coupons

One opportunity of NFC technology is that it provides a way for electronically storing and using loyalty points and coupons. The NFC enabled device provides a good opportunity for consumers to manage their coupons and loyalty points. This also enables the providing stakeholder to reward a customer for using NFC enabled m-payment. This is one way that can increase the adoption rate of the m-payments.

4.5 Threats

Besides the threat of competition from other wireless technologies, the NFC technology also faces the threat of security issues. Security issues can hinder the adoption of NFC technology. Even though there are many opportunities for the NFC technology, customers will not adopt them as long as real and perceived security problems are not addressed. The remaining part of this chapter covers the security issues of the NFC technology. Security is considered to be one of the most important requirements for m-payments to be adopted by the major stakeholders and is currently an inhibitor of the adoption of m-payments.

According to a survey done by Lu et al (2011) the barrier in the acceptance of m-payments is the initial lack of trust that the customers have towards the m-payment application; the customers are initially worried about “security and transaction risks involved in making a payment” (Lu et al., 2011). Security also includes reliability, consumer protection, privacy, anonymity and trustworthiness (van der Heijden, 2002).

Because of the level of penetration that has been achieved by mobile devices; the privacy and security of mobile communication has become very important. For any transaction that involves sharing of personal information such as payments, both privacy and security play crucial roles (Liebenau, Elaluf-calderwood, Karrberg, & Hosein, 2011). Privacy is ensured by security. Developers of m-payment application have to ensure that the security they put in place guarantees the privacy of sensitive data that will be used during any payment transaction. Even though the range of communication is limited to about 10cm for NFC; an attacker can retrieve usable signals to distances of up to 10m for active devices and 1m for passive devices (Haselsteiner & Breitfuß, 2006). There are four major objectives that needs to be addressed when dealing with security: confidentiality, data integrity, authentication and non-repudiation (Shon & Swatman, 1998). The next section looks at the security issues in more details.

4.5.1 Security Threats

OBJ2 is fulfilled in this section. This section covers the threats that can be encountered when using NFC enabled m-payments. These threats are not unique to NFC only but affect most of the technologies that involve wireless transfer of data. The section also covers the different methods that can be used to minimize the risk of these threats.

4.5.1.1 Eavesdropping

Eavesdropping affects all wireless communication interfaces including NFC. NFC enabled devices communicate with each other using radio frequency (RF) waves and an attacker can use an antenna to receive the transmitted signals (Haselsteiner & Breitfuß, 2006). The knowledge on how to extract transmitted data from RF waves can be obtained by doing a review of relevant literature. The equipment that is used to decode the RF signals is easy to obtain and it is also cheap. The distance that an attacker needs to be from the transmitted signal in order to carry out eavesdropping depends on many factors which include:

- The type of the antenna the attacker is using
- The quality of the signal that is received by the attacker
- quality of the transmitted signal
- the type of the decoder that will be used to decode the radio frequency send

The distance that the attacker needs to be from the transmitted signal can be roughly estimated to be 10m if the transmitting device is active and 1m if the transmitting device is passive (Haselsteiner & Breitfuß, 2006). This type of attack can be prevented by establishing a secure channel. For NFC enabled m-payments, making the mobile device operate in the passive mod reduces this attack.

4.5.1.2 Data Corruption

This is a type of a Denial of Service attack. The attacker listens and tries to modify transmitted data so that invalid data is received. The aim of the attack is to disturb communication (Haselsteiner & Breitfuß, 2006). The attacker achieves data corruption by transmitting valid frequencies of data spectrum at a correct time (Haselsteiner & Breitfuß, 2006). For this attack, the attacker needs to have an excellent understanding of modulation schemes and coding, and he/she also needs to know the coding scheme used to transmit the data. The attacker cannot manipulate the actual data but only the signal. The NFC device needs to check the RF field while transmitting data and this will enable the devices to detect the attack and thus prevent it.

4.5.1.3 Data Modification

In this type of attack, the attacker wants the receiving device to receive valid data that has been manipulated. The possibility of this attach occurring depends on the amplitude modulation strength that was applied (Allah, 2011). This is due to the fact that decoding of signal depends on the type of modulation used (either 10% or 100%). This attack is highly technical and we are not going into the finer details of how it occurs. What should be noted is that this kind of attack is feasible on all bits on the Manchester coding of 10% ASK and it is only feasible for certain bits and impossible for other for the modified Miller encoding with 100% (Haselsteiner & Breitfuß, 2006). This type of attack can be prevented through the following ways:

- The devices can communicate with each other in the active mode (both devices will be active) using 106k Baud. But this has the disadvantage that this kind of mode is very vulnerable to eavesdropping (Haselsteiner & Breitfuß, 2006). This does not provide 100% protection but it makes it extremely hard for the data to be manipulated.
- When a device is sending data is should continuously check for the presence of another transmitting signal. It should abort the transmission of the data as soon as it detects it (Haselsteiner & Breitfuß, 2006).
- The best solution will be to use a secure channel (Allah, 2011; Haselsteiner & Breitfuß, 2006).

4.5.1.4 Data Insertion

In this attack the attacker inserts valid data into the data exchange of the two communicating devices. The attacker has to send his/ her data before the valid receiver responds. If the attacker's data and the authentic receiver's data streams overlaps, the data will be corrupted. This attack can be prevented through any one of the following methods:

- By ensuring that the answering device responds with no delay (Allah, 2011; Haselsteiner & Breitfuß, 2006).
- The answering device can listen to the channel during the time it is open and can detect the originating point of the transmission (Allah, 2011; Haselsteiner & Breitfuß, 2006).
- Using a secure channel between the two devices.

4.5.1.5 Man-in-the-middle

This type of attack occurs when two parties that want to communicate are tricked to communicate through a third party which is the attacker without their knowledge. The attacker can eavesdrop on the conversation and manipulate any type of data that he/she wants to change (Allah, 2011; Haselsteiner & Breitfuß, 2006). This type of attack is not feasible for NFC enabled communication because one of the communicating parties will always detect the presence of a third party (Allah, 2011; Haselsteiner & Breitfuß, 2006).

4.5.1.6 Unwanted Activation

It is similar to eavesdropping (Jovanovic & Organero, 2011). In this case the attacker will try to activate the NFC technology on the mobile device and will then try to access NFC application on the mobile such as the payment application.

4.5.1.7 Denial of Service

“The attacker tries to interfere with the RF field, in order to prevent the transaction” (Jovanovic & Organero, 2011).

4.5.2 Information Security

The security issues to consider include the security of the payment application sensitive data, security of the operation of the payment application and security of the operation of the software platform. The evaluation of the security issues is based on the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4.

Table 6: Definitions of security objective (Linck et al., 2006)

Security Objective	Definition	Enabling concept/technique
Confidentiality	Ensure that transaction information cannot be accessed by unauthorized users	Encryption
Authentication	Ensures that the transaction information actually originates from the presumed transaction partner	Possession(e.g. mobile phone) Knowledge (e.g. of a PIN) Property (e.g. biometric property)
Integrity	Ensures that the transaction information remains intact during transmission and cannot be altered	Digital Signatures
Authorization	Property that the involved parties must be able to verify if everyone involved in a transaction is allowed to make the transaction	Digital Certificate
Non-repudiation	Property that no one should be able to claim that the transaction on his/her behalf was made without their knowledge	Digital Signatures

4.5.2.1 Confidentiality

Viehland and Leong identified confidentiality as a major security concern of users when it comes to m-payments in general (Viehland, Siu, & Leong, 2010). In an m-payment application we consider the confidentiality of all the message and information that are passed between the involved parties. The information that is sent or received by a device during a payment transaction must not be accessed by any unauthorized device, application or person .The messages sent must be encrypted and only the involved parties in the payment transaction must be able to retrieve plain text from these messages. Confidentiality is usually attacked by eavesdropping, traffic analysis and man-in-the middle. The confidentiality of NFC is not guaranteed because of eavesdropping. The data sent can be extracted by an attacker.

4.5.2.2 Data integrity

This includes the integrity of all the messages and transactions. This can be achieved by adding secure electronic signatures to all the messages (Eze, Gan, Ademu, & Tella, 2008). Integrity can be compromised by man-in-the middle, session hijacking and sometimes by replay attacks. In m-payment the purpose of integrity attack is to alter the messages being exchanged during a transaction. Service providers have to ensure that transactions are protected from integrity violations.

4.5.2.3 Authentication

Authentication is very important in payment transaction. Each transaction in an m-payment application must be authenticated. There are many different ways of performing authentication which includes using personal identification number (PIN) or using network based authentication protocols. The same way that Integrity is usually compromised is the same that authentication is compromised, that is through man-in-the middle, session hijacking and replay attacks.

4.5.2.4 Non-repudiation

“This ensures that a user cannot deny that they performed a transaction. The user is provided with a proof of the transactions and recipient is assured of the user’s identity” (Eze et al., 2008).

The non-repudiation of payment parties and objects in a transaction should be taken into account. This can be ensured by digital signatures.

4.5.3 NFC Security Standards

NFC also has a series of security standards called NFC-SEC (NFC security standards) which define “a protocol stack that enables application independent and state of the art encryption functions on the data link layer, on top of NFCIP-1” (Jovanovic & Organero, 2011). NFC-SEC standards can be deployed for all the NFCIP-1 connection which does not require application specific encryption mechanisms to protect the data from eavesdropping and data manipulation. It should be noted that application specific encryption can be used instead of NFC-SEC.

4.5.4 Secure Channel

Establishing a secure channel helps prevent any kind of data modification attack. A channel can be secured by using a standard key like Diffie-Hellmann based on RSA or Elliptic Curves which is shared between the devices. This standard key can then be used to obtain a symmetric key such as the Advanced Encryption Standard (AES). There are two types of services for providing a secure channel: Shared Secret Service (SSE) and Secure Channel Service (SCH). Figure 4-1 shows the steps that are followed by an application when using either SSE or SCH.

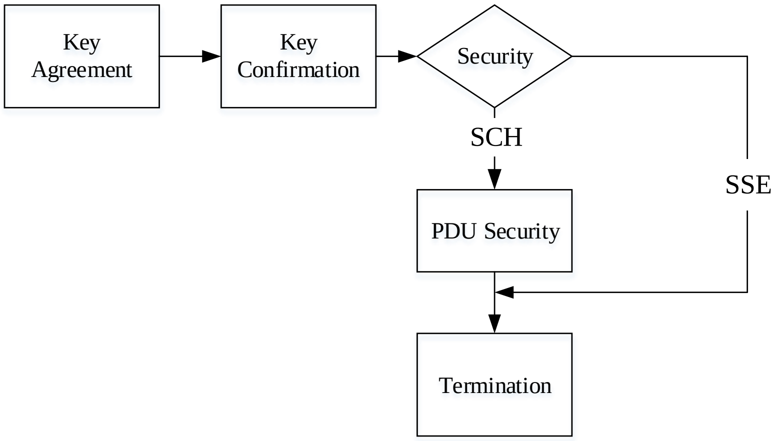


Figure 4-1: NFC-SEC Protocol Steps

The SSE only establishes the shared secret between the devices and the SCH “uses the shared secret established beforehand for a standardized secure channel service to protect all subsequent communication in either direction according to the mechanisms specified by the cryptography standard" (ECMA International, 2013a). The ECMA-386 standard outlines the cryptographic mechanisms that use the Elliptic Diffie-Hellman (ECDH) protocol for establishing the key agreement and the AES algorithm to encrypt data (ECMA International, 2010). A secure channel provides confidentiality, integrity, and authenticity of the transmitted data.

4.5.5 NFC Specific Key Agreement

An NFC specific key agreement does not require asymmetric cryptography and this reduces the computational requirements for the key (Allah, 2011; Haselsteiner & Breitfuß, 2006). This type of key provides an almost perfect security. Obtaining the key is achieved by first of all the two devices sending random data to each other at the same time until they synchronize on both the timing of bits and on the amplitude and RF signal phases. After they have synchronized, the devices will now be able to send data at the same time using the same amplitude and phases. When both devices send the same bit, an attacker who will be listening will know this and it will not help the devices to secure the channel. The devices will continue to send each other data and the only important information that is needed is when the devices send different bits at the same time. That is when one device sends a one and the other device sends a zero. When this happens the attacker will not be able to figure out which device send what. The two devices will then discard all bits where the devices sent the same value and collect all bits where the devices sent different values. The devices will then agree on an arbitrary long shared secret based on these collected bits. "Thus, the generation of a 128 bit shared secret would need approximately 256 bits to be transferred. At a baud rate of 106k Baud this takes about 2.4 ms, and is therefore fast enough for all applications" (Haselsteiner & Breitfuß, 2006). For the channel to be more secure, the synchronization needs to be perfect. The protocol is broken if the attacker can distinguish the data send by each device. The protocol is secure if the difference between the devices is significantly below the noise level received by the attacker (eavesdropper). The level of security depends on the signal quality at the receiver which in turn depends on many parameters such as distance of the eavesdropper.

4.5.6 Information security requirements for e-money in South Africa

After reviewing the literature on the security threats of the NFC technology we also reviewed the NPS position paper in order to find out if the NPS Act covers security issues involved in m-payments (South African Reserve Bank, 2009). In the NPS Act it is stated that both information and funds transfer must be protected from access by unauthorized users. The position paper also states that the technology enabling e-money services must be secure and the provider of the payment application must ensure that confidentiality, integrity, authenticity and non-repudiation are catered for. Also “security and operational services should meet the requirements of international standard bodies” (South African Reserve Bank, 2009). As mentioned in Chapter 3, the purpose of the NFC Forum is also to come up with standards for both interoperability and security; this means that NFC enabled m-payment application has also to adhere to those standards.

4.5.7 Summary for Threat and Security Issues

Perceived security of mobile payments by the user is very important for the m-payments to be widely adopted by the customers (Linck et al., 2006; Shin, 2009). Perceived security is defined as the degree to which a customer believes that using a particular mobile payment procedure will be secure (Shin, 2008). The trust and intentions by a customer to use mobile payment depends largely on the customer’s perception of the security and not on technological solutions (Shin, 2009). According to a report that was done by Smart Card Alliance in 2008, the data protection features and the security features are similar to that of contact cards (Smart Card Alliance, 2008). These features can also be implemented for the mobile device when it is emulating the contactless card. This section looked at various security issues and threats that may be encountered when using NFC technology and their solution. This purpose of this section was to fulfil objective OBJ2.

4.6 Conclusion

The strengths of NFC include ease of use, compatibility with RFID technology and ability to provide m-payments that are more secure than other forms of payments. The mobile device also adds to the strengths of NFC in that they can be wiped out remotely which provides more security to the m-payment. Since NFC is a new technology, it makes companies which provide applications and/or services that are enabled by it appear up to date and progressive. The weaknesses of NFC which include: lack of devices among consumers, risk of adoption since it is a new technology and limited data transfer rate of up to 424kps were also discussed. NFC technology also increases the cost of mobile devices. Lack of devices among the customers is not a big issue because the customers are always changing their devices and when it comes to m-payment the data exchange rate is not much of a problem because only small amount of data are exchanged. This chapter also discussed the opportunities of which include m-payments, peer to peer money transfer, ticketing, marketing and; loyalty and coupons. We only looked at opportunities that are related to m-payments as this research is focused on m-payments. Based on these opportunities and the strength of NFC, we concluded that NFC is a powerful technology which can bring gain in the m-payment sector. Like any technology, NFC also has some security issues and threats that need to be addresses when using the technology. From the discussion on the threats and security issues of NFC, we conclude that the threats and security issues can be minimized, mitigated or prevented.

In addition NFC technology is standards based and this ensures that its applications are interoperable. The NFC standards are internationally recognized. Because of this fact and also the fact that NFC technology is open, it makes it easy for it to be used globally. The NFC technology also defines a secure channel which can be used when transmitting data. NFC technology offers many benefits to both the stakeholders and customers but it is not going to be adopted overnight. There is still more that needs to be done in terms of research, educating consumers and marketing before its benefits are visible in South Africa. Through the literature that was reviewed in this chapter, we conclude that the threats and the weaknesses of NFC are outweighed by its strengths and opportunities.

5 NFC M-PAYMENT ECOSYSTEM AND THE SECURE ELEMENT

5.1 Introduction

This chapter looks at the NFC m-payment digital ecosystem and the secure element in detail. The NFC ecosystem is complex because it is made up of stakeholder from both financial services and telecommunications sector. A digital ecosystem is a distributed, adaptive, open socio-technical system with properties of self-organisation, scalability and sustainability inspired from natural ecosystems. The first section looks at the ecosystem for NFC m-payments and the major stakeholder of the ecosystem. The second section will look at the Secure Element (SE). A SE is an encrypted chip that can be used to store payment applications, credentials and financial data. The business model that is used to in a payment application depends on either the stakeholder who is offering the m-payment application or the stakeholder who owns the secure element where the application will be residing. This chapter seeks to fulfil objective 8.

5.2 NFC Technology Mobile Payment Ecosystem

Moore (1996) defined the ecosystem as “an economic community supported by a foundation of interacting organizations and individuals – the organisms of the business world” (Moore, 1996). In the context of m-payments the organisms are the stakeholders. For m-payments, the ecosystem is managed by many different stakeholders that take part in m-payments products and services. The m-payment ecosystem is affected by both the supply and the demand side.

The NFC ecosystem is part of the problem space of NFC research (Ozdenizci et al., 2010). The debate about who will build and deploy the infrastructure for mobile commerce has been going on for some time now (Smart Card Alliance Contactless Payments Council, 2007). Some researchers believe that the MNO will be a better option for taking on the payment process (Global Platform, 2009), while others believe that the Financial Institutions (FI) should deploy readers, software and the necessary technology needed in m-payment and handle the payments applications (Jovanovic & Organero, 2011; Mobey Forum, 2011b; Ok, Coskun, Ozdenizci, & Aydin, 2011). There are others who believe that third parties which will develop and deploy payment applications would be a better option. This debate has also slowed the adoption of NFC technology in mobile payment (Ergeerts et al., 2012) but this did not prevent some of the stakeholders involved in the NFC ecosystem from negotiating and coming up with a compromise especially in Japan and South Korea (Ezell, 2009).

One of the things that have been hindering the wide scale implementation of NFC payment application is the lack of a standard and unambiguous ecosystem that can support the long-term evolution of this market while addressing the individual needs of the wide range of stakeholders (Mobile Financial Services, 2011). The success of NFC payments application lies mainly in recognizing and understanding the structure of the overall ecosystem of the technology and on the degree of collaboration among the stakeholders in the ecosystem. A survey done by Ozdenizci et al in 2010 showed that little was done on the NFC ecosystem and that it was an area that was still open to research - this is true even today. The relationships between the stakeholders are not clearly defined and are also unstable.

Figure 5-1 shows some of the stakeholders that can be involved in an NFC payment application. A stakeholder implementing a payment application does not need to include all the other stakeholders but collaboration among the stakeholders brings about interoperability of m-payment application. The MNOs and the FIs dominate the mobile payment ecosystem.

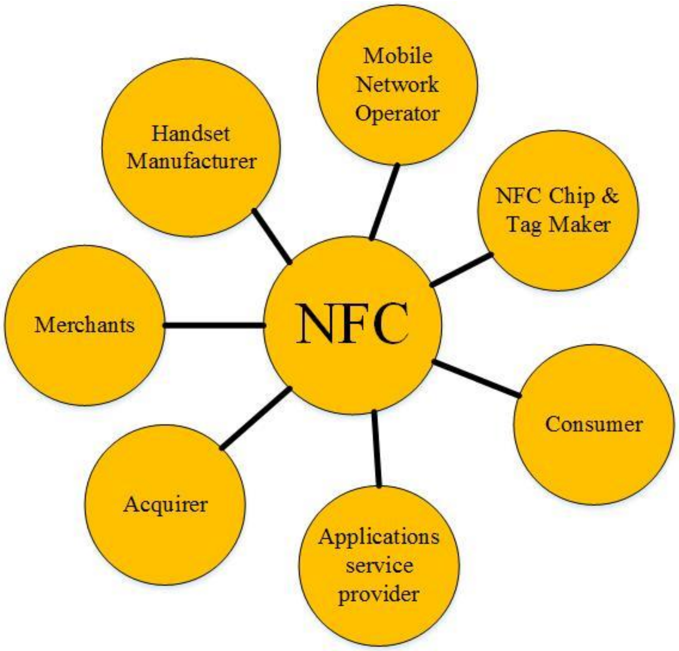


Figure 5-1: NFC Ecosystem (Patel & Kothari, 2013)

5.2.1 Major Stakeholders

This section gives brief discussions on the major stakeholders of the NFC ecosystem.

5.2.1.1 Mobile Network Operators

The most influential stakeholders in m-payments are the MNO because they are the ones that provide GSM (Global System for Mobile Communication) and GPRS (General Packet Radio Service) services needed for data traffic. Currently the MNO are pushing for their SIM card to be used as a secure element. If they succeed the mobile purchases will likely be charged directly to the mobile number in the same way that mobile data and calls are charged (Jovanovic & Organero, 2011). One of the ways that the MNO can attract consumers to use m-payments is to offer consumers NFC enabled devices. MNOs can develop their own m-payment applications and currently they are using strategic ideas in adopting mobile payments in their aim to retain their current customers and also gain new customers. Vodafone and Safaricom gained 2.37 million subscribers over a period of one year after launching M-PESA in Kenya in 2007 (Jenkins, 2008).

M-payments also develop a new source of revenue for the MNO. MNOs have an advantage over the other stakeholders because their SIM can be used as a secure element to store the payment application and sensitive data. According to Smart Card Alliance (2007); MNOs face a high churn rate. One of the ways the MNO can reduce this rate is through the introduction of more appealing application such as payments applications. The MNO can provide the consumer with a virtual account or they can partner with the existing financial institutions. Another advantage that the MNOs have over the other stakeholder in providing an NFC m-payment application is that they already have the trust of customers and customer service structures (Jenkins, 2008). In offering an m-payment application the MNOs can also reduce airtime distribution costs. According to Jenkins (2008) the MNO can play the following roles in the NFC ecosystem:

- Provide infrastructure and communications service
- Provide Agent oversight and quality control
- Issue e-money (where commercially desirable and permitted by law)
- Exercise leadership in drawing m-money ecosystem together

- Advise other businesses (e.g. banks, insurers, utilities) on their m-money strategies

5.2.1.2 Financial Institutions (FIs)

FIs include banks and card networks. FIs have the advantage of already owning a secure payment infrastructure and they already have a large consumer base. Consumers are loyal and trust the banks they bank with (Barbuta, Dobrean, Gaza, Mihaila, & Screpnic, 2012). FIs can add contactless m-payment by leveraging the contactless infrastructure currently being used (Smart Card Alliance, 2007). M–payments are more convenient than cards and they can enhance customer loyalty. This will help the FIs to "penetrate cash and check-heavy merchants segments and open new acceptance channels" (Smart Card Alliance, 2007). FIs would like to control m-payments by offering it to all their customers without regard to the MNO that the customers use (Deloitte, 2011). FIs have limited networks compared to MNOs but they have the "ability to facilitate foreign exchange, clearing and settlement" (Jenkins, 2008). M-payments help banks reduce costs of delivering services to customers and can enable them to reach new customer segments and new geographical areas (Jenkins, 2008). The FIs can play the following roles (Jenkins, 2008):

- Offer banking services via mobile
- Hold float or accounts in customers' names
- Handle cross-border transactions, manage foreign exchange risk
- Ensure compliance with financial sector regulation

5.2.1.3 Consumers

Consumers are the key stakeholders for the acceptance of any m-payment application. M-payments have to meet the needs of the customers. With m-payments; consumers will not need to carry cash. M-payments offer convenience of remote payment, remittance and other financial services. M-payments can greatly benefit the unbanked and the underbanked. The customers are increasingly using mobile phones to improve their lives and m-payments are a big step in achieving that. Most customers have limited financial literacy and lack awareness of m-payments (Jenkins, 2008). Therefore more needs to be done in terms of marketing and educating consumers about the benefits of m-payments. The consumers determine the adoption of m-payments.

5.2.1.4 Merchants

Merchants play a significant role in the successful deployment of m-payments. The larger the number of merchants involved the greater the number of positive externalities generated. Merchants benefit from NFC enabled m-payments because they offer faster payments transactions and improved convenience to consumers. M-payments reduce cash handling for merchants. Since m-payments are perceived as fast, they can reduce queues at peak times (Jenkins, 2008). Merchants have limited ability to partner with large corporations, and they also lack the trust of customers with regards to providing m-payment systems (Jenkins, 2008). According to Jenkins the merchants can play the following roles:

- Perform cash-in and cash-out functions
- Handle account opening procedures, including customer due diligence (where commercially desirable and permitted by law)
- Report suspicious transactions
- Identify potential new m-money applications

5.2.1.5 Trusted Service Manager

The TSM is an independent trusted party acting on behalf of the SE issuer and/or the Mobile Contactless Payment Application Service Provider which facilitates the provisioning and secure life cycle management of mobile contactless services. The primary role of the TSM in the NFC ecosystem is to facilitate management of the NFC payment application stored on the Secure Element (Smart Card Alliance, 2011). According to the Global Platform (2009) the TSMs enables the link between the Service Providers (for example, banks and retailers) and the MNO by providing the technical capability. The TSM provides the following services:

- Integration of the accounts of the issuing entities
- Integration of technology
- Hosting of the payment system
- Operation of the payment ecosystem

- Management of the relationships of the stakeholders in the ecosystem

5.2.1.6 Mobile Handset Manufactures

Innovative mobile applications attract new customers and create new business partnerships for handset manufactures (Smart Card Alliance, 2007). Mobile handset manufacturers offering mobile phones that support mobile payment applications such as NFC enabled phones have a competitive advantage over those who do not offer such mobile devices. The mobile handset manufacturers can enhance the security of NFC m-payments by creating devices that offer more security such as through the use biometrics authentication. They can provide budget phones that can used to attract consumers when an m-payment is being launched.

5.2.1.7 Acquirer

An acquirer is a payment service provider enabling the processing of merchants' transactions with the issuer through an authorization and clearing network. The Acquirer may also facilitate with the placement of terminals at retail locations (Smart Card Alliance, 2011).

5.2.1.8 Payment Network

The payment network facilitates the authorization processing of payments and the settlement of bank card transaction and they also support contactless messaging and authentication functions (Smart Card Alliance, 2011).

5.2.2 Stakeholders Requirements

A white paper produced by Smart Card Alliance Payments Council in 2011 expressed the requirements of the stakeholders in seven attribute categories:

- Reliability at POS
- Security
- Ease-of-use and convenience
- Wallet Functionality
- Acceptance
- Device deployment/availability

- Value-add applications

5.2.3 Existing Business Models

The major stakeholders of the NFC ecosystem are the banks and MNOs. Many researchers have come up with different business models based on the major stakeholders. Generally there are only four types of business models that can be adopted by the stakeholders. Figure 5-2 shows the four business models.

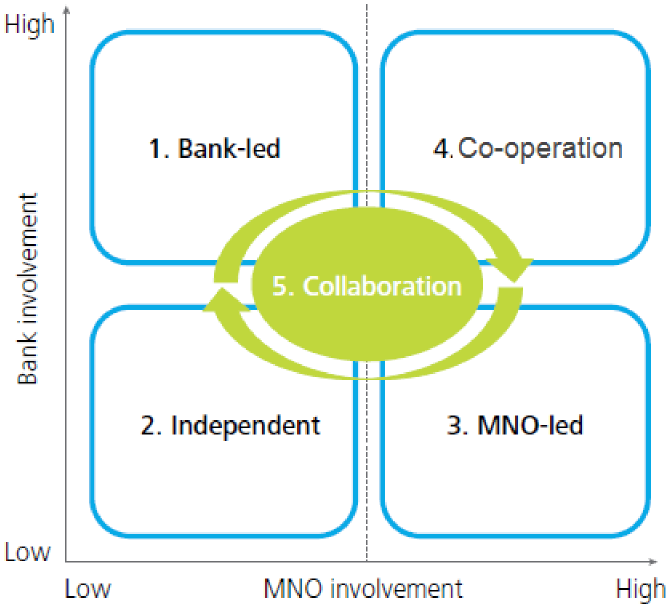


Figure 5-2: Potential NFC Ecosystem (Deloitte, 2011)

5.2.3.1 Bank-led

In this model at least one bank will be in control of the m-payment application and is responsible for launching the payment application. The partnership with the MNO depends on the requirements of the bank.

5.2.3.2 Independent

This model is led by a TSM such as trusted third party. The trusted third party will develop and manage the payment application. Its partnership with the banks and the MNOs will depend on its terms and conditions. The third party might use the already existing banking accounts or offer their own accounts. “One of the largest risks inherent with the Independent model is gaining both consumer and merchant adoption" (Deloitte, 2011). The customers and the merchants might not trust the TSM or trusted third party - this might cause them to reject the payment application.

5.2.3.3 MNO-led

MNO- led model has an advantage over the other models because most of MNOs already offer P2P money transfer and have a large customer base (MTN Mobile Money and M-PESA). MNOs have penetrated most remote parts of the world and offer network facilities in areas where there are no banking services (Adkins, 2013; Aker & Mbiti, 2010; Ondiege, 2010). This will make the m-payment accessible to everyone within their network coverage.

5.2.3.4 Co-operation

Financial Institutions and the MNOs enter into a partnership. The advantage of this model over the others is that it is interoperable. This model will benefit the customers of both the FIs and the MNOs. Currently this is the only way that the MNOs in South Africa can offer mobile banking because the only FIs are allowed to issues electronic money (South African Reserve Bank, 2009).

5.2.4 Discussion

The NFC technology offers new revenue generating services to the major stakeholders of the ecosystem (Innovision Research & Technology, 2007). For NFC m-payment to be successful each stakeholder should clearly understand its role. The complexity of the NFC ecosystem is impacting the global adoption of technology in mobile phones which is in turn is causing a low market penetration of NFC enabled m-payments (Ergeerts et al., 2012). This is also affecting the adoption of NFC enabled m-payments by both consumers and merchants. For NFC enabled m-payments to succeed, there is need for the stakeholders to collaborate. "The challenge the United States and many other nations are facing is the problem that all actors in the mobile payments ecosystem are pursuing their own interests and concentrating on maximizing their own return, thus making it more difficult for a true infrastructure platform to emerge" (Ezell, 2009). Even if the stakeholders do not collaborate, they still need to come to some agreement especially on the standards of the m-payment in order to ensure interoperability of the payment applications.

5.3 Secure Element (SE)

A payment application needs to be securely stored because it contains sensitive data. Coskun et al (2013) defined the SE as "a combination of hardware, software, interfaces, and protocols embedded in a mobile handset that enables secure storage and processing" (Coskun, Ok, & Ozdenizci, 2013). Figure 5-3 shows the three possible location of the SE on a mobile phone.

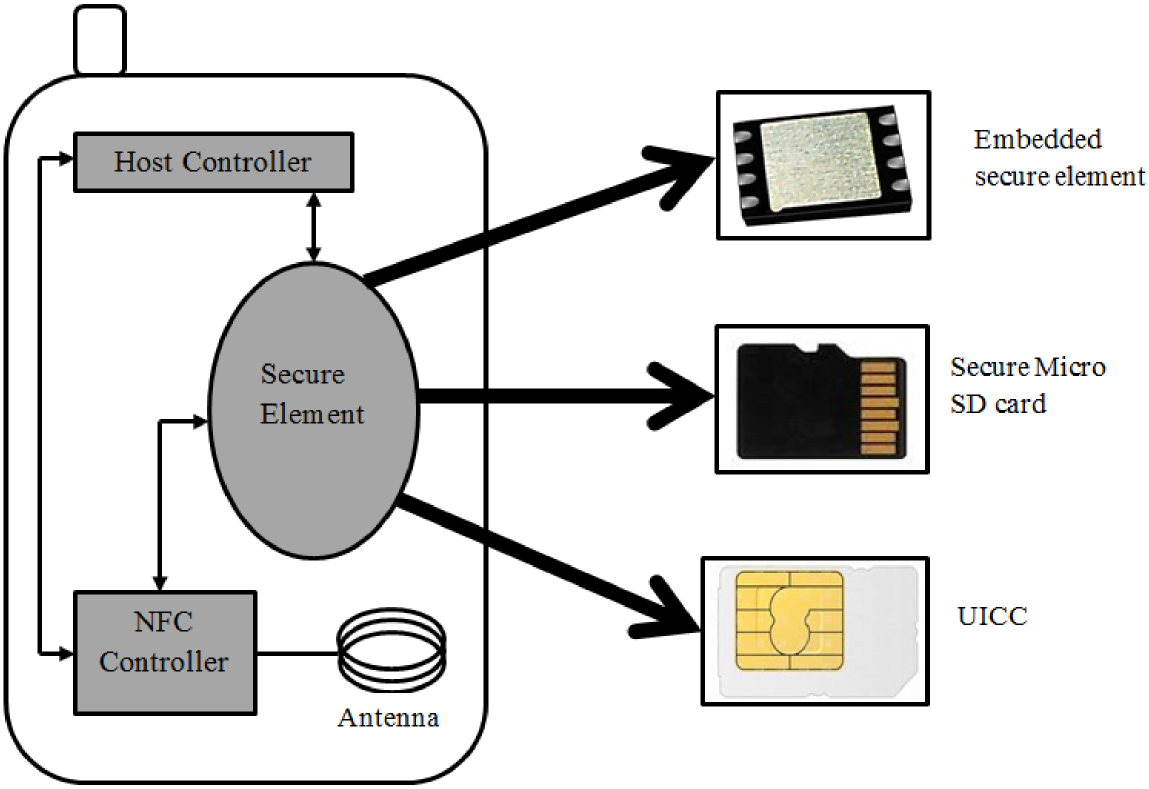


Figure 5-3: Possible SE locations

The SE ensures that all communication from outside is processed in encrypted form. The information stored in the SE can be accessed only by certain applications under certain conditions. The SE is separate from the NFC technology. The SE uses the NFC interface to transmit the encrypted data.

5.3.1 SE Alternatives

Figure 5-3 shows the basic locations of the SE that are commonly used but there are other alternatives such as stickers which can be used as SEs. According to Coskun et al (2013), the SE can be categorized into four groups: Nonremovable SEs, Removable SEs, Flexible SE solutions and Software-based SEs. The nonremovable SEs are the ones that are embedded in the mobile device. The removable SEs includes UICC, stickers and Secure Memory Cards (SMC). The Flexible SE solutions include SMC and UICC/SIM. And the Software-Based SEs are located at Trusted third party base.

Besides the issue of the ecosystem another big issue which is affecting the adoption of NFC is the issue of who will control the SE (Ergeerts et al., 2012). Even though there are three possible SE locations on the mobile phone; there are four possibilities of managing the SE (Ergeerts et al., 2012): handset manufacturer centric approach, MNO centric approach, service provider centric approach and neutral third party.

5.3.1.1 Handset manufacturer centric approach

The SE is embedded in the mobile device by the handset manufacture. In this case; it is the handset manufacturer who manages the SE. This option does not support the portability requirement because the SE is not removable. The SE which is integrated in the mobile device is tamper proofed and does not depend on OS of the handset (Madlmayr, 2008). The SE is connected to the NFC controller. Examples of mobile phones equipped the SE include Samsung Galaxy Nexus and the Google Nexus S. These SEs are owned by Samsung and Google respectively. This type of SE has all the hardware and software certifications it needs. This architecture has already been tested around the world and has been found to be secure (Smart Card Alliance, 2007). The type of SE used here needs to be replaced and personalized each the mobile device is owned by a different user (Coskun et al., 2013).

5.3.1.2 MNO centric approach

The SE resides in the Universal Integrated Circuit Card (UICC) also known as the SIM card. This approach meets the portability requirement of m-payments. MNOs in most countries that have huge numbers of the unbanked and underbanked already provide money transfer services therefore they can easily add a payment service. The SIM card is issued by the MNO and contains a SIM applet that allows secure authentication on the mobile network (Ergeerts et al., 2012). This option gives too much control to a single stakeholder (Ghag & Hedge, 2012). One of the benefits of this option is that it “meets the security standards imposed by the Financial Institutions” (Ghag & Hedge, 2012).The application on the SIM card can be easily blocked and unblocked. If the UICC is used as the SE, end-to-end processes need to be in place to prevent the new applications from damaging or corrupting the UICC (GSMA, 2011). A question arises as to who maintains control and visibility of credit or debit cards from separate banks if there are multiple payment application on the SIM card.

5.3.1.3 Service provider centric approach

According to Benyo (2009) a Service Provider can be simply defined as an actor that deploys or manages the application or data stored on the SE. In this approach the SE is located on an external memory such as a Micro SD card or an active sticker (Benyo, 2009). In this case the SE is controlled by a TSM. TSM such as Visa and MasterCard are already powerful in the payment industry and they already have a large number of customers (Ergeerts et al., 2012). The Micro SD should be NFC enabled. This option allows banks or financial institution to own the secure element (Ghag & Hedge, 2012). The Micro SD card is compatible with different models of mobile phones.

5.3.1.4 Neutral third party

In this case an independent third party manages the SE. The SE will be located in the Micro SD as well for this option. The third party provide the application and acts as a middle man between the banks and the MNOs. This option provides interoperability.

5.3.2 Summary

The SE affects the m-payment because if affects the business model that is adopted. An NFC enabled m-payment cannot be provided without a SE for the storage of the sensitive information. The business model is also affected by the dominating stakeholders and, the standards and laws of the area where the m-payment will be used. For the use of the SIM card and the mobile device embedded SE, there is need for the stakeholders to collaborate. The MNO centric approach, service provider centric approach and neutral third party provide interoperability but the MNO centric approach will only be limited to the subscribers of the MNO. This research also seeks to propose a business model that is sustainable in MRA. Chapter 10 will look at this business model in more details.

5.4 Conclusion

Contactless m-payments are successful in countries like Japan and South Korea due to the collaboration of the major stakeholders (Ezell, 2009). Because of the complexity of the NFC ecosystem the governments of these countries had to assist in the collaboration. The collaboration of the stakeholders affects the business model that will be adopted and the interoperability of the m-payment applications offered by different stakeholders. Even though there are many m-payments applications that have been deployed in Japan, they lack interoperability and this has caused the retailer merchants to have up to four POS reader terminals (Ezell, 2009). This might cause the merchants to reject m-payments because this will increase the transaction time. Therefore it is very important that the stakeholders collaborate even if they will not provide a single m-payment application. This will ensure interoperability of the m-payments.

The type of business model that is adopted in an m-payment can also be affected by the location of the SE. An NFC enabled m-payment cannot be provided without a SE. Since customers are always changing their mobile devices, it is a good idea use a removable SE if possible. Using the UICC as a SE provides more security because the UICC can be remotely wiped if the device is stolen.

6 THEORETICAL MODELS FOR TECHNOLOGY ACCEPTANCE

6.1 Introduction

Over the past years different theoretical models have been developed for measuring the acceptance of a new technology by users. In this chapter we will look at the most popular of these models and modify it for use in this research.

6.2 Literature Review for Theoretical Models for Technology Acceptance

There many different theoretical models which analyse the relationship between user attitudes, perception, beliefs and the use of the system. These theories include the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB), the Technology Acceptance Model (TAM) and the diffusion of innovation theory (Amoako-Gyampah & Salam, 2004). Of all the theoretical models the TAM and the diffusion of innovation theory are the most popular among researchers and these are the only theories that were considered for use in this research. The following sections give a brief discussion of these theories.

6.2.1 The Diffusion of Innovation Theory

This theory was invented by Rogers and its details are found in his book "Diffusion of Innovation" which was published in 1962. He defined adoption as a "decision of full use of an innovation as the best course of action available". Rogers (2003) used the words technology and innovations interchangeably (Rogers, 2003). He defined technology as a "design for instrumental action that reduces the uncertainty in the cause-effect relationship involved in achieving a desired outcome". He identified four elements that are important in the theory: innovation, communication channels, time and social system.

6.2.1.1 Four Main Elements of the Diffusion of Innovations

- Innovation - “An innovation is an idea, practice, or project that is perceived as new by an individual or other unit of adoption” (Rogers 2003). An innovation can either be new or can be perceived as new by some people (Sahin, 2006). Sahin (2006) identified uncertainty as a major obstacle of the adoption of innovations and he suggested that this can be overcome by informing the consumers about the advantages and disadvantages of the innovation.
- Communication Channels - Rogers (2003) defined communication as a “process in which participants create and share information with one another in order to reach a mutual understanding”. This communication occurs through channels between sources. “A source is an individual or an institution that originates a message. A channel is the means by which a message gets from the source to the receiver” (Rogers, 2003). Communication is made up of 3 elements: an innovation, two individuals or other units of adoption, and a communication channel. Communication channels can either be mass media and interpersonal communication. Examples of mass media include TV; radio, or newspaper and interpersonal channels consist of a two-way communication between two or more individuals (Sahin, 2006). Diffusion involves interpersonal communication relationships (Rogers, 2003).This makes interpersonal channels more powerful to create or change consumers’ decisions (Sahin 2006).
- Time - Rogers (2003) argues that time is a very important part of diffusion research and it helps to illustrate the strength of the diffusion research.
- Social System – “Social system is a set of interrelated units engaged in joint problem solving to accomplish a common goal” (Rogers, 2003). “Since diffusion of innovations takes place in the social system, it is influenced by the structure of the social system” (Sahin 2006). The individuals’ innovativeness is affected by the nature of the social system (Rogers 2003).

6.2.1.2 The Innovation-decision Making

“Innovation-decision process is an information-seeking and information-processing activity, where an individual is motivated to reduce uncertainty about the advantages and disadvantages of an innovation" (Rogers 2003). Figure 6-1 show the five steps that are involved in the innovation-decision process. Sahin concluded that these stages follow one another in a timed manner. Rejection of an innovation is possible at every stage of the innovation-decision process.

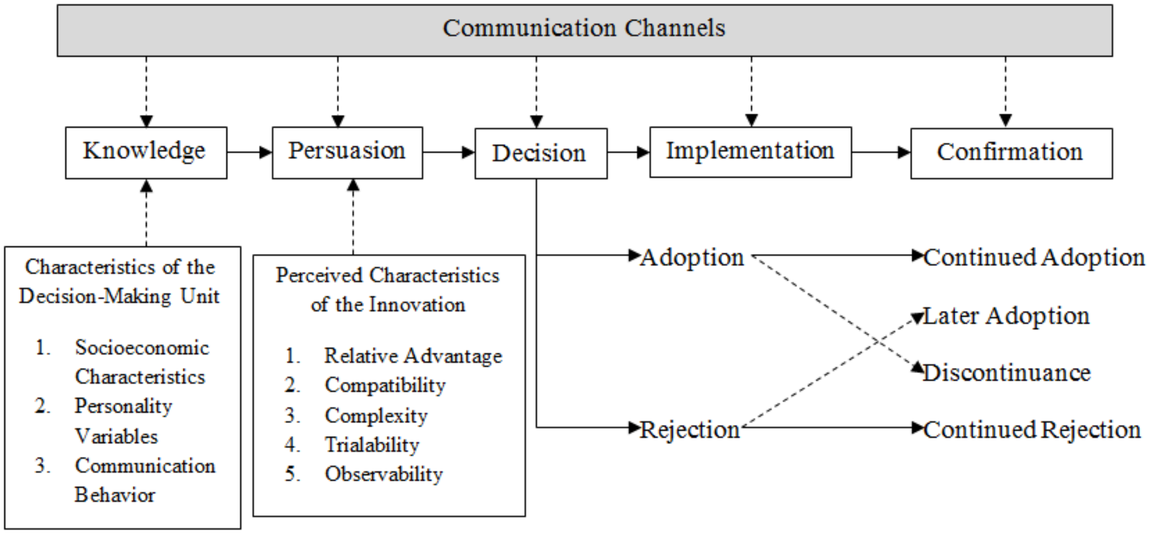


Figure 6-1: A Model of Five Stages in the Innovation-Decision Process (Rogers 2003)

6.2.1.2.1 The Knowledge Stage

This is the first stage of innovation-decision process. In this stage an individual obtains information about the existence of an innovation and attempts to gain more information about the innovation (Sahin, 2006). This stage seeks to answer the question, "What", "How" and "Why". From these questions Rogers derived three types of knowledge:

- Awareness-knowledge – It represents the knowledge of the existence of the innovation. It can motivate an individual to learn more about the innovation and to adopt the innovation (Sahin, 2006). It can also motivate the individual to seek information about the other two types of knowledge (Sahin, 2006).
- How-to-knowledge – this gives the information on the correct use of the innovation. An individual must have sufficient knowledge of an innovation before trying to use it. This is very important knowledge especially for complex innovations. Lack of this knowledge can cause an individual to reject an innovation.

- Principles-knowledge – these are the principles that will inform the individual about the purpose of the innovation and how it works. An innovation adopted without this knowledge will suffer discontinuance in the later stage.

6.2.1.2.2 The Persuasion Stage

This stage comes after an individual has developed either a positive or negative attitude toward the innovation but this does not mean the individual adopts or rejects the innovation (Rogers 2003). Rogers (2003) states that the individual is sensitively involved at this stage and also that this stage is feeling-centred. The individual's perceptions of the innovation are affected by others.

6.2.1.2.3 The Decision Stage

This is the stage where an individual chooses to adopt or reject an innovation. According to Sahin (2006), an innovation that is on a trial basis is adopted quickly because the individuals would want to try it for themselves before they come to an adoption decision. Rogers (2003) categorized rejection into two categories: active rejection and passive rejection. Active rejection is when an individual tries out an innovation and then decides not to adopt it and passive rejection is when an individual rejects an innovation without even trying it out.

6.2.1.2.4 The Implementation Stage

This is the stage where an innovation is put into practice (Sahin 2006). There is still some degree of uncertainty at this stage. The implementer may have to reinvent the innovation to reduce the degree of uncertainty. Reinvention is "the degree to which an innovation is changed or modified by a user in the process of its adoption and implementation" (Rogers, 2003).

6.2.1.2.5 The Confirmation Stage

At this stage the individuals' seeks support for their decision. According to Rogers (2003), this decision can be reversed if the individual is "exposed to conflicting messages about the innovation". But usually the individual seeks messages that support his/her decision (Sahin, 2006). This is the stage where later adoption or discontinuance takes place depending on the support of the innovation.

6.2.1.3 Attributes of Innovations and Rate of Adoption

The attributes of innovation help to reduce uncertainty of an innovation and also help to predict the rate of adoption. Of all the attributes of innovation, relative advantage is strongest predictor of the rate of adoption (Rogers 2003). The innovation diffusion theory states that the following attributes affect the acceptance of a technology:

- Relative advantage - In case of m-payments, the relative advantages is the advantages that mobile payments have over all the other methods of payments.
- Compatibility -Compatibility in this case if the degree to which an m-payment application is perceived as consistent with the past experiences of the consumers, their needs and how to it will it in the lives of the consumers.
- Complexity - Rogers (2003) defined complexity as "the degree to which an innovation is perceived as relatively difficult to understand and use".
- Trialability - "Trialability is the degree to which an innovation may be experimented with on a limited basis" (Rogers 2003). Trialability allows the customers to use the m-payment application on a trial basis.
- Observability – this is the "degree to which the results of an innovation are visible to others" (Rogers 2003).
- Image - The perceived public image of the consumer due to the use of the innovation plays an important role when the consumer is deciding to use an innovation (Lu et al 2011).

Rogers concluded that any innovation that offers all these factors is likely to be adopted faster than an innovation that does not. Relative advantage and compatibility provides consistent explanation in determining consumer adoption of mobile and financial technologies (Lu et al., 2011). Perceived public image plays a significant role in the decision that is made by the consumer either to use a mobile payment application or not (Lu et al., 2011).

6.2.2 The TAM Theory

Davis proposed this theory after there had been many system failures in many organizations. According to Davis (1989), “system use is a response that can be explained or predicted by user motivation, which, in turn, is directly influenced by an external stimulus consisting of the actual system’s features and capabilities”. The TAM theory is used to test user acceptance of a technology. The TAM theory enhances the perception of user acceptance processes and also “the theoretical basis for a practical ‘user acceptance testing’ methodology” (Davis, 1986). According to Davis (1986) this theory provides a means for system developers to weigh out a proposed system before its installation. This prevents a system from failing. Figure 6-2 depicts the TAM.

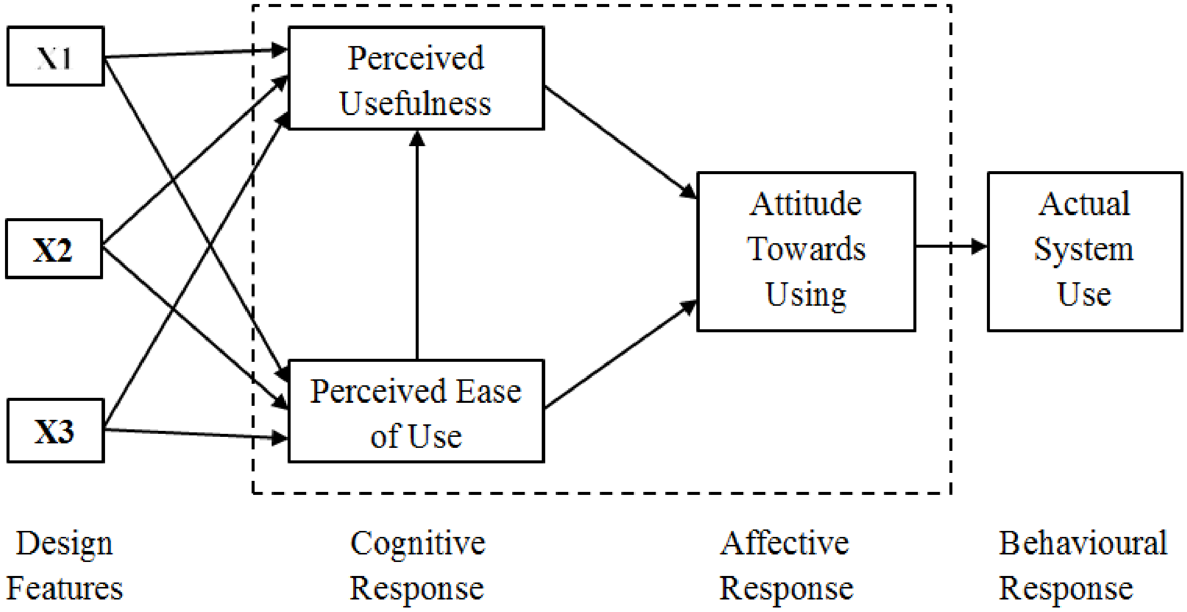


Figure 6-2: Technology Acceptance Model (Davis, 1986)

The TAM theory stipulates that whether or not the user uses a new system solely depends on the user’s attitude (Davis, 1989). According to Davis (1989) perceived usefulness and ease of use determine the use of a technology of a system. Davis (1989) defined perceived usefulness as “the degree to which an individual believes that using a particular system would enhance his or her job performances” and perceived ease of use as “the degree to which an individual believes that using a particular system would be free of mental and physical effort”. Perceived ease of use influences perceived usefulness.

The TAM concludes that the use of a technology is explained by three factors: attitude toward using the technology, perceived usefulness and perceived ease of use of the technology. Of the three, attitude toward using the technology is the major determinant of system use and it is also influenced by the other two. According to the TAM theory, perceived ease of use and perceived usefulness are directly influenced by the system design features.

6.2.3 Discussion

The TAM theory mainly focuses on the acceptance behaviour of technology by the users. The TAM theory is the most popular theory of all the technology acceptance theories that are available. This theory has been successfully used to predict the adoption of new technology over the years by different fields especially by the Information Systems community (Chuttur, 2009). According to Pavlou (2003) the TAM theory provides instruments that have excellent measurement properties, which are straight to the point and they are also empirically sound (Pavlou, 2003). The most relevant factors that consumers are concerned with are perceived ease of use, perceived usefulness and security (T Dahlberg, Mallat, & Öörni, 2003; N Mallat, 2004).

Due to the success of the TAM in measuring the acceptance of technology, we have decided to use this technology to measure the acceptance of NFC enabled mobile payments by people living in the MRA. We also included Trialability from the Diffusion of Innovation theory. User acceptance testing will include exposing the user to the prototype NFC payment application; this gives Trialability to our testing of user acceptance. This will enable us to measure the motives of the users to use the system. In addition to the already stated attributes of the model, relative advantage based on the Diffusion of Innovation theory and user satisfaction will also be evaluated. We also adopted the knowledge stage of the Diffusion of Innovation theory to introduce the NFC technology and the prototype application to the participants. We will mainly concentrate on measuring perceived usefulness and perceived ease of use of the users based on their experience after using the prototype. The measuring was done through the use of a questionnaire. The questionnaires are modified to suit the context of mobile payments. The remaining sections of this chapter will explain how all the considered factors will be measured.

6.2.4 Hypotheses

We will use the core hypotheses of the TAM and incorporate additional ones so that the model will be best suited for m-payments. Figure 6-3 shows the factors that will be used to measure the adoption of NFC m-payment in this research together with their associated hypotheses. In statistical analysis, these factors are known as latent variables. The measurements for each of these latent variables are given in APPENDIX A - Latent Variables Measurements. The remainder of this section discusses the hypotheses.

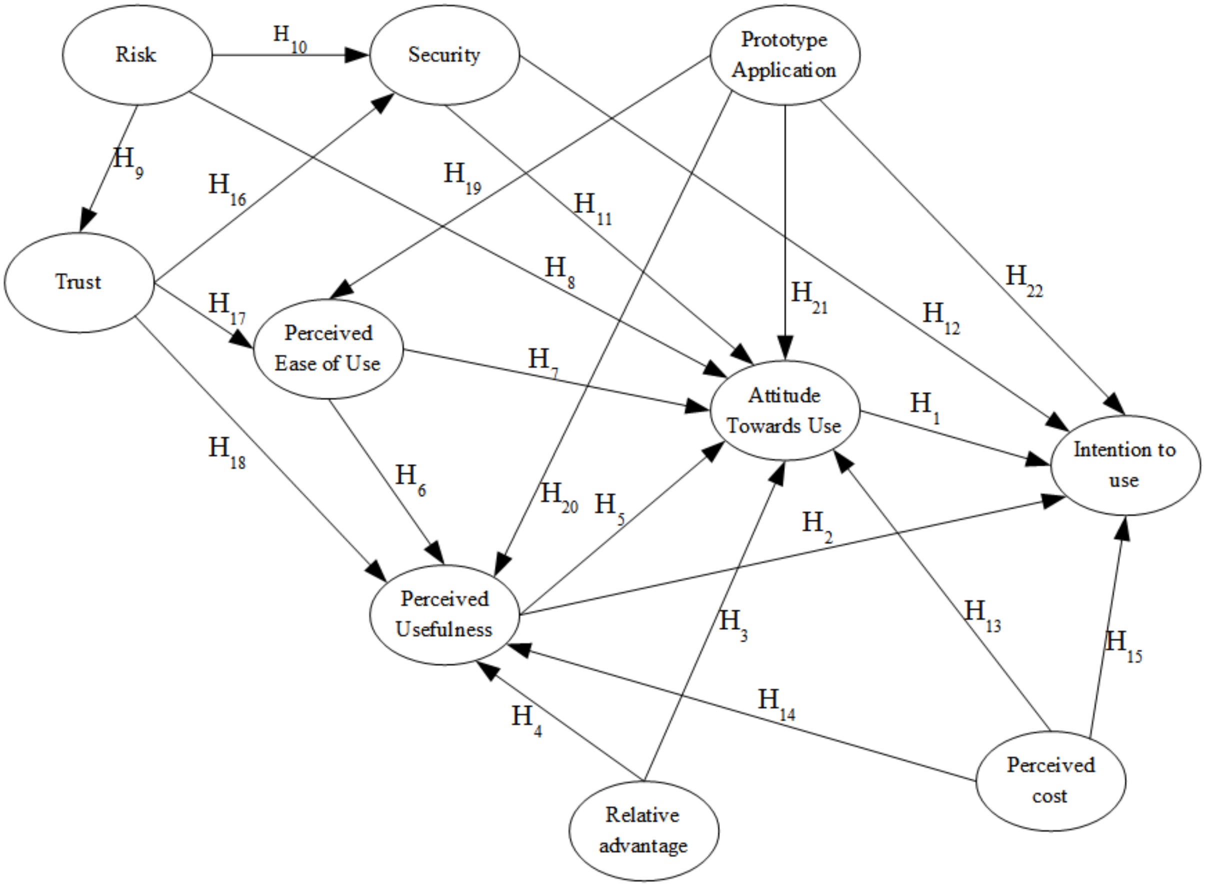


Figure 6-3: Consumer Acceptance Research Model

A person's *attitude towards using a technology* has influence on all the other variables that affect the user's *intention on using* the technology (Davis, 1989). From the TAM we can deduce that *attitude towards using* a technology has direct effect on *actual system use;* in this case *actual system use* is replaced by *intention to use* because there was no NFC enabled m-payment actual system available for use on the market and the decisions of the users would be based on the prototype application. This leads us to our first hypothesis:

H_1: *Attitude towards using* NFC enabled m-payments has direct effect on *intention to use* NFC enabled m-payments.

Consumers want to adopt a new technology if they know the *relative advantage* of the technology compared to the existing technology it is replacing (Rogers, 1995). The higher the *perceived usefulness* of the system is, the more likely the consumers will use the system. If *relative advantage* is high then *perceived usefulness* will also be high. This leads us to our next three hypotheses:

H_2: *Perceived usefulness* of NFC enabled m-payments has direct effect on *intention to use* NFC enabled m-payments.

H_3: *Relative advantage* of NFC enabled m-payments has direct effect on *attitude towards using* NFC enabled m-payments.

H_4: *Relative advantage* of NFC enabled m-payments has direct effect on *perceived usefulness* of using NFC enabled m-payments.

In the TAM theory, *perceived usefulness* directly affects *attitude towards using*, *perceived ease of use* directly affects *perceived usefulness* and *perceived ease of use* directly affects *attitude towards using*. This leads us to our next three hypotheses:

H_5: *Perceived usefulness* of NFC enabled m-payments has direct effect on *attitude towards using* NFC enabled m-payments.

H_6: *Perceived ease of use* of NFC enabled m-payments has direct effect on *perceived usefulness* of NFC enabled m-payments.

H_7: *Perceived ease of use* of NFC enabled m-payments has direct effect on *attitude towards using* NFC enabled m-payments

Lwin *et al* (2007) found that security risk is an area of major concern among the consumers when it comes to electronic services (Lwin, Wirtz, & Williams, 2007) . Consumers are usually concerned with security and privacy issues. This leads us to the issue of *perceived risks* of NFC enabled payments. *Perceived risk* of m-payments are increased by the fact that carrying out m-payments transaction is associated with high loss of personal data and transaction information (Bauer, Reichardt, Barnes, & Neumann, 2005). *Trust* and *perceived security* were also included on our research model as shown in Figure 6-3. In a similar manner like in the research carried out by Schierz *et al* (2010) we included *perceived risk* of using NFC enabled m-payments and this gives our next hypotheses (P G Schierz, Schilke, & Wirtz, 2010):

H_8: *Perceived risk* of using NFC enabled m-payments has direct effect on the *attitude towards use* of using NFC enabled m-payments.

H_9: *Perceived risk* of using NFC enabled m-payments has direct effect on trust on using NFC enabled m-payments.

H_{10}: *Perceived risk* of using NFC enabled m-payments has direct effect on the *perceived security* of using NFC enabled m-payments.

H_{11}: *Perceived Security* of using NFC enabled m-payments has direct effect on the *attitude towards* of using NFC enabled m-payments.

H_{12}: *Perceived Security* of using NFC enabled m-payments has direct effect on the *intention of use* of using NFC enabled m-payments.

Our first data collection showed that the people staying in Dwesa had very low income and most of them relied on government grants and money send from family members and friends staying in urban areas. This makes the issue of cost a major concern. Therefore *perceived cost* of NFC enabled m-payments will affect *attitude towards using* the m-payment.

H_{13}: *Perceived Cost* of using NFC enabled m-payments has direct effect on the *attitude towards* of using NFC enabled m-payments.

H_{14}: *Perceived Cost* of using NFC enabled m-payments has direct effect on the *perceived usefulness* of using NFC enabled m-payments.

H_{15}: *Perceived Cost* of using NFC enabled m-payments has direct effect on the *intention* of using NFC enabled m-payments.

Trust is a very important issue when it comes to any kind of payment. "*Trust* reflects a willingness to be in vulnerability based on the positive expectations towards another party's future behaviour" (Maroofi, Kahrarian, & Dehghani, 2013). According to Benamati et al (2013) *trust* is made up of three factors: ability, integrity and benevolence (Benamati, Fuller, Serva, & Baroudi, 2010). In this context ability simply means that the m-payment service providers possess enough knowledge and skill to provide the service, integrity means they are able to keep all their promises and benevolence means besides their own interest they will take consumers and merchants interest into consideration as well. Trust affects *perceived usefulness* of the m-payment application. Eze et al in 2008 came up with a conceptual model that is based on the TAM to measure user *trust* and adoption of m-payments (Eze et al., 2008). *Trust* affects *perceived ease of use*, *perceived usefulness* and *intention to use* (Eze et al., 2008). This leads us to the next three hypotheses

H_{16}: *Trust* on NFC enabled m-payments has direct effect on the *perceived security* of using NFC enabled m-payments.

H_{17}: *Trust* on NFC enabled m-payments has direct effect on the *perceived ease of use* of using NFC enabled m-payments.

H_{18}: *Trust* on NFC enabled m-payments has direct effect on the *perceived usefulness* of using NFC enabled m-payments.

The prototype will be used to introduce NFC enabled m-payments to the people in our research area. Their perception of NFC enabled payment application will be affected by the prototype. Hence the prototype application will have direct effect on both *perceived ease of use* and *perceived usefulness* and this gives us our last four hypotheses:

H_{19}: *Prototype application* has a direct effect on the *perceived ease of use* of using NFC enabled m-payments.

H_{20}: *Prototype application* has a direct effect on the *perceived usefulness* of using NFC enabled m-payments.

H_{21}: *Prototype application* has a direct effect on the *intention of use* of NFC enabled m-payments.

H_{22}: *Prototype application* has a direct effect on the *attitude towards use* of NFC enabled m-payments.

6.3 Conclusion

Through this research we also want to make our contribution in the field of the research of NFC enabled m-payments. In this research we were not proving that NFC enabled m-payments will be adopted but using scientific methods we investigated whether it will be adopted or not. The model that was developed is based on literature that has already been tested. This ensured the validity of our results for consumer adoption. In developing the model and the hypotheses various similar literatures was reviewed. Most of the measurement items were adopted from existing validated measurements that were developed by other researchers.

7 PROTOTYPE APPLICATION ANALYSIS, DESIGN AND IMPLEMENTATION

7.1 Introduction

User acceptance of a new technology can only be accurately and fully measured through a system that requires that actual practical use of the technology. This chapter details the analysis, design and implementation of a prototype NFC enabled m-payment application. A prototype is defined by Moggridge as “a representation of a design, made before the final solution exists” (Moggridge, 2007). Prototypes can be used to demonstrate and explore new technology and also to gain empathy (Buchenau & Suri, 2000). The prototype application was used to test user acceptance of NFC as an m-payment technology and the technology itself. The first section covers the analysis and the design of the application and the last section details the implementation of the prototype. The prototype consists of an m-payment service, a peer-to-peer money transfer service, and other standard banking services such as balance enquiry.

Figure 7-1 shows the flow diagram of the process that was followed during the prototyping. Prototyping is a process that developers follow when creating a prototype.

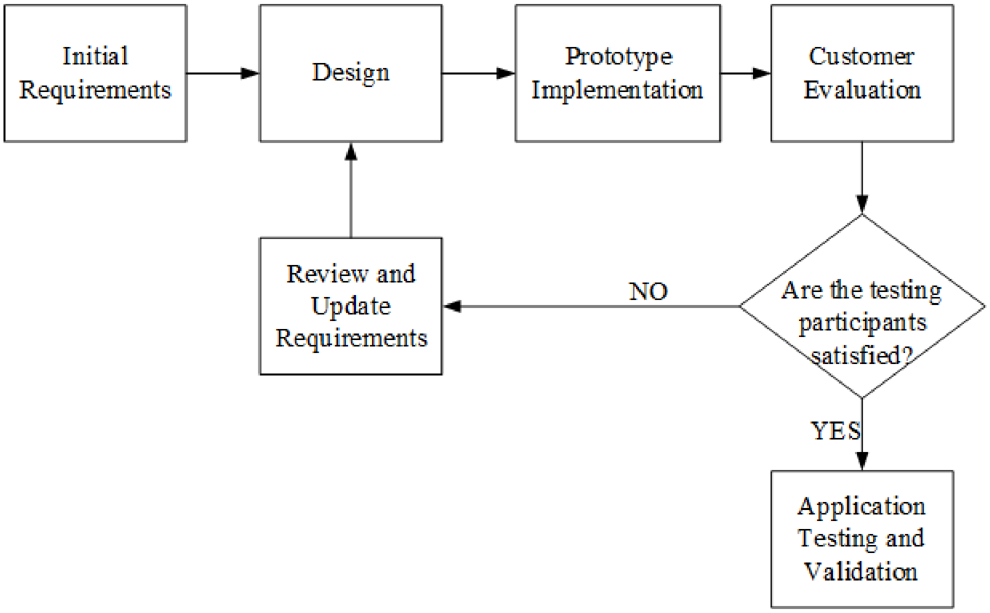

Initial Requirements
Design
Prototype Implementation
Customer Evaluation
Review and Update Requirements
NO
Are the testing participants satisfied?
YES
Application Testing and Validation

Figure 7-1: System Prototyping

Initial Requirements – these are the first requirements that we had. Since the interviews showed that most of our participants lacked knowledge of m-payments and NFC technology, we relied on literature review, m-payments enabled by other technologies and also on expert opinion for these requirements.

Design – the design of the prototype was based on the requirements that were available beginning of the design process. After each prototype was reviewed, additional requirements were integrated into the design.

Implementation – this stage involved implementing the system based on the available requirements and based on the design.

Participants Evaluation – this stage involved taking the application to the users to be tested. Additional requirements were collected from the users and the design and prototyping stages were repeated to in order to implement the new requirements.

Test – This was done after the implementation and usability testing. The prototype was developed to provide as close to full functionality of a complete application as possible so that the users would understand m-payments enabled by NFC technology as well as mobile payments in general.

7.2 Requirements and Design

This section is concerned with gathering requirements and analyzing them in order to come up with a practical design which can be implemented. This section provides answers to the questions on consumer requirements for an NFC enabled m-payment which are associated with objectives OBJ3a and OBJ3b.

Figure 7-2 shows the flowchart of our proposed-payment application. The flowchart only shows the services that are enabled by the NFC technology: money transfer service and the m-payment service.

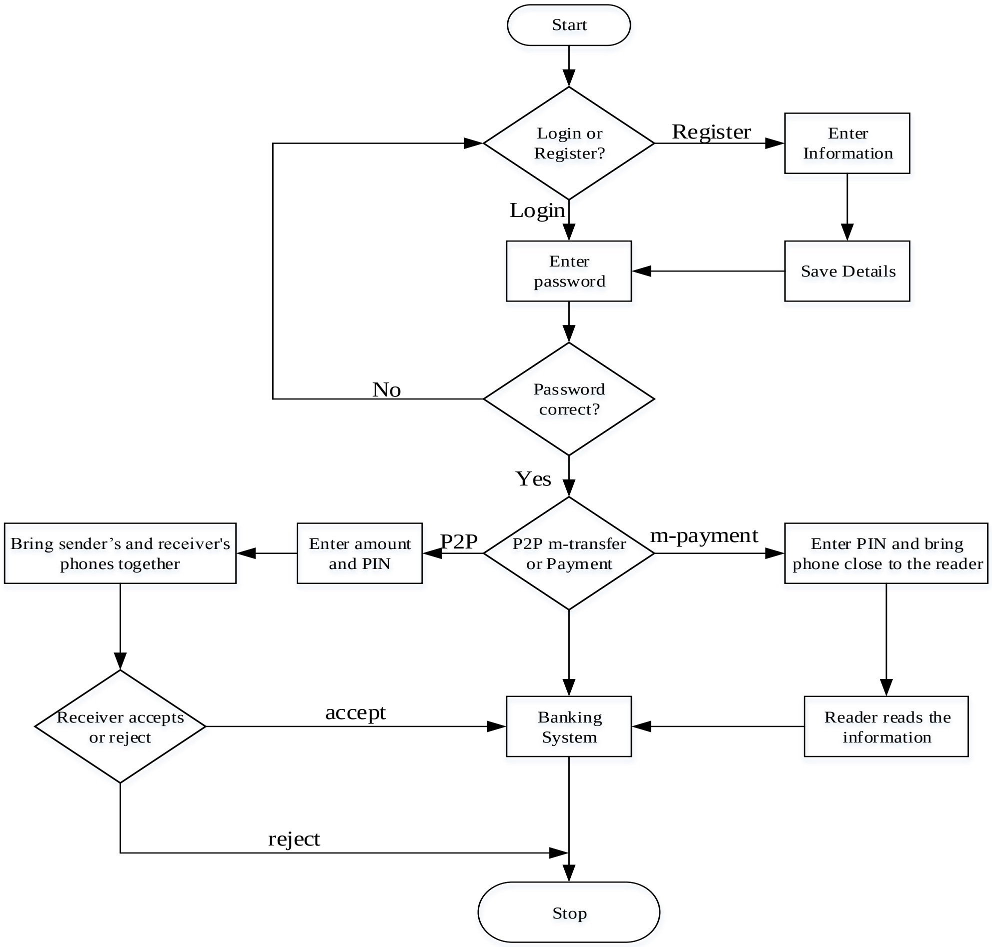

Start
Login or Register?
Register
Enter Information
Login
Enter password
Save Details
No
Password correct?
Yes
Bring sender's and receiver's phones together
Enter amount and PIN
P2P
P2P m-transfer or Payment
m-payment
Enter PIN and bring phone close to the reader
Receiver accepts or reject
accept
Banking System
Reader reads the information
reject
Stop

Figure 7-2: Flowchart of the prototype m-payment

7.2.1 Requirements

It is very important for the requirements of the application to be correctly and accurately collected so that the users will not reject the prototype because it lacked what they needed. The requirements were gathered by asking the users what they would expect to see in an m-payment application. Because the people in Dwesa had little knowledge about m-payments and NFC technology we did not base our requirements gathering on them only. We also had to undertake a detailed review of literature and analyze relevant documents on m-payments.

7.2.1.1 Requirements Elicitation

The requirements were collected through one-to-one interviews and focus groups. The interviews were unstructured to allow the participants to freely express themselves. During requirements elicitation the overall purpose and operation of m-payment systems was explained to the participants. The interviews that were conducted showed that the participants had very little knowledge about m-payments and how they work. After explaining m-payments and the NFC technology, the participants expressed their particular requirements which mostly pertained to the usability of the application.

7.2.1.2 Functional Requirements

The following are the key functional requirements that were also determined from the users:

- The application should authorize and authenticate users.
- The account number should be stored persistently on the device.
- The application should support account management services.

7.2.1.3 Non-Functional Requirements

The following are the non-functional requirements that were determined from the data gathering engagement with the users:

- The m-payment application should provide high levels of reliability.
- The m-payment application should be secure and provide end-to-end security.
- The m-payment application user interface should be easy to understand and should give sufficient feedback
- The system should efficient and the transactions should be fast. Since mobile devices have limited processing power the system should take up as little CPU memory as possible.
- The m-payment application should be easy to use. In this context this means:
    - The m-payment application should be made up of simple steps.
    - Each application service must take at most 4 steps.

- The m-payment application should be easy to learn to use, users who have used a mobile device before should be able to use the application without any tutorial on using it.

- The m-payment application should be fault tolerant.

7.2.2 System Design

This section describes the design of the payment application. Figure 7-3 shows the system architecture for the m-payment application. Since this was a prototype that was aimed at introducing NFC to the participants and at investigating the functionality of NFC, the system was made as simple as possible while at the same time taking great care not to compromise the functionality and security of the application. Three systems were developed: the backend banking system, the POS system and the Android application for the mobile devices. The banking system handles all the banking services. The Android application gives the user access to the banking system and the POS system was used when making an m-payment.

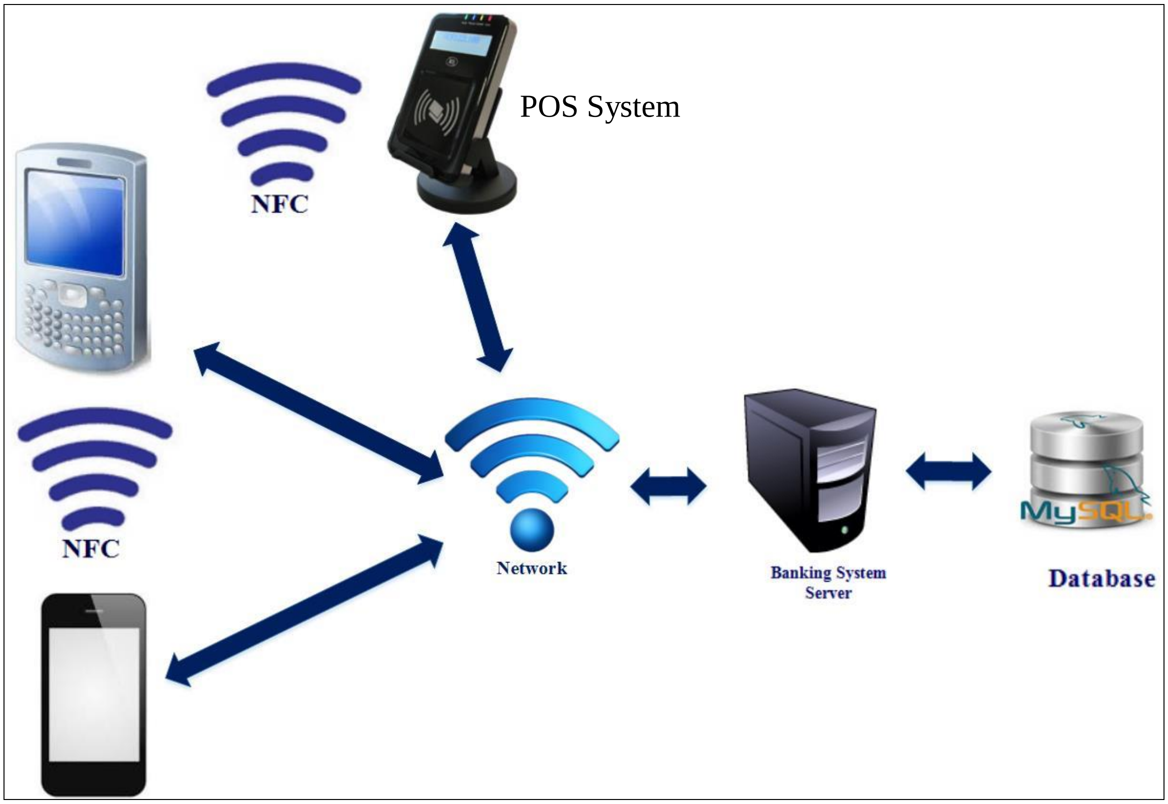


Figure 7-3: System Architecture

7.2.2.1 Use Cases

A use case defines an interaction between an actor and system that is initiated by the actor in order to achieve certain goals. In software development use case modelling enhances the description of requirements. The use case model is made up of the use case diagrams together with their description. The use case model represents an external view of the system. Figure 7-4 shows the use cases of the prototype payment application. In all the use cases the user will be interacting with the banking system.

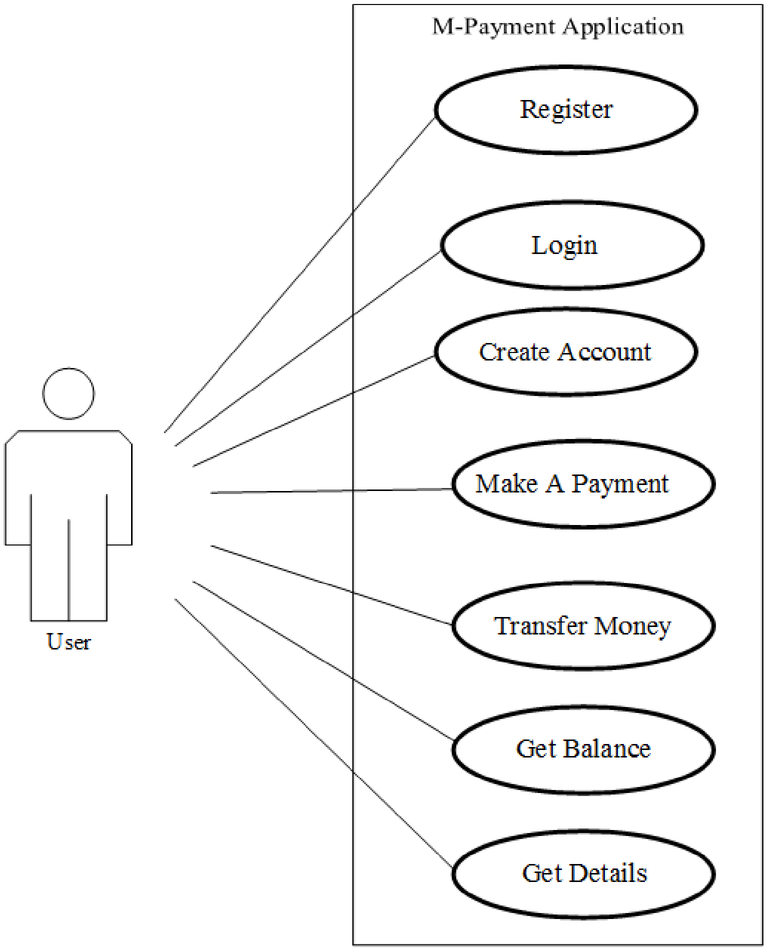


Figure 7-4: M-Payment Application Use Cases

7.2.2.2 Use Case Description

This section gives the description of the Make Payment, the Send Account and the Peer-to-Peer money transfer use case in Figure 7-4. Only the description of the Send Account and the Peer-to-Peer are given because they are the focus of this research.

Table 7: Make A Payment Use Case Description

Use Case Name	**Make Payment**
Description	Enables the customer to carry out an m-payment
Precondition	The customer is logged on to the application and has a bank account.
Flow of events	1. The customer brings the device close to the reader to make a payment. 2. The application receives the payment information and prompts the use to enter his/her PIN number. 3. The application validates the information and sends the information to the banking system. 4. The banking system verifies the PIN. 5. The banking system will perform the transaction and sends confirmation to the customer the merchant as well. 6. The application displays the confirmation.
Alternatives	2b. If the entered information is not correct the customer is prompted to enter the information again. 5b. If the PIN is incorrect the banking system sends back a notification to application prompting the customer to enter the PIN again. 6b. If there is an insufficient balance in the account, the banking system sends a notification the application and aborts the transaction.
Post condition	Payment transaction has been performed.

Table 8: Peer-to-Peer Money Transfer Use Case Description

Use Case Name	**Peer-to-Peer Money Transfer**
Description	Allows a consumer to transfer money to another consumer using NFC.
Precondition	Both the sender and receiver should be logged on to the system and their screens should be active.
Flow of events	1. The consumer to transfer money (sender) enters his/her PIN number and amount to transfer 2. The application will then validate the information. 3. After validation the application will then prompt the sender to bring his/her mobile device close to the receiver's mobile device. 4. To send the message the customer must touch the screen of his/her mobile device when the Touch to Beam UI is displayed. 5. The application on the receiver's mobile device will receive a message requesting receiver to accept or decline the money that is about to be sent. 6. Upon accepting the request the application will validate the information received and then send the information to the banking system. 7. The banking system will validate and authenticate the sender's information 8. After authentication the transaction will be processed. 9. After completing the transaction the bank will notify the both the receiver and the sender of the money.
Alternatives	2b. If the information is not valid, the application will prompt the sender to enter the information again. 5b. If the receiver declines the request, the transaction will be aborted. 7b. If the information received by the banking system is not valid, the application will be notified and the application will prompt the customers to repeat the above steps again, starting with step 1. If the PIN number is not correct the banking system will notify the application and the application will prompt the customers to repeat all the steps again. 9b. if there are insufficient funds in the sender's bank the transaction will be terminated and the customers will be notified.
Post condition	Money is transferred from the sender to the receiver and they are both notified about the transaction.

7.3 Prototype Implementation

A prototype is a working system which is developed mainly to test the ideas of a new system. Prototyping was chosen because:

- All the user requirements were not available
- The proposed system is a new idea and there was no similar systems available
- The system had to be quickly built and validated

In the prototype application we mainly concentrated on the payment service and the peer-to-peer money transfer even though we included other services to make the application as real as possible. One of the major requirements was to make the application as simple as possible to ensure that the participants get to experience the simplicity of NFC technology. This was done without compromising the security of the application. The application was made is such a way that we were able to simulate a real world m-payments environment.

This section describes the implementation of the m-payment prototype, the POS system and the banking system. The m-payment application was implemented using Android and, the POS system and the banking system were implemented using Java. The banking system is a Java Simple Object Access Protocol (SOAP) Web Service. For the development environment an Eclipse IDE bundled together with the Android Developer Tools (ADT) plug-in was used. Table 9 shows the software that was used to implement the system. For the prototype, an m-payment application which also included a peer-to-peer money transfer service was implemented on the Android platform.

Only an Android prototype was developed even though NFC is supported by other operating system platforms. Android is an open-source operating system that is based on Linux which was designed for mobile devices. Android, being open source, enables easy application development. It also makes it easy to implement changes which were very important for our system prototyping. Currently Android has been adopted by major device manufacturers which include Motorola, Samsung, HTC and Sony Ericsson. Even though the Android OS is the relatively newer of the OSes for smartphones it now has a great market share and a larger developer base (Khan & Jain, 2013; Patinge & Soni, 2013).

The Android platform was chosen mainly because it is the most popular operating system for smartphones that supports the NFC technology and also that there are already NFC enabled m-payments that have been successfully implemented such as the Google Wallet. The Graphical User Interface is one of the most important parts of an application and Android supports easy and flexible development of GUI (Jackson, 2011).

Table 9: Software

Software	Description
Operating System	Windows 7
Relational Database Management System	MySQL Server
Programming Language	Android and Java
Plug-in	Android Developer Tools (ADT) Plug-in
Integrated Development Environment	Eclipse for Java EE Developers
Server	Glassfish
Software development kit	ACR122U NFC Reader SDK
Libraries	• MySQL connector for java • NFCtools

NFCtools is a collection of tools and libraries for NFC and it is written in Java. NFCtools provides libraries for both peer-to-peer and card emulation. Table 10 shows the hardware that was used in the development of the m-payment application.

Table 10: Hardware

Hardware	Description
Mobile devices	• Samsung Galaxy s3 and s4 • Samsung Galaxy FAME
NFC Smartcard Reader	ACR122U-A9

Figure 7-5 shows the smart card reader that was used for this research. The ACR 122U also known as an NFC reader is a product of Advanced Card Solutions. It is a USB contactless smart card reader developed on the 13.56 MHz contactless technology.

Figure 7-5: ACR 122U-A9 Smart Card Reader

The reader adheres to the CCID standard. This enables the Windows OS to use the Microsoft CCID drivers for the reader. The ACR 122U comes with its own drivers and SDK. The reader supports NFC, FeliCa, Mifare and ISO 14443 tags. It can be used many different applications which include payment, mass transit, attendance and physical access control. In the payment prototype application, the reader was the initiator therefore the computer where the reader was connected started communication by sending a message to the NFC reader over the USB connection.

7.3.1 NFC Data transmission specifications

Figure 7-6 shows the NFC Forum specifications which ensure interoperability. The NFC Forum specifications include a standard data format called NFC Data Exchange Format (NDEF) for NFC Forum devices. The specifications of the data format are given in the NDEF specification. An NFC Forum device is a device which complies with the NFC Forum specifications. The NFC Data Exchange Format (NDEF) specification defines the NDEF as a "lightweight, binary message format that can be used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct" (Specification, 2006). The payload is the message that is contained in the transmitted data. The payload is described by a type, length and an optional identifier. The Record Type Definition (RTD) enables the application to determine the semantics and structure of the contents of the record. The NFC Forum has defined different types of RTDs and NDEF messages to ensure interoperability and easy communication. The Type Name Format (TNF) enables the NFC device to determine the type of data contained in the message.

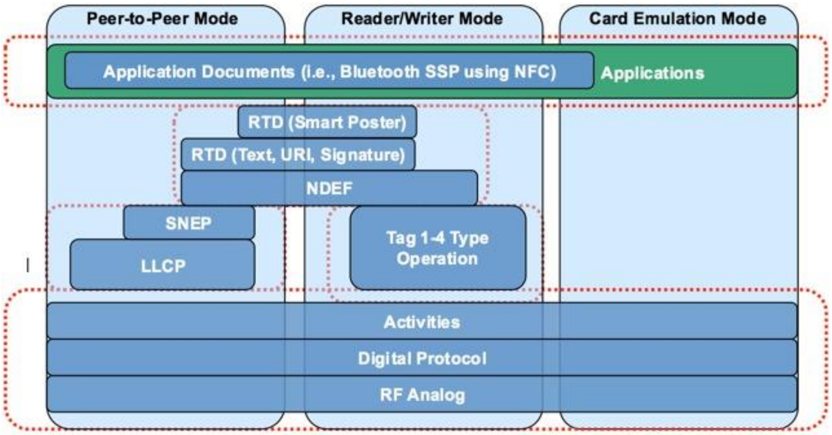


Figure 7-6: NFC Forum Specifications Protocol for ensuring interoperability

The peer-to-peer mode uses either the Logical Link Control Protocol (LLCP) or the Simple NDEF Exchange protocol (SNEP) to transmit data as shown in Figure 7-6. The LLCP specifications enables the transfer of upper layer messages between two NFC Forum devices (NFC Forum, 2009). The LLCP provides link activation, supervision, deactivation of communication, connection oriented transport, connectionless transport, protocol multiplexing and asynchronous balance mode. The SNEP enables an NFC Forum device to send NDEF messages to another NFC Forum device (NFC Forum, 2011). The next section will look at

NDEF messages in great depth. The SNEP employs the connection-oriented transport mode of the LLCP in order to exchange data reliably. The NFCtools libraries supports both SNEP and LLCP, for this implementation we employed the LLCP because it supports bi-directional communication which was needed to send confirmation of the payment to the customer for the m-payment service.

Both the money transfer and the m-payment service use the peer-to-peer mode of NFC. The message that is sent by the devices during communication should be prepared according the NFC Forum standards to ensure interoperability. Figure 7-7 shows the protocols that are associated with the peer to peer mode. The Analogue layer is the NFCIP 1 (ISO/IEC 18092) which gives the specification details of NFC which includes its data exchange rate and radio frequency. The Digital Protocol layer is a simple data exchange protocol for peer-to-peer communication. As mentioned above, the prototype application was implemented using LLCP. The LLCP establishes smooth communication by handling things such as initiator and target configurations and controlling the flow communication. As a library was used to, the Protocol Bindings and other protocols that were used were handled by the library.

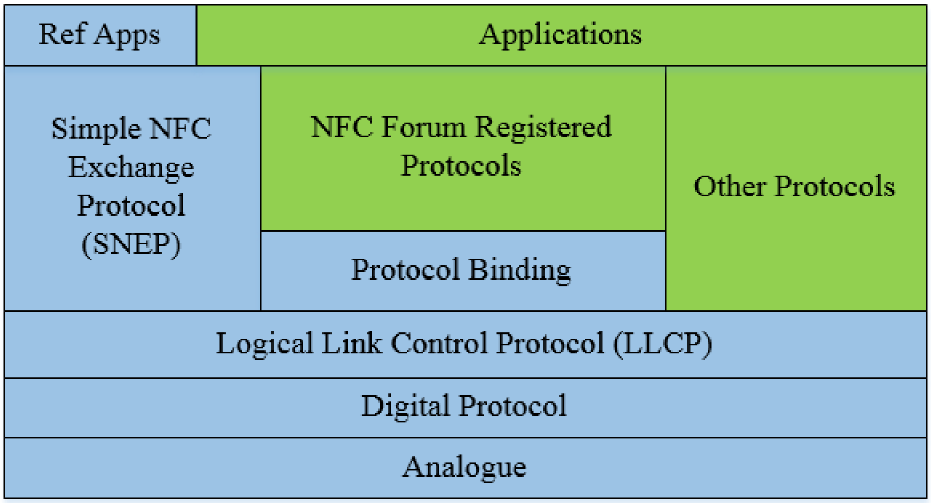

Ref Apps
Applications
Simple NFC Exchange Protocol (SNEP)
NFC Forum Registered Protocols
Protocol Binding
Other Protocols
Logical Link Control Protocol (LLCP)
Digital Protocol
Analogue

Figure 7-7: NFC Peer-to-Peer Mode

Protocol binding provides bindings to registered NFC Forum protocols. The bindings for LLCP are provided in the NFC registered protocols.

7.3.2 System components

The main components of the mobile payment application are the Android application, the web service and the database as shown in Figure 7-8. The Android money transfer service allows for money transfer using the peer-to-peer mode of the NFC technology. The POS system is used when carrying out m-payments. The simulated banking system is composed a SOAP Web Service and a database as shown in Figure 7-8. Arrow B represents the connection between the web service and the database. For every request that is made to the banking system there is a response, this is shown by the double arrows in Figure 7-8. Arrow A represents the request to and a response from the Simulated Banking System. When the sender requests to transfer money the Android application first sends a request to the banking system to enable the transfer, this is represented by the arrow labelled 2. If the PIN is wrong or there is an insufficient balance, the transaction is cancelled. The next step if transaction will be to transfer the banking details to the receiver and this is represented by the arrow labelled 1 in Figure 7-8. After the receiver has accepted the transfer the banking information will be sent to the simulated banking system (arrow 3). To perform an m-payment the user has to be logged on to the application. The reader will transfer the merchant's banking system to the customer's device (arrow 4). After receiving the payment details, the application will request the customer to authenticate the payment by entering PIN number and accepting and the information will be sent to the banking system (arrow 5). After the transaction has been processed both the customer and merchant will be notified (arrow 5 and arrow 6).

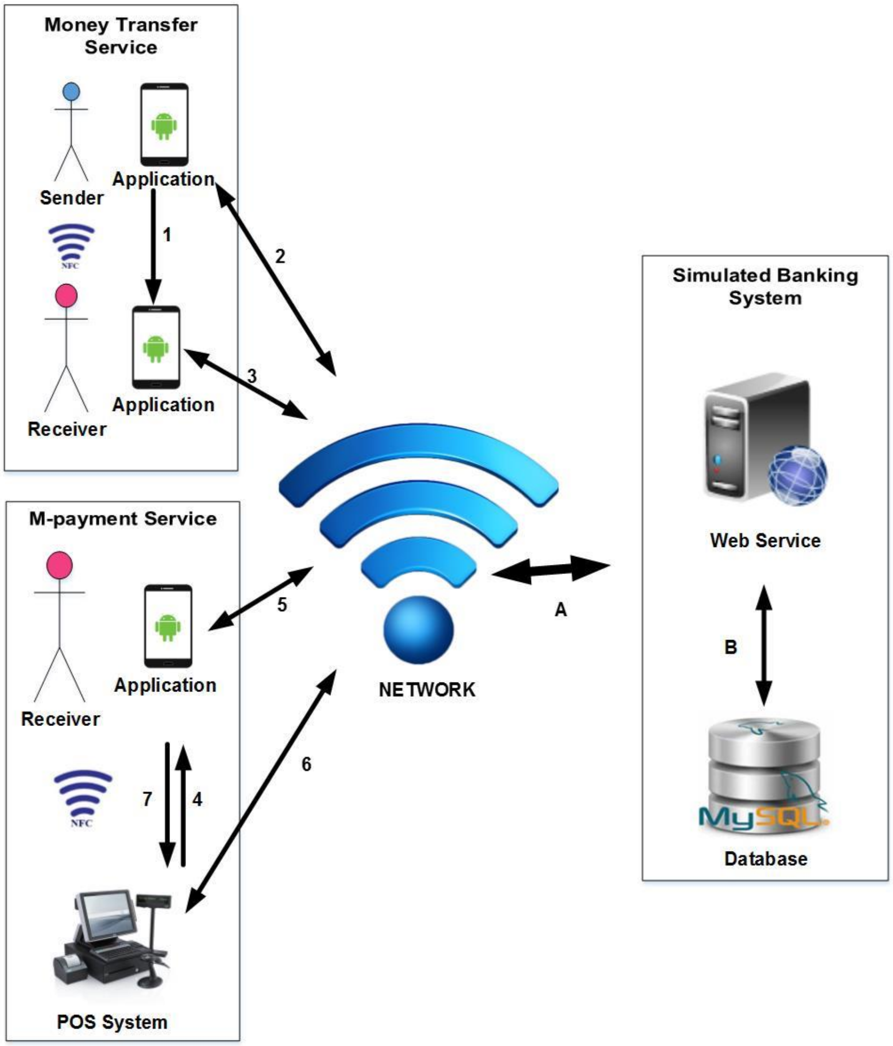


Figure 7-8: Components of the M-Payment Application

7.3.2.1 Back-end Simulated Banking System

In order to fully implement a working prototype, we also had to develop a stub of the back-end banking system. Figure 7-9 shows the model of a web service. The banking system was implemented using the Java web services using the JAX-WS API. A web service is "interface that describes a collection of operations that are network-accessible through standardized XML messaging" (Gottschalk, Graham, Kreger, & Snell, 2002). As the banking system was not the main focus of the research, a basic functioning backend was implemented to support the operation of the mobile application.

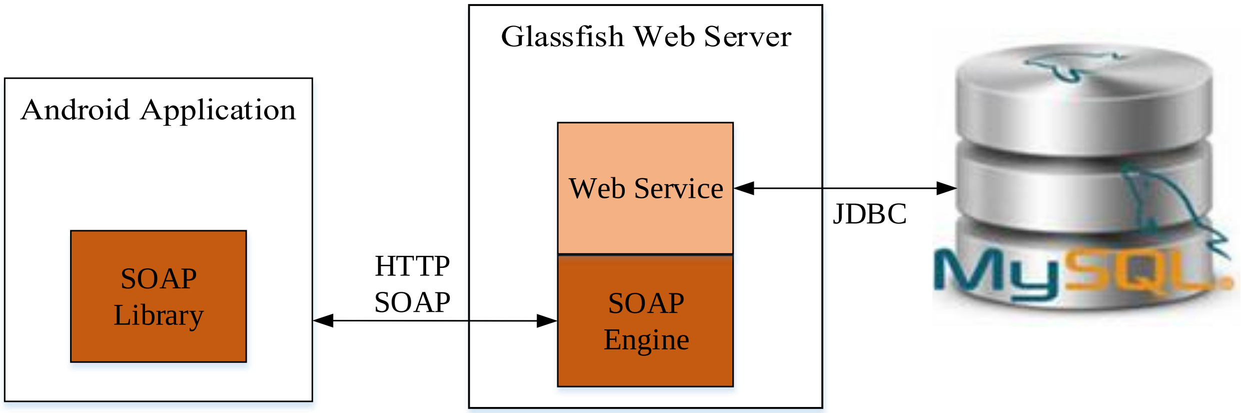


Figure 7-9: Web Service Model

Web services were the best option for the banking system because their access is independent of its implementation and deployment platform and we needed to access the simulated back-end banking system from both the android application and the POS system.

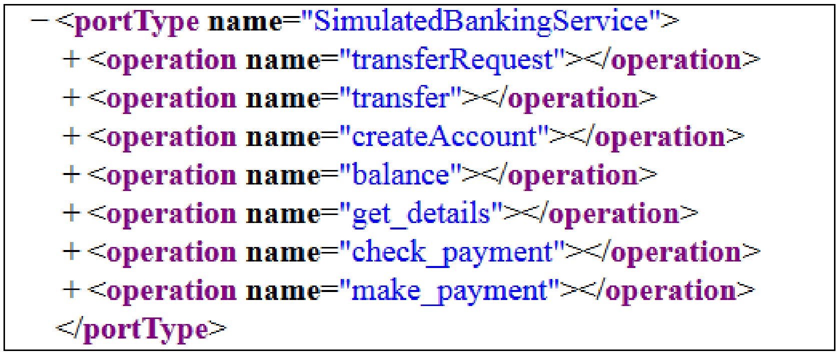
The web service can be accessed using either Simple Object Access Protocol (SOAP) or Representational State Transfer (REST). SOAP is a web service access protocol that is based on standards. “SOAP provides a standard packaging structure for transporting XML documents over a variety of standard Internet technologies, including SMTP, HTTP, and FTP. It also defines encoding and binding standards for encoding non-XML RPC invocations in XML for transport” (Chappell & Jewell, 2002). REST is an “architectural style for distributed hypermedia systems” (Fielding, 2000). “The RESTful approach espouses that Web service solutions can be developed by simply representing and exposing system’s resources, and by transferring data over HTTP” (Pavan, Sanjay, & Zornitza, 2012). SOAP web services are easy to consume, provides guaranteed reliability and are more secure than REST web services. SOAP has specifications that enable the service provider and the consumer to agree on the exchange format. SOAP is independent of language, platform and transport. The focus of SOAP is to access the operations of the web service. SOAP was chosen due to the following:

- WS-Security - SOAP protocol has a data privacy and data integrity implementation standard.

- Atomic Transaction - this offers transaction reliability for the banking transaction. REST does not comply with the ACID (Atomicity, Consistency, Isolation and Durability) standards. Atomicity guarantees that all steps involved in a transaction must happen or none of the steps must take place. Consistency guarantees that all data will be consistent; isolation means that all transactions will not have access to data form another transaction before that transaction has completed its task on the data. Durability guarantees that the changes made by the transactions will be saved on a durable and persistent medium.

- Reliable Messaging - SOAP has a standard massaging system which is lacked by REST. SOAP has built in logic for successful/retries thus making it more reliable.

The details that are needed by a client in order to interact with the web service are found in an XML document for the web service called the service description. The description of the web services are expressed in the Web Services Description Language (WSDL). Listing 1 show the operations of the banking system extracted from the WSDL (for the full WSDL see APPENDIX D – SOAP WSDL).



```
– <portType name="SimulatedBankingService">
   + <operation name="transferRequest"></operation>
   + <operation name="transfer"></operation>
   + <operation name="createAccount"></operation>
   + <operation name="balance"></operation>
   + <operation name="get_details"></operation>
   + <operation name="check_payment"></operation>
   + <operation name="make_payment"></operation>
  </portType>
```

Listing 1: Simulated back-end banking system operations

Upon receiving banking messages from the Android application, the simulated back-end banking system first decrypted the message before performing the requested transaction. The web service has seven operations:

- `transferRequest` – handles the money transfer request made by the sender during money transfer

- `transfer` – performs the actually transfer of money.

- `createAccount` – handles all transactions that involve the creation of an account by the user
- `balance` – handles balance enquiries
- `get_details` – enables the user to retrieve all their account details
- `check_payment` – enables the POS system to keep track of a payment transaction
- `make_payment` – handles the payment transaction

Each operation is authenticated by the PIN number from the user. After completing the transaction the system sends a responds informing the user about the outcome of the transaction.

7.3.2.2 The Point of Sale System

A simple java application was developed to simulate the point of sale system that is used by merchants. This application was responsible for sending payment information to the reader and to the simulated back-end banking system as well. If the communication between the reader and the customer device was still open, the payment application would send the payment confirmation to the customer's device. The payment data was transmitted using the LLCP protocol.

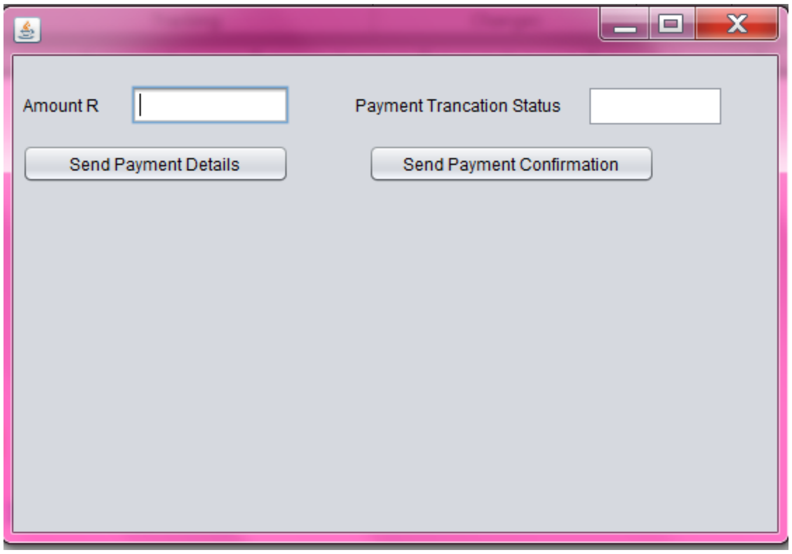
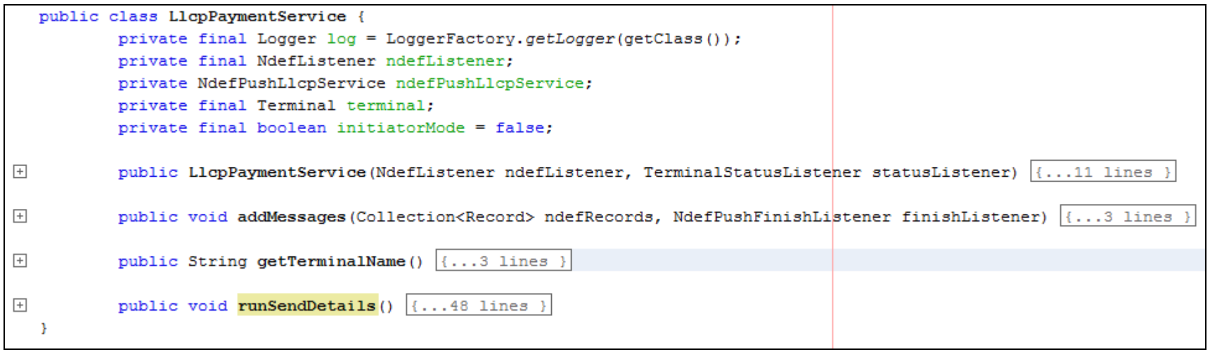


Figure 7-10: POS system user interface.

The POS system has three classes: `POSApp`, `POSInterface` and the `LlcpPaymentService`. The `POSApp` is the main class. `POSInterface` extends the JFrame and is responsible for extracting the amount and also displaying the payment transaction details. The class has an inner class called `CheckTransaction()` that extends the `TimerTask` class. The `CheckTransaction`() class keeps a timer which is one minute long that starts when the payment details are send to the reader. If the timer ends before the transaction details have been received from the banking system, a message will be send to the simulated banking system to cancel the transaction. The web service only response to a request, so the `CheckTransaction`() will send messages to the banking system at regular intervals to check on the transaction status until either the timer runs out or the transaction has been processed. Listing 2 shows the `LlcpPaymentService` () class. This class is responsible for sending the payment details to the reader.



```
public class LlcpPaymentService {
        private final Logger log = LoggerFactory.getLogger(getClass());
        private final NdefListener ndefListener;
        private NdefPushLlcpService ndefPushLlcpService;
        private final Terminal terminal;
        private final boolean initiatorMode = false;

+       public LlcpPaymentService(NdefListener ndefListener, TerminalStatusListener statusListener) {...11 lines }

+       public void addMessages(Collection<Record> ndefRecords, NdefPushFinishListener finishListener) {...3 lines }

+       public String getTerminalName() {...3 lines }

+       public void runSendDetails() {...48 lines }
}
```

Listing 2: Class responsible for sending payment details to the reader

The `LlcpPaymentService()` is invoked when the ‘Send Payment Details’ button is clicked and it sends the payment details to the reader. The reader keeps the payment until the next payment details are sent to it. The `LlcpPaymentService()` makes use of the NFCtools to transfer the payment details. For the details to be received by the payment application, the screen of the device has to active and unlocked. The next section covers the Android payment application in detail.

7.3.2.3 Android Application

The package `android.nfc` includes all the classes that are required by an application to read and write NDEF messages and it also enables NFC enabled mobile devices to exchange data. The `android.nfc` consists of six classes shown in Table 11.

Table 11: Classes in the `android.nfc` package

Class Name	Description
`Tag`	Represents the discovered NFC tag
`NfcAdapter`	Represents the NFC adapter of the mobile phone
`NfcManager`	Obtains an instance of the NFC adapter
`NdefMessage`	Represents an NDEF message
`NfcEvent`	Wraps information associated with an NFC event
`NdefRecord`	Represents an NDEF record

NFC is enabled for an application by adding the following line in the manifest file:

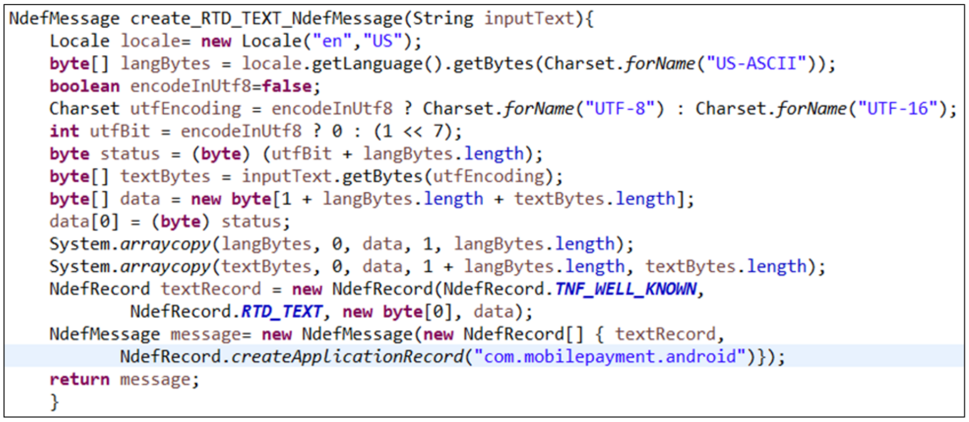
```
<uses-permission android:name="android.permission.NFC" />
```

The above statement notifies the user during installation that the application uses the NFC technology. The minimum API level that supports NFC technology is API 9 but this API does not support the peer-to-mode of the NFC technology, therefore the minimum API that was used for the application is API 14.

7.3.2.3.1 Creating the NDEF Message

The NDEF message is created using the `NDEFMessage` class. The number of records contained in the NDEF message is not restricted. In Android OS the Android beam is enabled by implementing either the `setNdefPushMessageCallback()` method or the `setNdefPushMessage()` method. We chose to implement the application using the `setNdefPushMessage()` method because this method automatically links itself to the life-cycle of the activity, thereby removing the need to call enables and disable in the Resume/onPause method. Before the encapsulation of the message in the `NdefMessage` object the message was encrypted. The m-payment application uses TNF_WELL_KNOWN for the Type Name Format (TNF) of the data with RTD_TEXT as the Record Type Definition (RTD).

The following code was used to create the NDEF message. Listing 3 shows the code that was used to create the NDEF message.



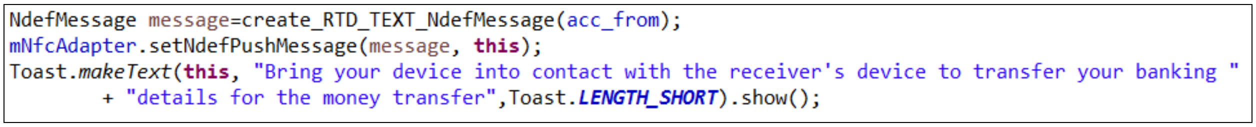
```
NdefMessage create_RTD_TEXT_NdefMessage(String inputText){
    Locale locale= new Locale("en","US");
    byte[] langBytes = locale.getLanguage().getBytes(Charset.forName("US-ASCII"));
    boolean encodeInUtf8=false;
    Charset utfEncoding = encodeInUtf8 ? Charset.forName("UTF-8") : Charset.forName("UTF-16");
    int utfBit = encodeInUtf8 ? 0 : (1 << 7);
    byte status = (byte) (utfBit + langBytes.length);
    byte[] textBytes = inputText.getBytes(utfEncoding);
    byte[] data = new byte[1 + langBytes.length + textBytes.length];
    data[0] = (byte) status;
    System.arraycopy(langBytes, 0, data, 1, langBytes.length);
    System.arraycopy(textBytes, 0, data, 1 + langBytes.length, textBytes.length);
    NdefRecord textRecord = new NdefRecord(NdefRecord.TNF_WELL_KNOWN,
            NdefRecord.RTD_TEXT, new byte[0], data);
    NdefMessage message= new NdefMessage(new NdefRecord[] { textRecord,
           NdefRecord.createApplicationRecord("com.mobilepayment.android")});
    return message;
    }
```

Listing 3: Creating NDEF Message that use TNF_WELL_KNOWN with RTD_TEXT

7.3.2.3.2 Beaming a message

Listing 4 shows the code for beaming a message. Beaming using `setNdefPushMessage()` occur as follows:

- Create the NDEF message to send as shown in Listing 4.
- Call the `setNdefPushMessage()` method. When the target (the receiver's mobile device when transferring money or customer's device when making an m-payment) is discovered the message is beamed.



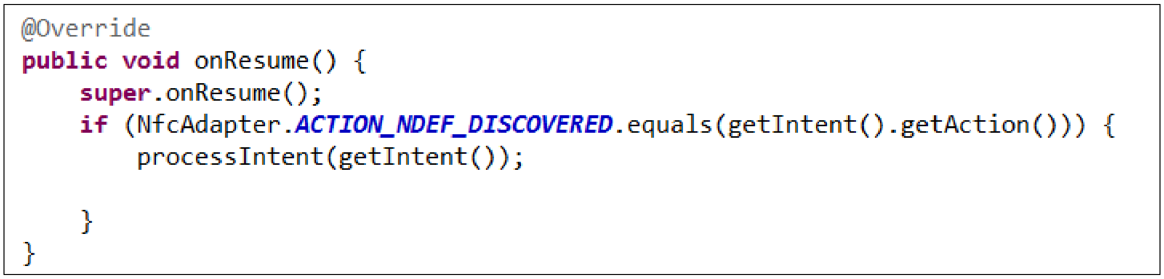
```
NdefMessage message=create_RTD_TEXT_NdefMessage(acc_from);
mNfcAdapter.setNdefPushMessage(message, this);
Toast.makeText(this, "Bring your device into contact with the receiver's device to transfer your banking "
        + "details for the money transfer",Toast.LENGTH_SHORT).show();
```

Listing 4: Beaming a message

7.3.2.3.3 Receiving a beam

To receive the beam, the following two steps were followed:

- An `onNewIntent(Intent)` method which calls the `setIntent(Intent)` was implemented.
- The `onResume` method was called from the above method.

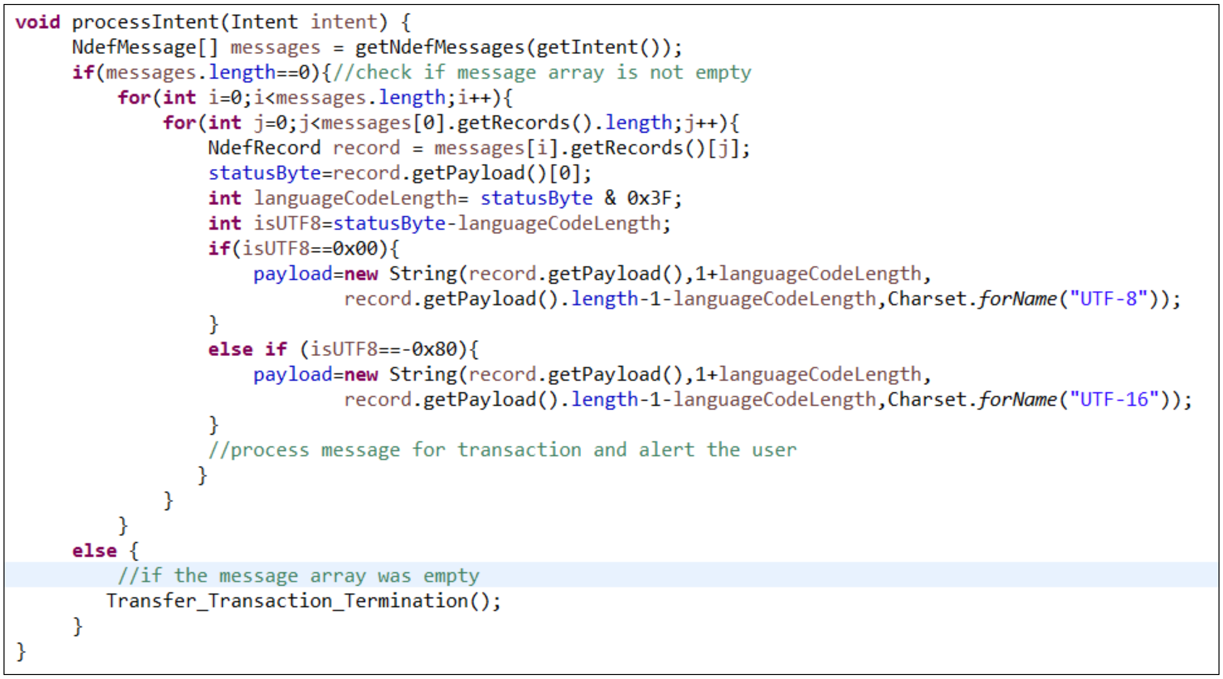


```
@Override
public void onResume() {
    super.onResume();
    if (NfcAdapter.ACTION_NDEF_DISCOVERED.equals(getIntent().getAction())) {
        processIntent(getIntent());

    }
}
```

Listing 5: `OnResume()` method

Listing 5 shows the `onResume` method. The `onResume` method checks to ensure that the activity is executed with a beam and then it invokes the `processIntent` () method which will process the received NDEF message as shown in Listing 6.



```
void processIntent(Intent intent) {
     NdefMessage[] messages = getNdefMessages(getIntent());
     if(messages.length==0){//check if message array is not empty
         for(int i=0;i<messages.length;i++){
             for(int j=0;j<messages[0].getRecords().length;j++){
                 NdefRecord record = messages[i].getRecords()[j];
                 statusByte=record.getPayload()[0];
                 int languageCodeLength= statusByte & 0x3F;
                 int isUTF8=statusByte-languageCodeLength;
                 if(isUTF8==0x00){
                     payload=new String(record.getPayload(),1+languageCodeLength,
                             record.getPayload().length-1-languageCodeLength,Charset.forName("UTF-8"));
                 }
                 else if (isUTF8==-0x80){
                     payload=new String(record.getPayload(),1+languageCodeLength,
                             record.getPayload().length-1-languageCodeLength,Charset.forName("UTF-16"));
                 }
                 //process message for transaction and alert the user
                }
             }
         }
     else {
         //if the message array was empty
        Transfer_Transaction_Termination();
     }
}
```

Listing 6: `processIntent` Method

7.3.2.3.4 Flow of events

Figure 7-11 shows the activity flow diagram of the peer-to-peer money transfer option and Figure 7-12 shows the activity diagram of the m-payment transaction. The activity diagram summarizes the steps taken by both the user and the system in carrying out a transaction.

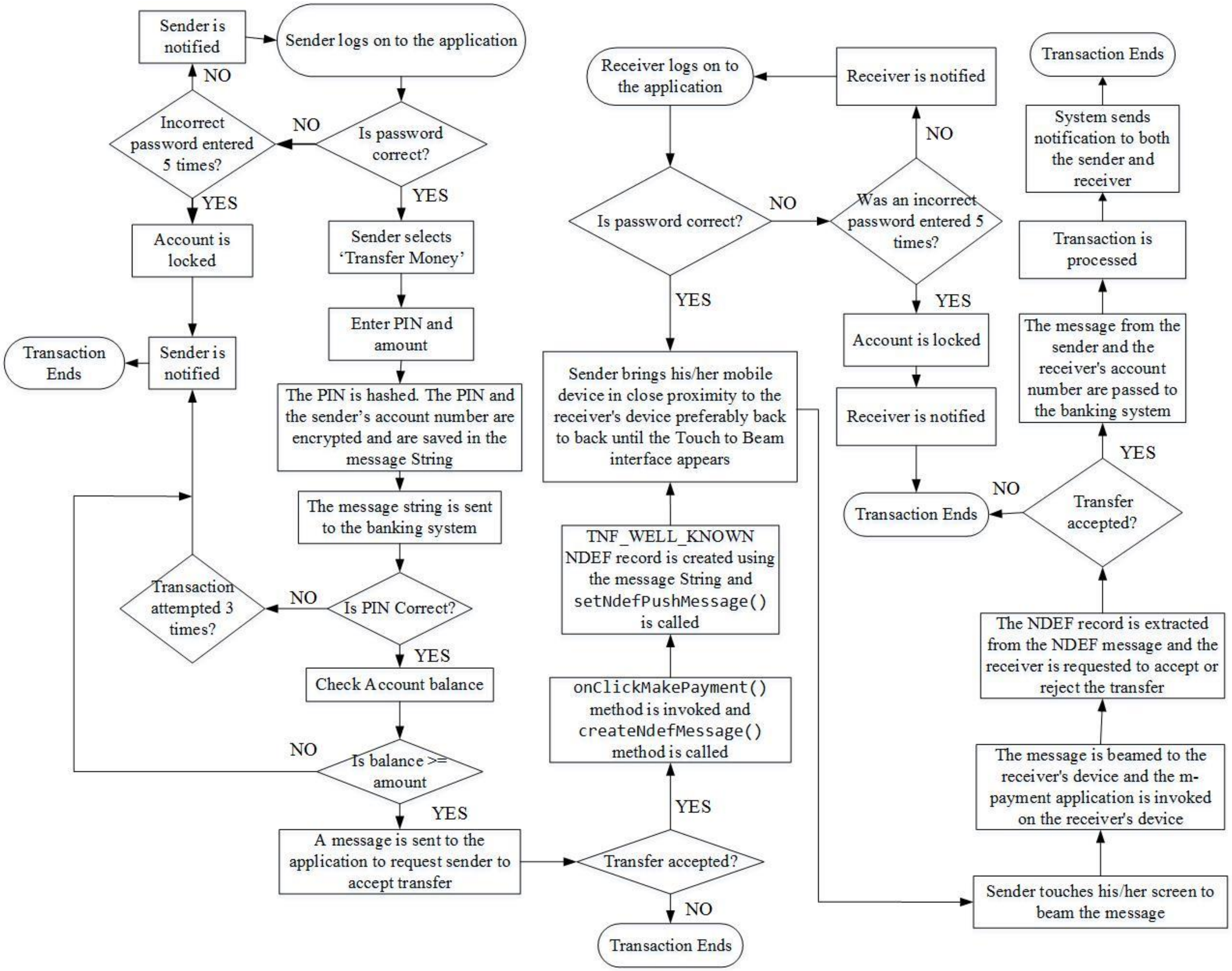

Sender is notified
Sender logs on to the application
NO
Incorrect password entered 5 times?
NO
Is password correct?
YES
YES
Account is locked
Sender selects 'Transfer Money'
Enter PIN and amount
Transaction Ends
Sender is notified
The PIN is hashed. The PIN and the sender's account number are encrypted and are saved in the message String
The message string is sent to the banking system
Transaction attempted 3 times?
NO
Is PIN Correct?
YES
Check Account balance
NO
Is balance >= amount
YES
A message is sent to the application to request sender to accept transfer
Transfer accepted?
NO
Transaction Ends
YES
onClickMakePayment() method is invoked and createNdefMessage() method is called
TNF_WELL_KNOWN NDEF record is created using the message String and setNdefPushMessage() is called
Sender brings his/her mobile device in close proximity to the receiver's device preferably back to back until the Touch to Beam interface appears
YES
Is password correct?
NO
Receiver logs on to the application
Receiver is notified
NO
Was an incorrect password entered 5 times?
YES
Account is locked
Receiver is notified
Transaction Ends
NO
Transfer accepted?
YES
Transaction Ends
System sends notification to both the sender and receiver
Transaction is processed
The message from the sender and the receiver's account number are passed to the banking system
The NDEF record is extracted from the NDEF message and the receiver is requested to accept or reject the transfer
The message is beamed to the receiver's device and the m-payment application is invoked on the receiver's device
Sender touches his/her screen to beam the message

Figure 7-11: Activity Flow diagram for the peer-to-peer money transfer transaction

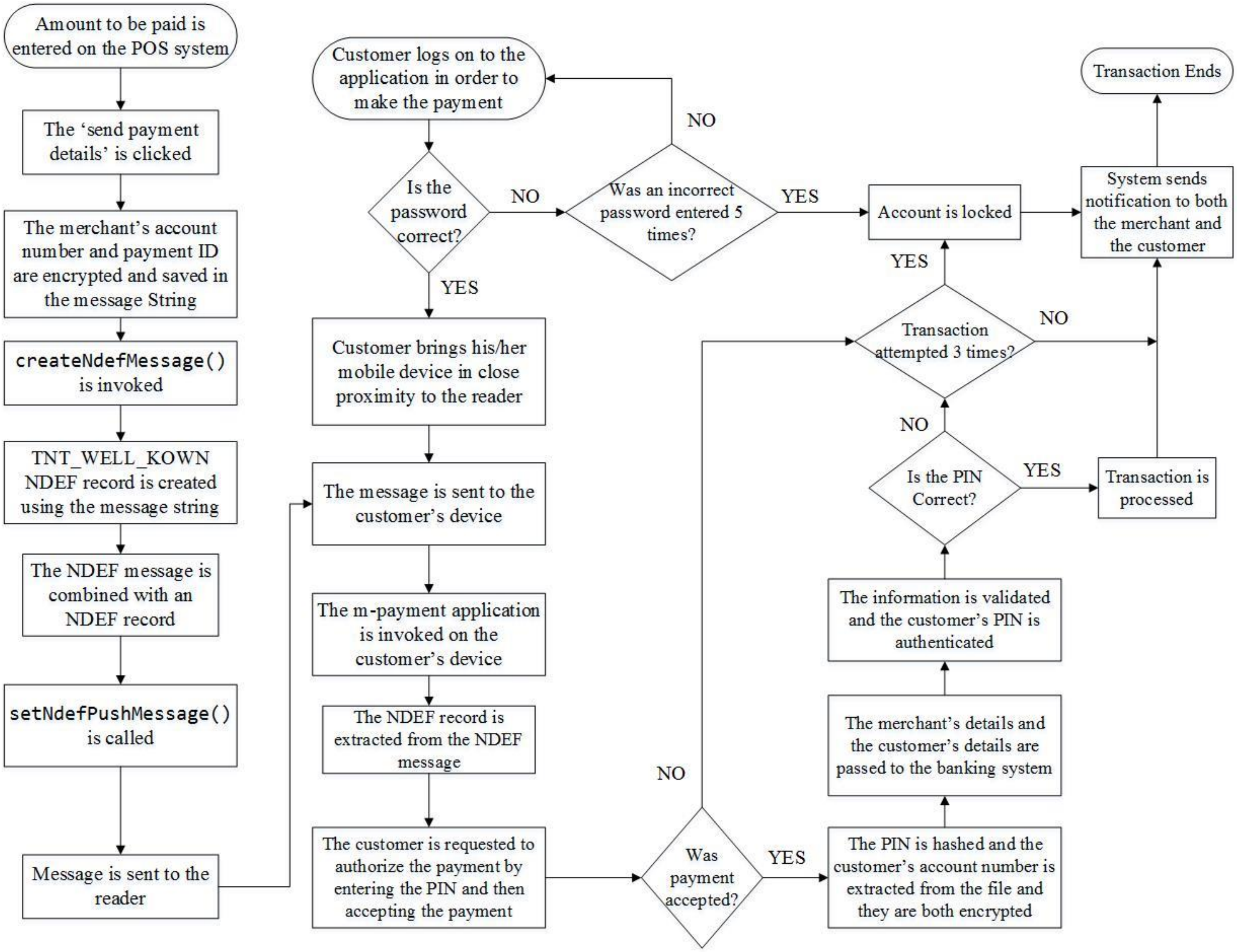

Amount to be paid is entered on the POS system
The 'send payment details' is clicked
The merchant's account number and payment ID are encrypted and saved in the message String
createNdefMessage() is invoked
TNT_WELL_KOWN NDEF record is created using the message string
The NDEF message is combined with an NDEF record
setNdefPushMessage() is called
Message is sent to the reader
Customer logs on to the application in order to make the payment
Is the password correct?
NO
YES
Was an incorrect password entered 5 times?
NO
YES
Customer brings his/her mobile device in close proximity to the reader
The message is sent to the customer's device
The m-payment application is invoked on the customer's device
The NDEF record is extracted from the NDEF message
The customer is requested to authorize the payment by entering the PIN and then accepting the payment
Was payment accepted?
NO
YES
The PIN is hashed and the customer's account number is extracted from the file and they are both encrypted
The merchant's details and the customer's details are passed to the banking system
The information is validated and the customer's PIN is authenticated
Is the PIN Correct?
NO
YES
Transaction attempted 3 times?
NO
YES
Account is locked
Transaction is processed
System sends notification to both the merchant and the customer
Transaction Ends

Figure 7-12: Activity Flow diagram for the m-payment transaction

In the peer-to-peer money transfer option, two NFC mobile devices will be used and in the m-payment transaction, a reader and an NFC device will be used. These are the only options in the m-payment application that uses the NFC technology and they are our focus of study.

7.3.2.3.5 Application Security Features

The application provides 2 levels of security. The application will request a user to create a password just after installation. The application will not allow the user to open an account before creating the password. Figure 7-13 shows the first screen that is displayed when the user launches the application. Figure 7-14 and Figure 7-15 are the next screens when the user chooses either Login or Register respectively.

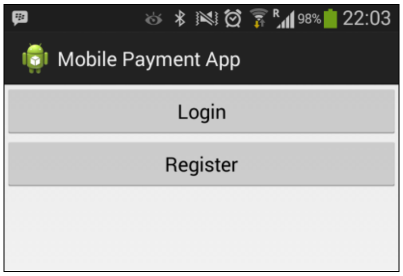


Figure 7-13: First Screen

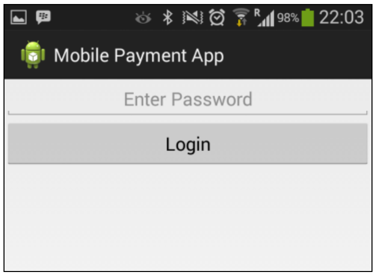


Figure 7-14: Login Screen

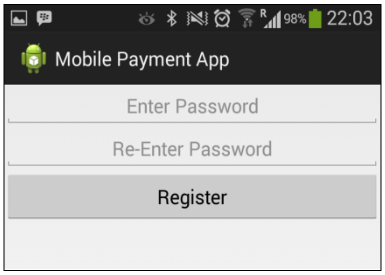


Figure 7-15: Registration Screen

The password that is entered by the user is encrypted before it is stored. Encryption is done using the AES algorithm. Also during peer-to-peer money transfer, the banking information is encrypted using the AES algorithm. No transaction is processed unless the user provides a valid PIN number. The PIN number is provided by the user during creation of the account. The PIN number must have 4 digits.

7.4 M-payment application services

The application had 5 options for the user to choose from as shown in Figure 7-16. The user has to create an account before accessing other services. An error message shown in Figure 7-17 is displayed when the user tries to use any option before creating an account. Figure 7-18 shows the screen for creating the account. Each user is allocated R5000 upon creation of an account.

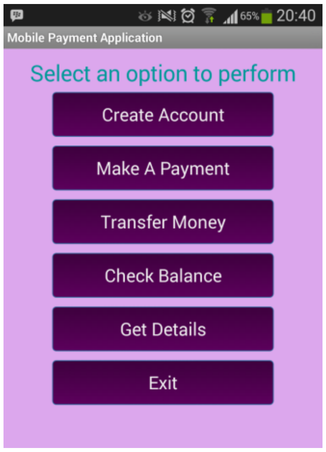
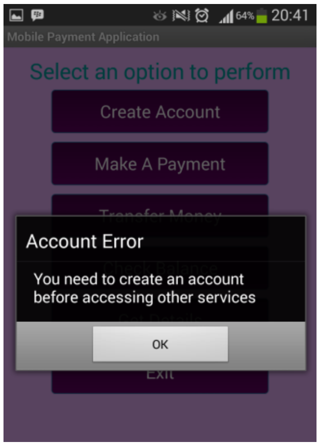


Figure 7-16: Main Screen



Account Error

You need to create an account before accessing other services

Figure 7-17: Error message for account

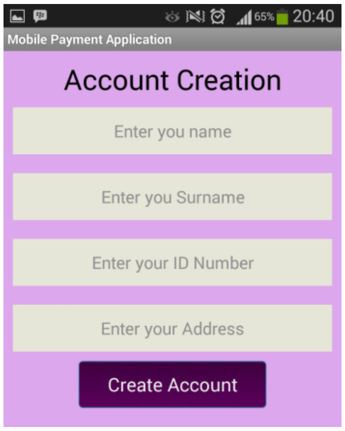
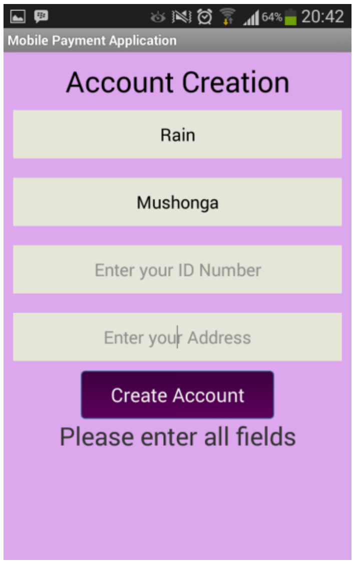


Figure 7-18: Account creation

If the user does not enter all the details that are shown in Figure 7-18, the error shown in Figure 7-19 is displayed. Upon pressing the create account button after entering all the fields the user is requested to create a PIN number that has at least 4 digits (Figure 7-20: Alert Dialog for creating a PIN). If the digits are less than four or the PIN number does not match the error message shown in Figure 7-21 will be displayed.



Rain

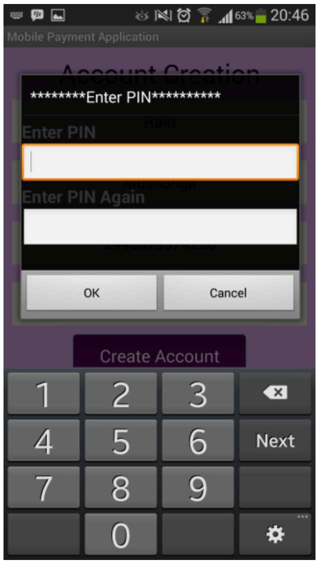
Mushonga

Enter your ID Number

Enter your Address

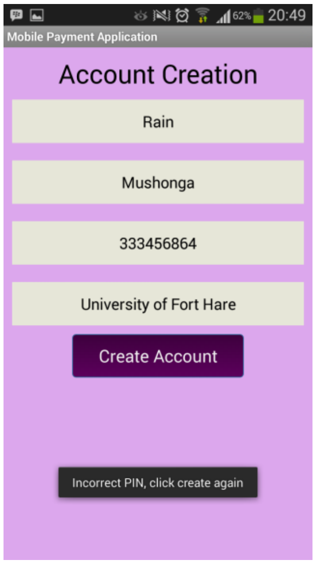
Please enter all fields

Figure 7-19: Error message for missing fields



********Enter PIN**********

Figure 7-20: Alert Dialog for creating a PIN



Rain

Mushonga

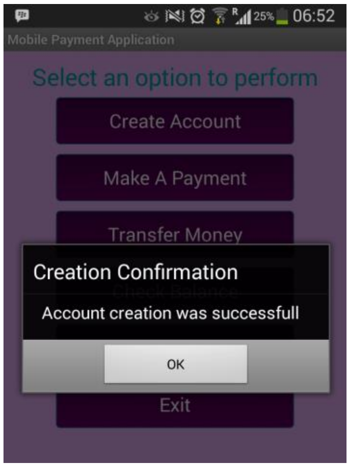
333456864

University of Fort Hare

Incorrect PIN, click create again

Figure 7-21: Incorrect PIN error message

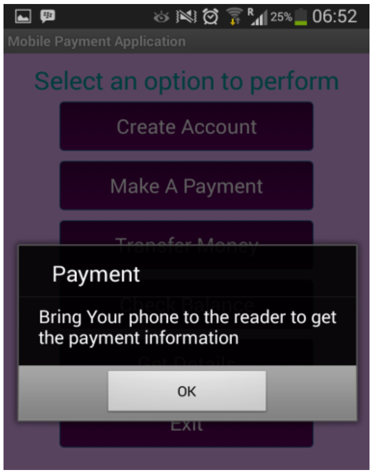
If the account is created successfully, the message shown in Figure 7-22 is displayed.



Creation Confirmation

Account creation was successfull

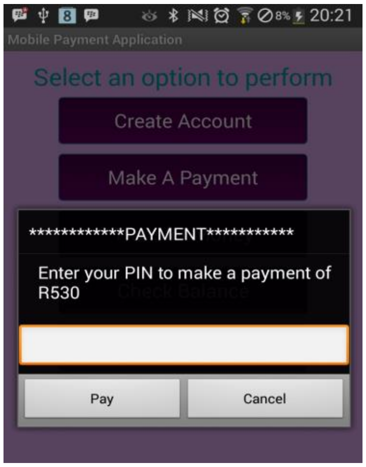
Figure 7-22: Account creation confirmation



Payment

Bring Your phone to the reader to get the payment information

Figure 7-23: M-payment information



************PAYMENT***********

Enter your PIN to make a payment of R530

Figure 7-24: Payment Confirmation

When the ‘Make A Payment’ button is pressed the message shown in Figure 7-23 is displayed. After the phone has received the payment information from the reader the message shown in Figure 7-24 is displayed. If the user enters the correct PIN and presses the pay button the transaction information will be sent to the banking information and the user will be informed of the transaction outcome.

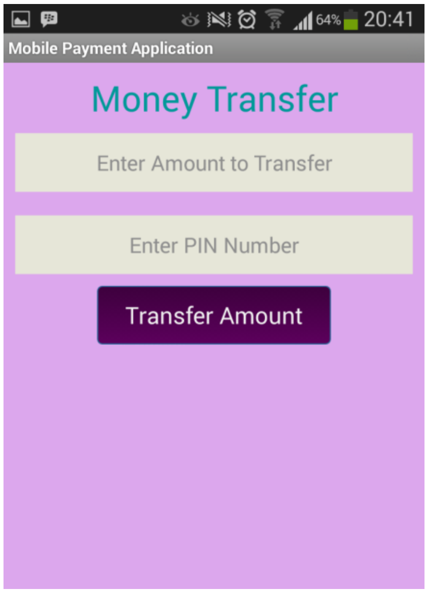
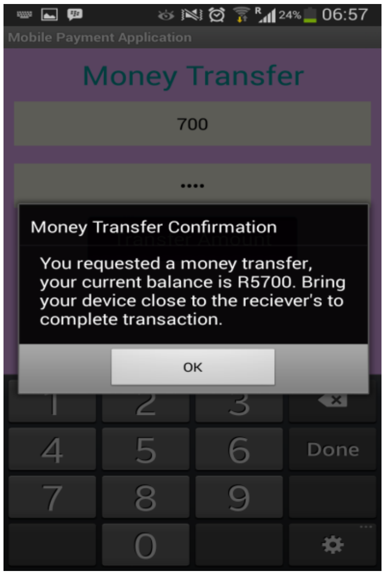


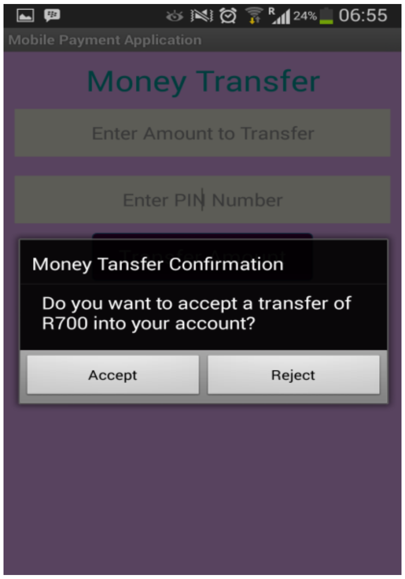
Figure 7-25: Money Transfer Screen



Money Transfer Confirmation

You requested a money transfer, your current balance is R5700. Bring your device close to the reciever's to complete transaction.

Figure 7-26: Money Transfer Confirmation



Money Tansfer Confirmation

Do you want to accept a transfer of R700 into your account?

Figure 7-27: Receiver's Confirmation request

Figure 7-25 shows the money transfer screen. The sender will enter the amount and his/her PIN, upon pressing the 'Transfer Amount' button, the message shown in Figure 7-26 will be displayed and the sender will confirm and move his/her device close to the receiver's phone (the devices should be back to back). The receiver has the choice to either accept or reject the payment. If the receiver accepts the payment, he/ she will be notified of the outcome after the transaction has been processed. The sender will also be notified of the outcome of the transaction. For every option that the user chooses except for the account creation option, the user is requested to provide his/ her PIN number. If the PIN is incorrect, the request will not be processed. This section looked only at main services of the prototype application to show that it is interactive and usable. The usability and the functions of the application will tested in the next chapter.

7.5 Conclusion

The implementation of the application was done using the prototyping methodology. The payment application went through four phases of refinement. It should be noted that this was a prototype to test the functionality of the NFC technology and to introduce the technology and m-payments to the participants in our study area. The next Chapter discusses the testing of the prototype application. The implementation was done successfully without any difficulty even though the amount of literature and books on the implementation of NFC enabled application was limited. This chapter has shown that it is possible and practical to implement an NFC enabled m-payment application. This chapter has partially fulfilled objective OBJ4. There is still need to carry out testing on the application and the next section will look at this in more details.

8 APPLICATION TESTING AND VALIDATION

8.1 Introduction

Software implementation cannot be complete without software testing. Testing evaluates the application and also helps in identifying problems, limitations and defects of both the application and the technology used by the application. This chapter discusses the testing that was done on the prototype application. The application testing focused on the application performance, memory usage and battery consumption. Since the application was developed using system prototyping, each prototype that was released was tested before it was modified. Since NFC is a new technology, we also saw that it was imperative for us to test its functionality. There are different types of application testing and the following tests were done on the payment application: functional testing, performance testing, network testing, installation testing, compatibility testing, secure testing and usability testing.

8.2 Functional Testing

Functional testing - ensures that the application meets all the requirements of the application. This testing was carried out to validate that the application meets the requirements given in Chapter 7. Two types of functional testing were done on the application: User Interaction testing and Transaction testing. Functional testing was done on both emulated and real devices. The functional testing was based on the use case given in Chapter 7. Functional testing included data validation and interruption testing.

Figure 8-1 shows the Android life cycle. To cater for interruptions during the transfer of payment details and money transfer details using the NFC technology, the `onResume()` and the `onPause()` methods were implemented. This ensured that the application received notifications even if the m-payment application was not on the foreground. All the other methods in the android life cycle were not implemented except for the `onCreate()` method which must be implemented by all activities.

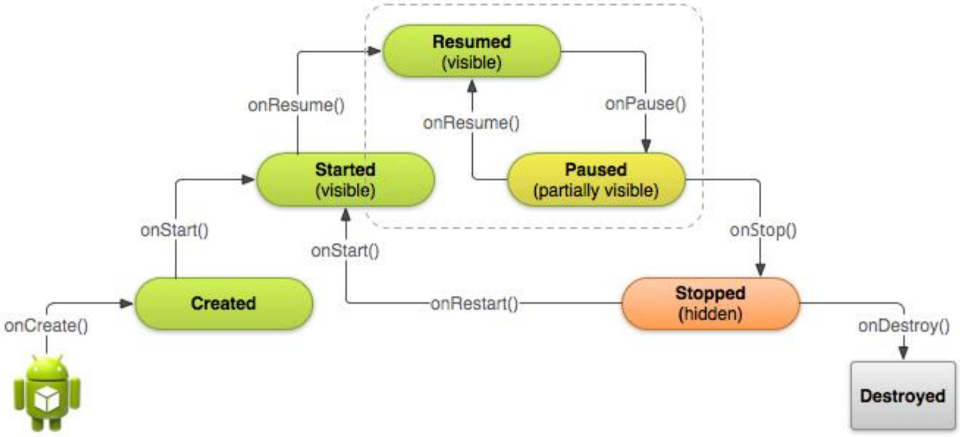


Figure 8-1: Android application life cycle (Android Developers, 2014)

The application was tested for interruption due to the following:

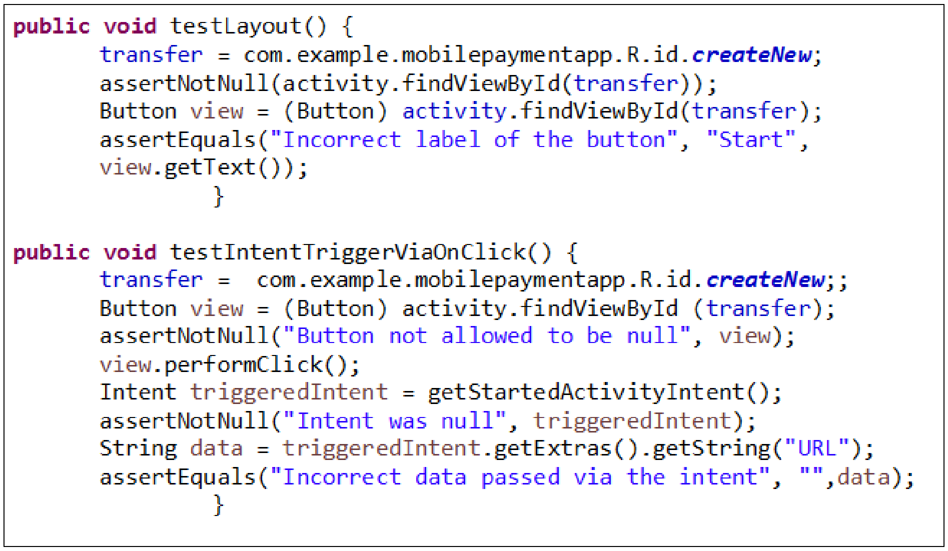
- Incoming SMS and MMS – receiving SMS or MMS when the application was running had no effect on the application, the application continued to run normally because the application remained on the foreground.
- Incoming calls – When a call was received during a transaction, the activity was paused as discussed in the previous chapter. In the case of account creation service, money transfer service or the m-payment service if the outcome of the transaction was received during the interruption, it was displayed when the application resumed. NFC technology only works when the application is open on the screen; the transaction was aborted if a call came before a message was beamed. The transaction had to be carried out again after the interruption.
- Incoming Notifications – incoming notifications had no effect on the application because the application remained on the foreground.
- Media Player on/off – media had no effect on both the money transfer service and m-payment service.

8.3 Unit Testing: Button Testing

During implementation the Android testing was used to test each functional part of the system. JUnit 3 was used to test the application because JUnit 4 is not supported for Android testing. The following were tested using the Android test unit:

- Activity life cycle - this tested the how the activity classes were handling the Android life cycle with different configurations.
- File system: The customer account number was stored on the device so we also tested the write and read access from and to the file.

A test activity class was created for each button during the implementation of the button to avoid having to install the application on the device for testing the behaviour of the button.



```
public void testLayout() {
        transfer = com.example.mobilepaymentapp.R.id.createNew;
        assertNotNull(activity.findViewById(transfer));
        Button view = (Button) activity.findViewById(transfer);
        assertEquals("Incorrect label of the button", "Start",
        view.getText());
                }

public void testIntentTriggerViaOnClick() {
        transfer =  com.example.mobilepaymentapp.R.id.createNew;;
        Button view = (Button) activity.findViewById (transfer);
        assertNotNull("Button not allowed to be null", view);
        view.performClick();
        Intent triggeredIntent = getStartedActivityIntent();
        assertNotNull("Intent was null", triggeredIntent);
        String data = triggeredIntent.getExtras().getString("URL");
        assertEquals("Incorrect data passed via the intent", "",data);
                }
```

Listing 7: Button testing

8.3.1 Hybrid device testing

The testing included testing the application on different emulated devices and also different real devices that run on the Android operating system. Testing on the emulated devices was limited in that the emulated devices cannot fully utilize the NFC technology. Since no open source NFC simulator could be found, testing of the NFC functionality was manually. This testing also included testing the application on different versions of the operating system.

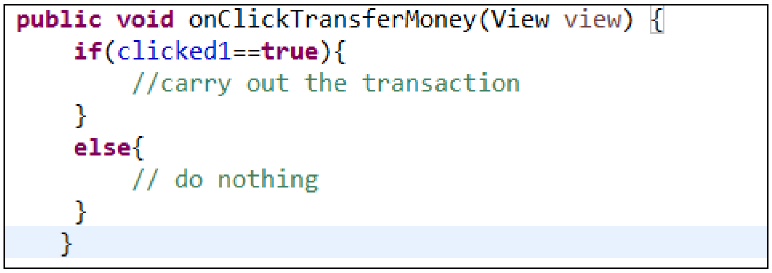
- Emulated devices
- Real device

8.3.1.1Real Device Testing

The application was tested on the following devices: Samsung Galaxy S4, Samsung Galaxy S3, Samsung Galaxy FAME, HTC amaze 4G and Sony Xperia S. The behaviour of the application was normal on all the other devices except for the Samsung Galaxy S3. The Galaxy S3 sometimes had problems receiving a beam from the reader. The problem was solved by closing the application and opening it again.

8.3.1.2 Application Behaviour testing

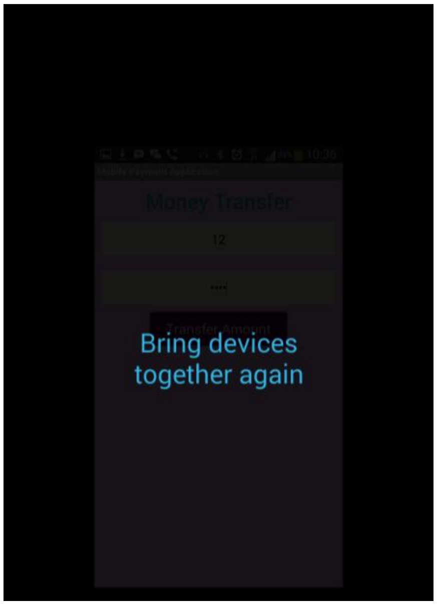
- Multiple pressing of buttons – pressing of a button multiple times was handled by keeping a Boolean variable that controls the execution of the code connected to the button as shown in Listing 8. The code will only be executed when the variable is true. The variable is made false the first time that the user presses a button until the request has been processes and feedback received.



```
public void onClickTransferMoney(View view) {
    if(clicked1==true){
        //carry out the transaction
    }
    else{
        // do nothing
    }
   }
```

Listing 8: Handling multiple pressing of a button

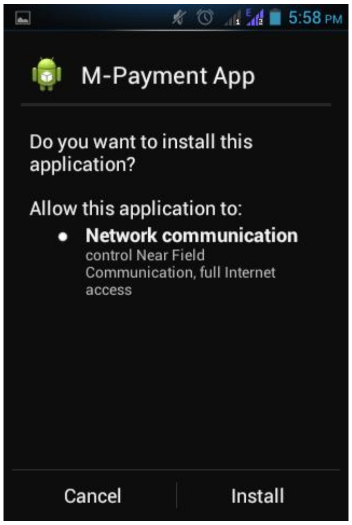
- Device moved before receiving the beamed message – when the devices are moved apart before the message has been beamed, the message shown in Figure 8-2 was displayed for about five seconds before the transaction is aborted.



Bring devices together again

Figure 8-2: Devices moved before message was received by the receiving device

- When the mobile device lacks required setup or technology – to test the behaviour of the application when the device lacked NFC, a GTEL A704_INSPIRE_X with Android OS 4.0.4 was used. The application alerted the user about the requirement of NFC using the message displayed in Figure 8-3. When the user continued with the installation the application was installed successfully (Figure 8-4) even though the requirement for NFC statement was added to the manifest file. When an attempt was made to start the application it crashed and displayed the message shown in Figure 8-5.



5:58 PM

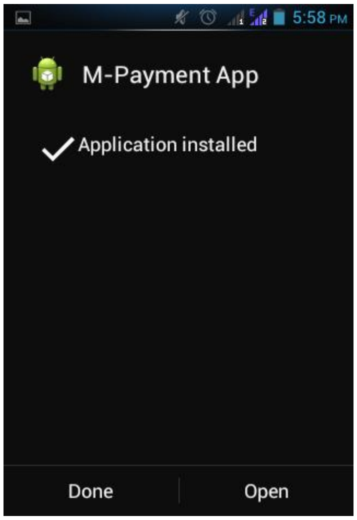
M-Payment App

Do you want to install this application?

Allow this application to:

- **Network communication**
  control Near Field Communication, full Internet access

Figure 8-3: Message displayed before installation begun

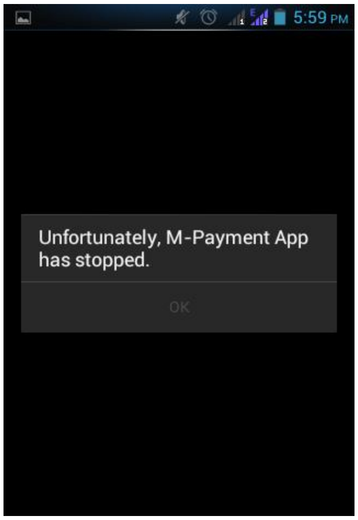


5:58 PM

M-Payment App

✓ Application installed

Figure 8-4: Message display after installation

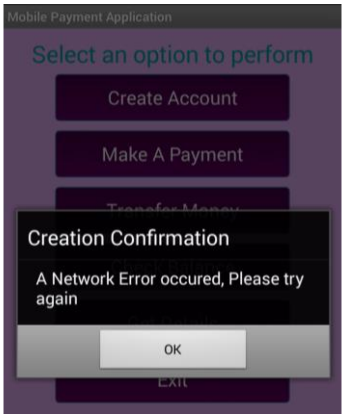


5:59 PM

Unfortunately, M-Payment App has stopped.

Figure 8-5: Message displayed when the user opened the application

- Trying to carry out a transaction without network coverage – during implementation the network error was handled in the application. The message shown in Figure 8-6 was displayed when there was no network coverage.



Mobile Payment Application

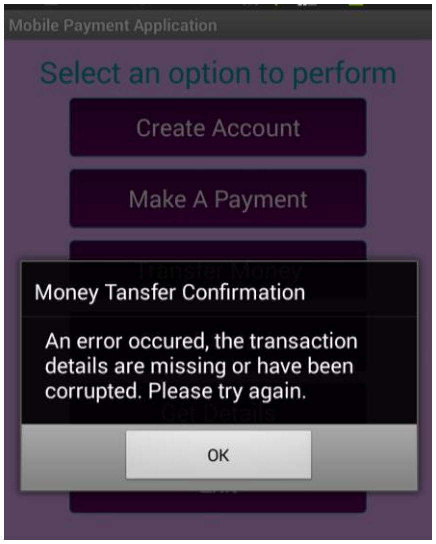
Select an option to perform

Creation Confirmation

A Network Error occured, Please try again

Figure 8-6: Network error message

- When a null or default message is beamed – this was handled by preventing the `processIntent` method from executing when the received messages was null and the message shown in Figure 8-7 was displayed for the money transfer service.



Money Tansfer Confirmation

An error occured, the transaction details are missing or have been corrupted. Please try again.

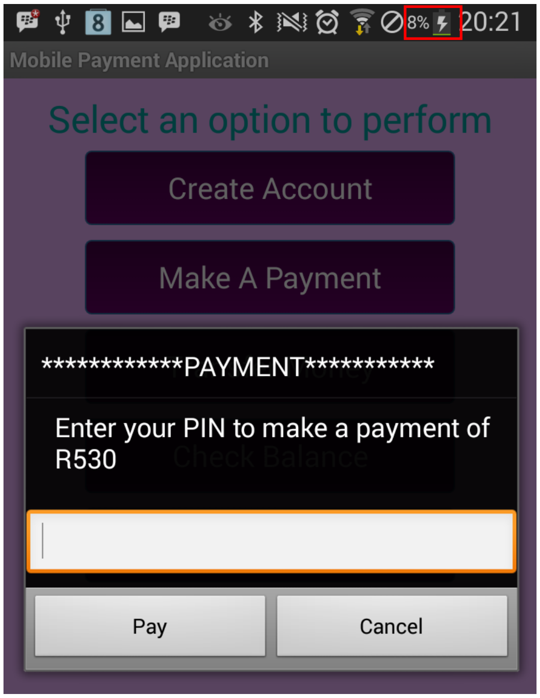
Figure 8-7: Error message when a null or corrupted message is received during a beam

- Beaming a single message multiple times before the received requested is honoured – this was handled the same way as the pressing of the button multiple times. When a beamed message was received an alert dialog was used to notify the user and request for the user's permission to process the transaction. Until the first message that was received was processed and the user notified, all the other beamed messages were ignored.

8.4 Performance Testing

Performance Testing tests performance and behaviour of the application in different conditions which includes low battery, when more than one NFC enabled mobile devices was in close proximity to the reader and battery usage. During performance testing the user interface was also tested for responsiveness. The time it took to complete a transaction was also tested.

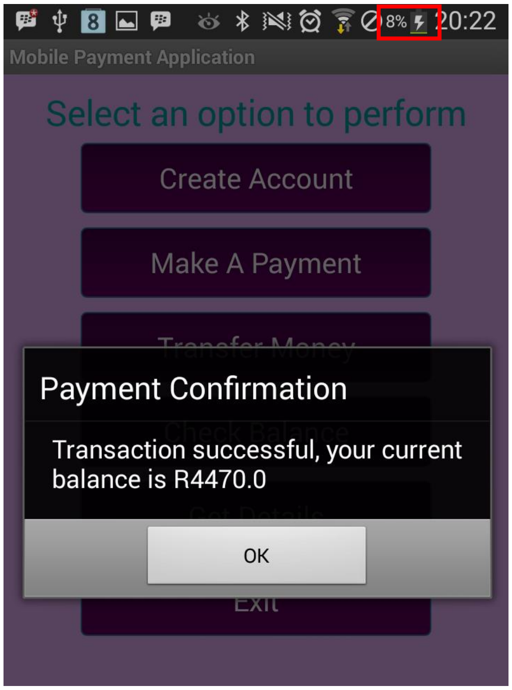
- Low Battery – The Android operating system kill the activities with low priorities when the battery is low, therefore we also tested the operation of the application when the battery was low. The application worked even when the battery was low as long as the device was still on. Figure 8-8 shows that m-payment application received payment details from the reader even though the device's battery was only 8 per cent (highlighted by a red box). After the user entered the PIN and accepted the payment, the details were processed and sent to the banking system and the confirmation was returned as shown in Figure 8-9.



************PAYMENT***********

Enter your PIN to make a payment of R530

Figure 8-8: Request for acceptance of a payment when the battery was low

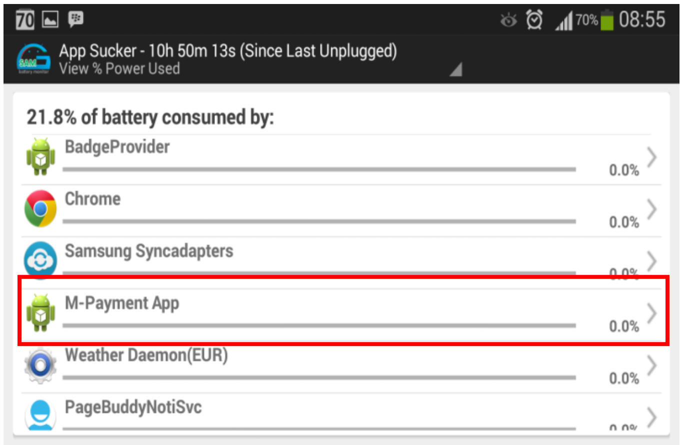


Payment Confirmation

Transaction successful, your current balance is R4470.0

Figure 8-9: Payment confirmation when the battery was low

- As mentioned before, NFC does not support broadcast of information. When more than one mobile device was close to the reader, the reader either established a connection with one device or did not send the payment information.
- Battery usage – Users are always concerned with the battery usage of their mobile devices, hence we also tested the battery consumption of the application. The application only uses battery when it is running. Figure 8-10 shows that the application was not consuming battery since the last time that the device had been charge. Figure 8-11 shows the amount of battery that the application had consumed after carrying out a single money transfer transaction and a single m-payment transaction. The m-payment application is highlighted in red.



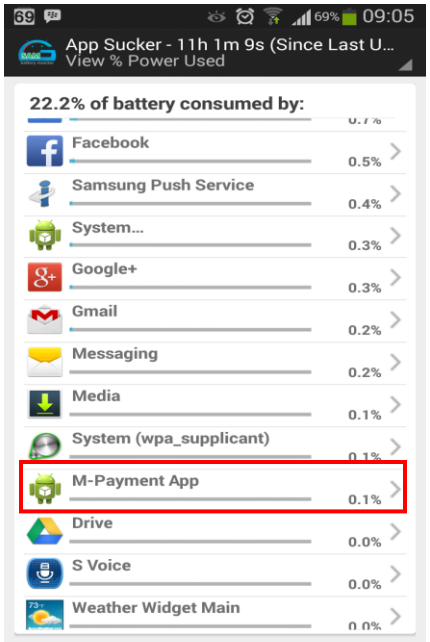
70% 08:55

App Sucker - 10h 50m 13s (Since Last Unplugged)
View % Power Used

21.8% of battery consumed by:

BadgeProvider	0.0%
Chrome	0.0%
Samsung Syncadapters	0.0%
M-Payment App	0.0%
Weather Daemon(EUR)	0.0%
PageBuddyNotiSvc	0.0%

Figure 8-10: Battery usage when the m-payment was not in use



69% 09:05

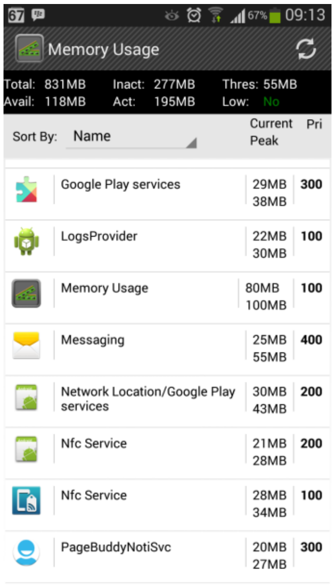
App Sucker - 11h 1m 9s (Since Last U...
View % Power Used

22.2% of battery consumed by:

Facebook	0.5%
Samsung Push Service	0.4%
System...	0.3%
Google+	0.3%
Gmail	0.2%
Messaging	0.2%
Media	0.1%
System (wpa_supplicant)	0.1%
M-Payment App	0.1%
Drive	0.0%
S Voice	0.0%
Weather Widget Main	0.0%

Figure 8-11: Battery Usage after performing a few transactions

- Memory Usage – When the application was exited from it stopped consuming the CPU as shown by its absence in Figure 8-12. When it was launched it appeared in the list of the applications that were consuming CPU and its CPU consumption is 36MB as shown in Figure 8-13 by a red box. Figure 8-14 shows the CPU usage sorted by name. The m-payment application is highlighted in red. The user has to exit from the application when it is not in use to prevent excessive memory use. But compared to other application, the m-payment application CPU usage is normal.

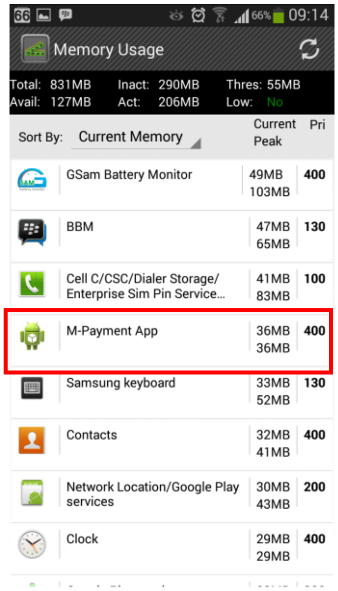


Total: 831MB Inact: 277MB Thres: 55MB
Avail: 118MB Act: 195MB Low: No

Sort By: Name

	Current Peak	Pri
Google Play services	29MB 38MB	300
LogsProvider	22MB 30MB	100
Memory Usage	80MB 100MB	100
Messaging	25MB 55MB	400
Network Location/Google Play services	30MB 43MB	200
Nfc Service	21MB 28MB	200
Nfc Service	28MB 34MB	100
PageBuddyNotiSvc	20MB 27MB	300

Figure 8-12: Memory Usage Before the M-payment was launched sorted by name

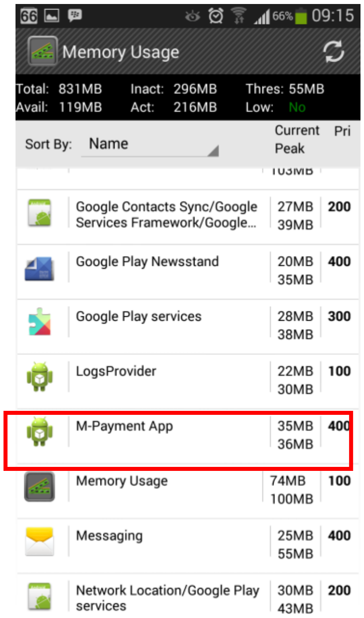


Total: 831MB Inact: 290MB Thres: 55MB
Avail: 127MB Act: 206MB Low: No

Sort By: Current Memory

	Current Peak	Pri
GSam Battery Monitor	49MB 103MB	400
BBM	47MB 65MB	130
Cell C/CSC/Dialer Storage/ Enterprise Sim Pin Service…	41MB 83MB	100
M-Payment App	36MB 36MB	400
Samsung keyboard	33MB 52MB	130
Contacts	32MB 41MB	400
Network Location/Google Play services	30MB 43MB	200
Clock	29MB 29MB	400

Figure 8-13: Memory usage sorted by current memory usage after launching the application



Total: 831MB Inact: 296MB Thres: 55MB
Avail: 119MB Act: 216MB Low: No

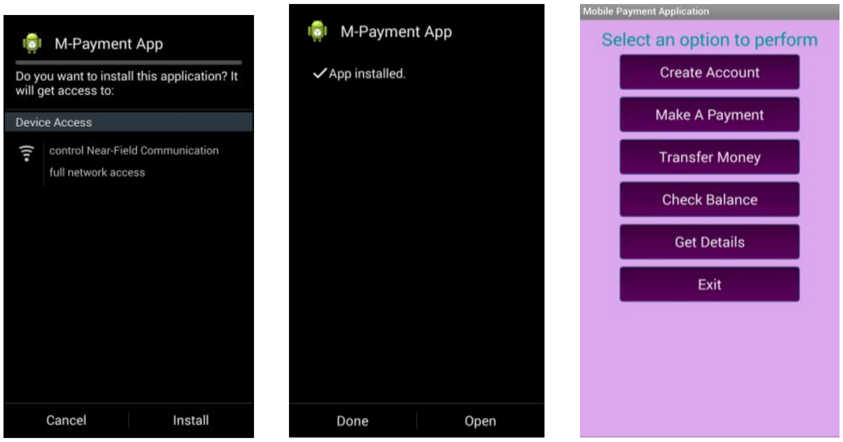
Sort By: Name

	Current Peak	Pri
Google Contacts Sync/Google Services Framework/Google…	27MB 39MB	200
Google Play Newsstand	20MB 35MB	400
Google Play services	28MB 38MB	300
LogsProvider	22MB 30MB	100
M-Payment App	35MB 36MB	400
Memory Usage	74MB 100MB	100
Messaging	25MB 55MB	400
Network Location/Google Play services	30MB 43MB	200

Figure 8-14: Memory usage sorted by name

8.5 Installation Testing

Figure 8-15 shows the screens that were displayed during installation in their correct order. Both the installation and un-installation process of the application were tested. Installation testing verifies that the installation process goes smoothly without any difficulty. The installation was tested on Samsung Galaxy S4, Samsung Galaxy S3, Samsung Galaxy FAME, HTC amaze 4G and Sony Xperia S. In all these instances the installation went smoothly.


M-Payment App

Do you want to install this application? It will get access to:

Device Access

control Near-Field Communication

full network access

M-Payment App

✓App installed.

Mobile Payment Application

Select an option to perform

Figure 8-15: Installation on NFC enabled device

8.6 Compatibility Testing

Compatibility of the application was also tested. We tested both the mobile platform compatibility and device model compatibility. This included testing on different versions of the operating system, starting with version 14 going upwards.

8.7 Usability Testing

The purpose of usability is to verify if the application is usable and if it meets the user requirements. In our case the application was tested by participants form the marginalized rural area. Usability testing measures the user experience after using or experimenting with the application. It is of great importance to note that usability is concerned mainly with finding flaws in the application. According to ISO 9241-11 (ISO/IEC 9241-11, 1998):

- "Usability is the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"
- "Effectiveness is the accuracy and completeness with which users achieve specified goals"
- "Efficiency is the resources expended in relation to the accuracy and completeness with which users achieve goals"
- "Satisfaction the comfort and acceptability of use"

ISO/IEC 9126-1 defined usability as the capability of a system to be understood, learned, used and attractive to the user when used according to its specified conditions. For our usability testing, we used different types of participants:

- Participants who never used a smartphone before
- Participants who used smartphones that run on an operating systems other than Android
- Participants who own or had once owned an Android smartphone

For each group we had 4 participants. For testing the usability, the framework in Figure 8-16 was used. We did not take into consideration the effectiveness because whatever error the participant made was insignificant. This was because:

- all the participants had used a mobile device before

- The interface of the application was very simple and it restricts the user input to be numbers only for both the amount and the PIN number.

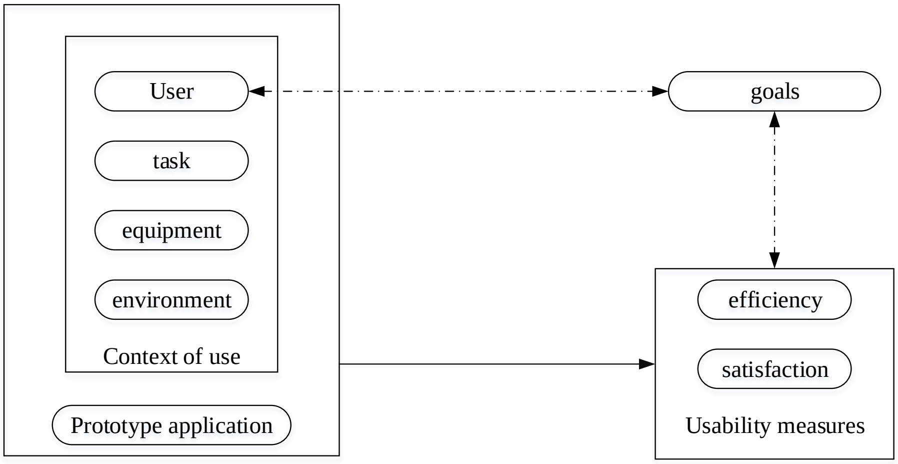


Figure 8-16: Usability framework (Bevan, 1995)

The main focus for usability testing for this research was transferring money using the money transfer service and making a payment using the money payment service. The main goals are:

- Money transfer
- M-payment

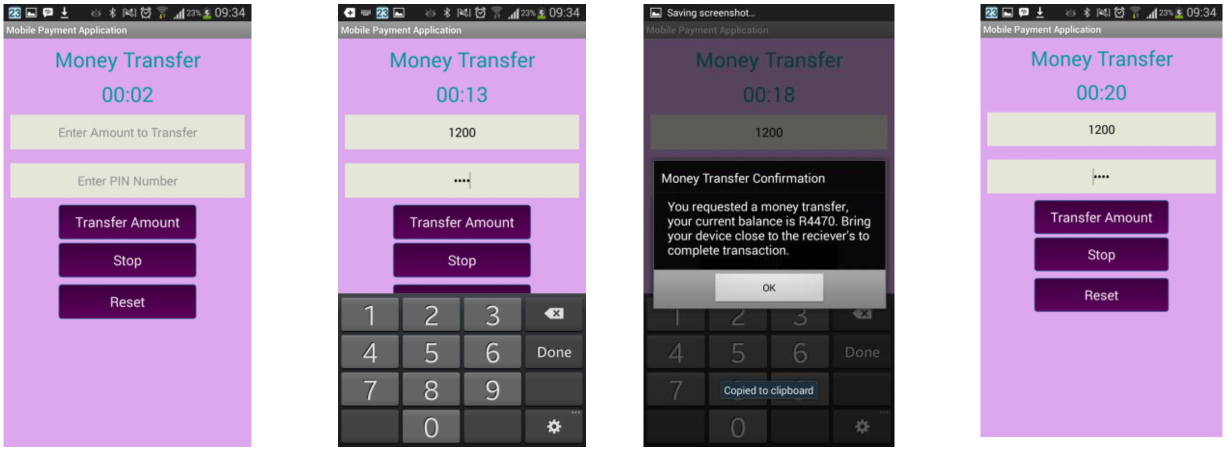
8.7.1 Efficiency measuring for Money Transfer

The goal of this section was for the participants to transfer money to each other. The participants were grouped as shown in Table 12.

Table 12: Groups of participants

	Participant1	Participant2
Group A	Never used a smartphone	Never used a smartphone
Group B	Never used a smartphone	Uses a smartphone other than an Android smartphone
Group C	Never used a smartphone	Uses an Android smartphone
Group D	Uses a smartphone other than an Android smartphone	Uses a smartphone other than an Android smartphone
Group E	Uses an Android smartphone	Uses a smartphone other than an Android smartphone
Group F	Uses an Android smartphone	Uses an Android smartphone

The efficiency was measured in seconds using the time the participant took to transfer money. The application was modified so that it included a stop watch which was used to measure the time taken. Figure 8-17 shows the screens that were displayed during efficiency testing.



Money Transfer Confirmation

You requested a money transfer, your current balance is R4470. Bring your device close to the reciever's to complete transaction.

Figure 8-17: Money Transfer Screens For Usability Testing

The timer was automatically started when the user selected the ‘Transfer Money’ button on the main screen and it was automatically stopped when the sender had successfully beamed the message to the receiver. Table 13 shows the time that was taken by each user to transfer the money.

Table 13: Time taken by participants

	Participant1 (Time in seconds)	Participant2 (Time in seconds)
Group A	22	19
Group B	26	21
Group C	23	17
Group D	24	25
Group E	18	20
Group F	20	24

Figure 8-18 shows the graphical representation of the performance of each participant according to their groups. The time taken by each participant varied from 18 seconds to 26 seconds, which has an 8 second difference.

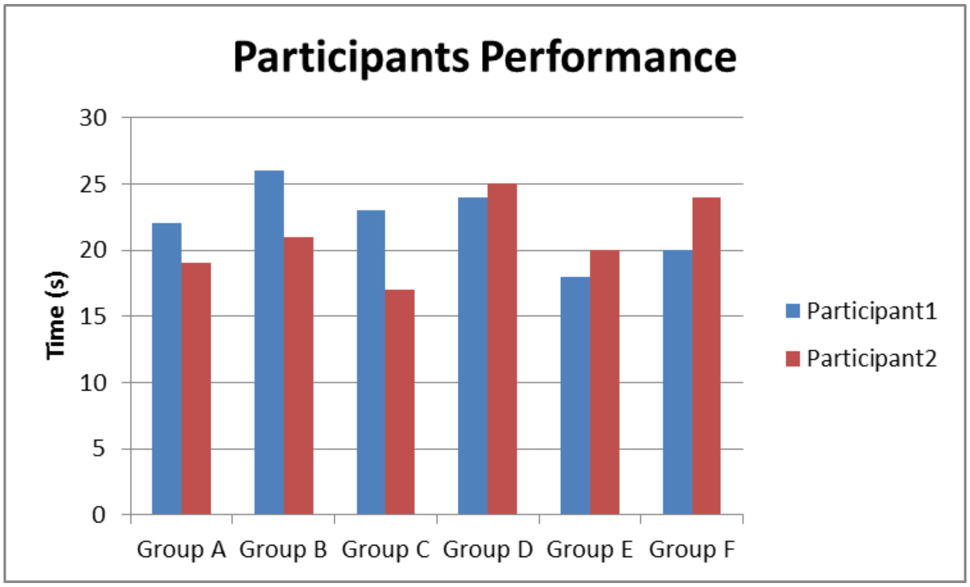
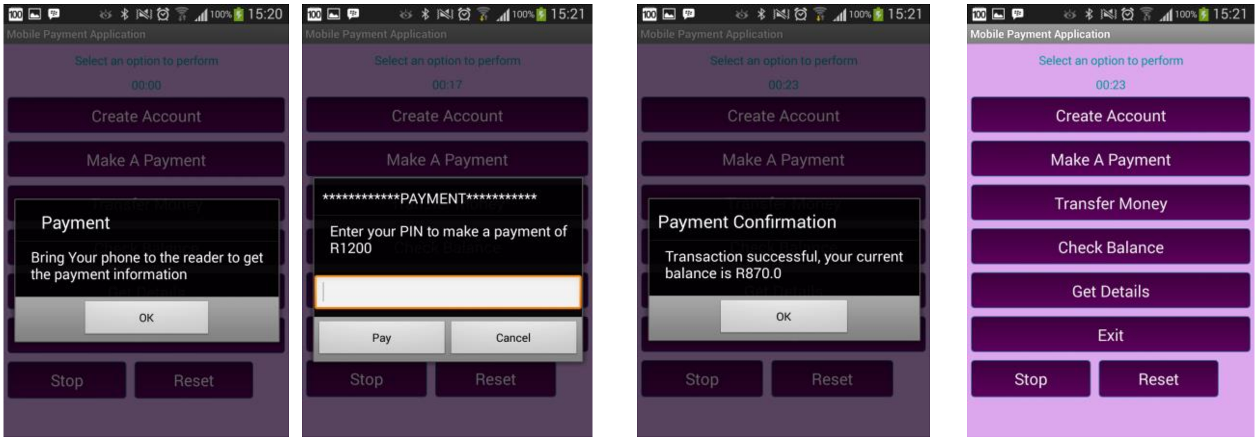


Figure 8-18: Participants performance

The standard deviation of the time taken by the participants to complete the transaction was 2.8s. This means that the time taken by the participants were on average approximately 3 seconds away from the mean. This shows that there is little difference among all the time taken by the participants. The time taken to make a payment using a credit card ranges from 22 seconds to 30 seconds (McElligott, 2007; Agnieszka Zmijewska, Lawrence, & Steele, 2007). The average time of making an m-payment takes approximately 45 seconds (Agnieszka Zmijewska et al., 2007). Taking these approximations into consideration, the prototype payment application was efficient. Hence for transferring money, we concluded that the application was efficient. It should be noted that none of the participants made an error when they were inputting their PIN numbers and that the network utilized in the tests was good.

8.7.2 Efficiency measuring for m-payments

Figure 8-19 shows the screens that were displayed by the application during usability. The main screen was modified in order to accommodate the stop watch, the stop button and the reset button. The timer was started when the user clicked the ‘Make A Payment’ button and it stopped when the payment confirmation was received.


Payment

Bring Your phone to the reader to get the payment information

************PAYMENT***********

Enter your PIN to make a payment of R1200

Payment Confirmation

Transaction successful, your current balance is R870.0

Figure 8-19: M-payment Service Screens for Usability Testing

The steps for making a payment are more or less the same with the steps for transferring money. After collecting the results for making an m-payment, we discovered that the time the participants took were almost the same as the time they took for transferring money, therefore we also concluded that the application was efficient for making m-payments.

8.7.3 Usability measuring using the System Usability Scale (SUS)

The SUS is a simple ten-item scale used to give an overall view of usability of a system (Brooke, 2013). The SUS is based on the Likert scale, for our testing we used the 5-point scale. The participants had to first install the application, create a password for the application and open an account. Opening the account included also creating a PIN number for the account. The banking system automatically allocated a balance of R5000 to each participant upon opening an account. The participants tested the application by using all its services to their satisfaction. The participants filled out the SUS questionnaire after they used and experimented with the application. The SUS score is calculated as follows (Sauro, 2014):

- Subtract one from the user’s response if the item is odd-numbered.
- Subtract the user’s responses from 5 if the item is even numbered.
- To get the SUS score, add the converted responses for each user and multiply that total by 2.5. This gives a total that is between 0 and 100 for each user.

Table 14 shows the score of each participant.

Table 14: SUS scoring for the participants

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SCORE
Participant1	4	4	4	4	4	4	0	4	3	3	85
Participant2	4	3	3	4	2	3	3	3	2	4	77.5
Participant3	3	3	4	4	4	4	2	4	4	3	87.5
Participant4	4	3	3	4	4	4	2	3	2	3	80
Participant5	3	3	3	4	2	4	4	3	4	3	82.5
Participant6	4	3	4	3	4	4	3	3	2	4	85
Participant7	3	2	4	4	3	2	3	4	4	1	75
Participant8	4	4	4	4	4	4	2	4	4	4	95
Participant9	3	3	4	4	3	4	3	3	2	1	75
Participant10	3	3	4	4	4	4	1	4	3	4	85
Participant11	3	3	2	4	4	3	2	4	4	4	82.5
Participant12	3	4	3	3	3	4	3	4	3	3	82.5
									Average Score		82.70833
	🟩	Positive response									
	🟨	Neutral Response									
	🟥	Negative Response									

According to a research done by Bangor et al products that had a SUS score in the 90s was an exceptional product, those in the 80s were good while those in the 70s had usability issues (Bangor, Kortum, & Miller, 2009). Based on the SUS scale our application was usable because the average SUS score for all the users was 82.7.

Participants Score comparison

In this section, the participants were grouped into three groups according to their experience using an Android smartphone as follows:

- Group A – participants who have never used a smart phone
- Group B – participants who used smartphones other than Android smartphones
- Group C – participants who used Android smartphones

The participants were grouped according to these groups so that the SUS score for each group would be measured. Table 15 shows the average score for each group.

Table 15: SUS scores for each group

Group	Average SUS Score
Group A	82.5
Group B	84.375
Group C	81.25

There is a little difference among the average scores as they are ranging between 81 and 84. The experience of participants on using smartphones did not affect their score. The participants who have never used a smart score had a SUS score that is higher than that of participants who owns an android smart phone. From these average scores we concluded that the prototype application was usable for all the groups.

8.8 Conclusion

The application testing was conducted before the data collection. Some of the participants who performed the usability testing were also part of the participants in the data collection. The application testing showed that the prototype application met the functional requirements defined in Chapter 7 and also showed that the application was compatible with different types of Android devices. The only problem that we encountered with the application was that it installed on some devices that did not have the NFC hardware. Usability testing showed that the application as usable and that the participants did not need any prior training to use the application.

9 DATA ANALYSIS AND RESULTS FOR THE TAM

9.1 Introduction

Various literatures on TAM were reviewed in order to ensure that a comprehensive list of measurement items was catered for. The measurement items of *perceived ease of use* and *perceived usefulness* were constructed directly from the TAM. The questionnaire we used to collect data consisted of three sections: the demographic section, banking information section and the TAM measurements section (see APPENDIX C – Questionnaire). Structural Equation Modelling (SEM) was used to analyse data. The survey questions were developed using the Likert scale approach.

9.2 Participants

One of the objectives of this research was to explore the user acceptance of NFC enabled m-payments. As mentioned in Chapter 1, the research was focused on the consumers staying in the rural areas with an age range of 16 and above. The number of participants that managed to fill and return the questionnaire was 79 but two of them were spoiled and could not be used in the data analysis. All the subjects were users of mobile devices but most of their devices were not NFC enabled. All the subjects were exposed to the NFC enabled m-payment prototype application before they were given the questionnaires.

9.3 Data Analysis and Results

This chapter focuses on data analysis for the TAM in order to scientifically determine the user acceptance of the technology. The SEM was used to validate the research model discussed in Chapter 6. SEM uses both multiple regression and factor analysis during model validation. The SEM consists of two parts: measurement model and the structural measurements. The measurement model defines the relationship between the measure variables and the latent variables. The structural model describes the relationships among the latent variables. As was shown in Chapter 6, most of the measurements were taken from reliable and proven items. The research model was analysed using the WarpPLS4.0. WarpPLS4.0 is a statistical tool that is based on Partial Least Squares (PLS). Both the reflective and the formative scales are accommodated by PLS. One of the reasons we chose PLS was because our sample size was small and according to Chin et al. this is acceptable for PLS (Chin, Marcolin, & Newsted, 2003). Table 16 shows the demographic information of the participants.

Table 16: Demographic attributes of participants

	Frequency	Percentage
Gender		
Female	47	61.04
Male	30	38.96
Age		
16 – 29	40	51.95
30 – 49	30	38.96
50 and above	7	9.09
Education Level		
Below grade 12	23	29.87
Grade 12 and above	54	70.13

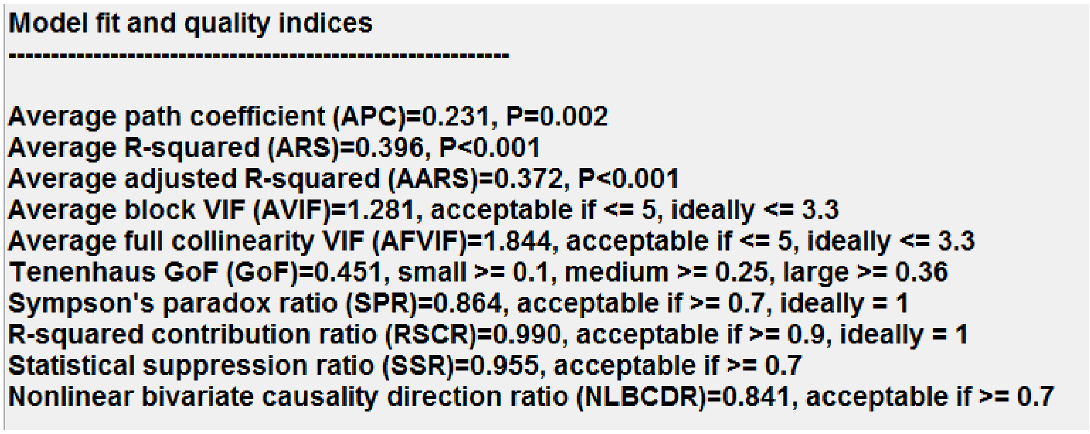
Table 17 gives the latent variable names that were used in this data analysis.

Table 17: Latent Variable names

Latent Variable	Latent Variable Name
Perceived risk	risk
Trust	trust
Perceived Security	security
Perceived ease of use	ease
Perceived usefulness	useful
Prototype application	prototyp
Relative advantage	advant
Attitude towards using	attitude
Intention to use	intentio

9.3.1 Measurement Model and Structural Models

Both the measurement model and the structural model were evaluated using warpPLS. The requirement for evaluating the model fit is that both values of P for Average Path Coefficient (APC) and Average R-Squared (ARS) must be lower than .05. The warpPLS software pre-processes the data automatically before SEM analysis.



```
Model fit and quality indices
----------------------------------------------------------

Average path coefficient (APC)=0.231, P=0.002
Average R-squared (ARS)=0.396, P<0.001
Average adjusted R-squared (AARS)=0.372, P<0.001
Average block VIF (AVIF)=1.281, acceptable if <= 5, ideally <= 3.3
Average full collinearity VIF (AFVIF)=1.844, acceptable if <= 5, ideally <= 3.3
Tenenhaus GoF (GoF)=0.451, small >= 0.1, medium >= 0.25, large >= 0.36
Sympson's paradox ratio (SPR)=0.864, acceptable if >= 0.7, ideally = 1
R-squared contribution ratio (RSCR)=0.990, acceptable if >= 0.9, ideally = 1
Statistical suppression ratio (SSR)=0.955, acceptable if >= 0.7
Nonlinear bivariate causality direction ratio (NLBCDR)=0.841, acceptable if >= 0.7
```

Figure 9-1: Model fit and quality indices

Figure 9-1 shows the values for model fit and the quality indices. The requirement for a model fit is that both Average block Variance Factor (AVIF) and Average Full collinearity Variance Inflation Factor (AFVIF) should be equal to or less than 3.3. In Figure 9-1 the Statistical Suppression Ratio (SSR) of 0.995 means that the paths in the model are 95.5%% free from statistical suppression. Nonlinear Bivariate Causality Direction Ratio (NLBCDR) of 0.841 means that in our research model the support for the reversed hypothesized direction of causality is weak or less for almost all the paths in the model. Therefore the research model fits all the criteria requirements for model fit. This means that the model represents the data well, has good exploratory fit and can be used to predict the data well.

In PLS based SEM analysis the path coefficients are also known as the beta coefficients. Figure 9-2 shows the values for these coefficients. Most of the hypotheses were supported except for H_2, H_7, H_8, H_{11}, $H_{13,}$ H_{18} and H_{17} as shown in Figure 9-2 by their P values which are greater than .05. For the hypothesis to be acceptable its paths must have a P value of <.05.

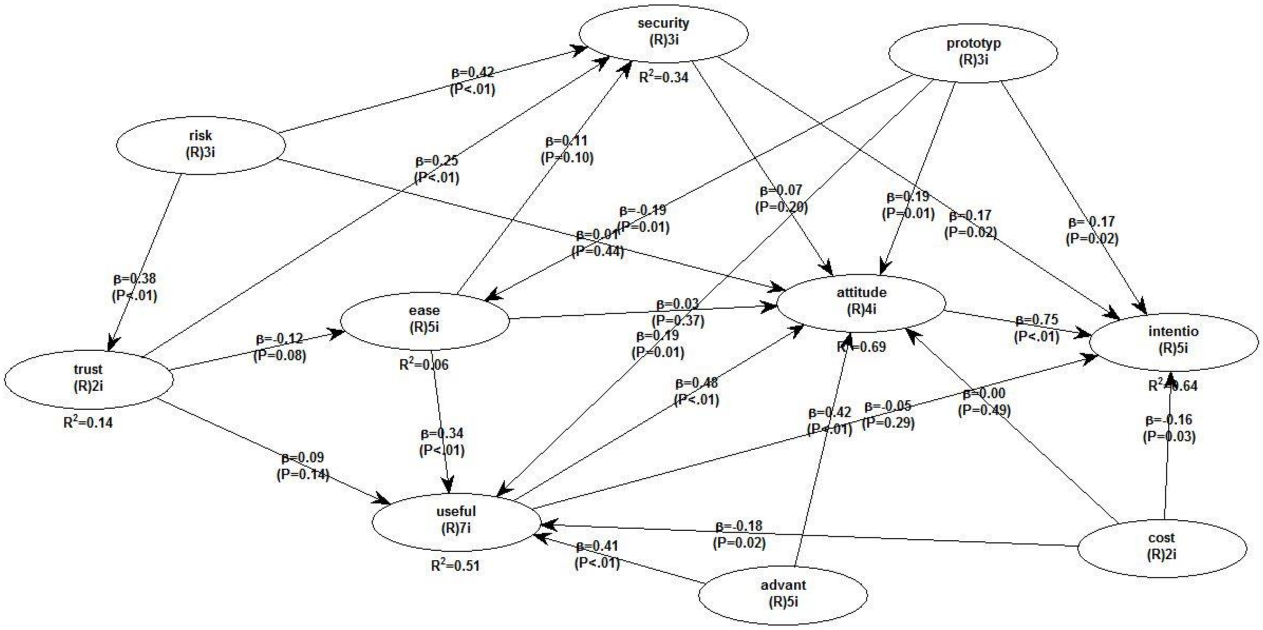


Figure 9-2: Research Model with estimated values

Figure 9-2 shows that:

- *Perceived ease of use* has an insignificant effect on *attitude towards use* and this made hypothesis H_7 to be rejected (β = 0.03 and P = 0.37).
- *Perceived usefulness* is an important antecedent of *attitude towards use* with β = 0.48 and P<.01 together with *relative advantage* with β =0.42 and p<.01.
- 14% of *trust* is determined by *perceived risk* (R^2 = 0.14). Trust does not have a direct effect on both *attitude towards use* and *intention to use* but it directly affects perceived security with β = 0.25 and P <.01.
- 34% of *perceived security* is determined by *perceived risk* and *trust* (R^2 = 0.34). Perceived risk has the strongest effect on security with β = 0.42
- 69% of *attitude towards use* is determined by *relative advantage*, *perceived usefulness*, *prototype application*, and *perceived cost.*
- 51% of *perceived usefulness* is determined by *perceived ease of use*, *prototype application*, *perceived cost* and *relative advantage;* with *relative advantage* being the most important antecedent with β = 0.41 with P<.01. *Perceived cost* has a negative effect on perceived usefulness with β = -0.18.
- 64% of *intention to use* NFC enabled m-payments is determined by *perceived cost attitude towards use, perceived security* and *prototype application*. *Perceived cost* has a negative effect on intention to use with β = -0.16

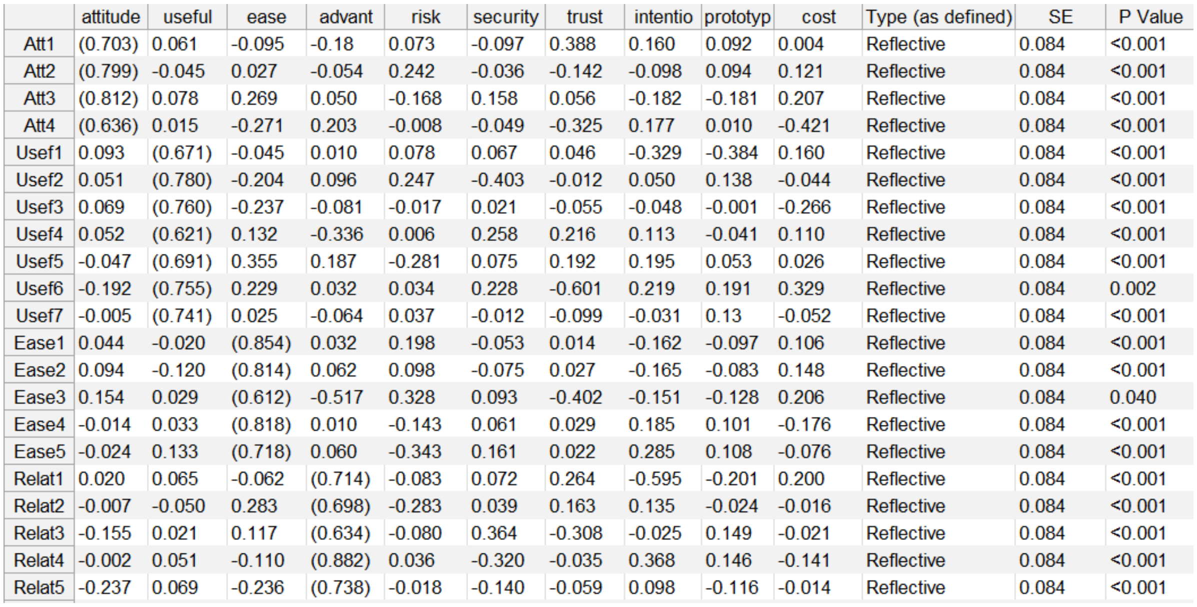
The results in Figure 9-2 shows that H_1 has a direct significant effect on the *intention to us*e with $\beta = 0.75$ and $P<.01$. This means that the participants' *attitude towards* NFC enabled m-payment is an important determinant of the intention by the participants to use the system. Table 18 shows the outcome of the hypotheses.

Table 18: Outcomes of the Hypotheses

Hypotheses	Outcome
H_1: *Attitude towards using* NFC enabled m-payments has direct effect on *intention to use* NFC enabled m-payments.	Accepted
H_2: Perceived usefulness of NFC enabled m-payments has direct effect on *intention to use* NFC enabled m-payments.	Rejected
H_3: *Relative advantage* of NFC enabled m-payments has direct effect on *attitude towards using* NFC enabled m-payments.	Accepted
H_4: *Relative advantage* of NFC enabled m-payments has direct effect on *perceived usefulness* of using NFC enabled m-payments.	Accepted
H_5: *Perceived usefulness* of NFC enabled m-payments has direct effect on *attitude towards using* NFC enabled m-payments.	Accepted
H_6: *Perceived ease of use* of NFC enabled m-payments has direct effect on *perceived usefulness* of NFC enabled m-payments.	Accepted
H_7: *Perceived ease of use* of NFC enabled m-payments has direct effect on *attitude towards using* NFC enabled m-payments	Rejected
H_8: *Perceived risk* of using NFC enabled m-payments has direct effect on the *attitude towards use* of NFC enabled m-payments.	Rejected
H_9: *Perceived risk* of using NFC enabled m-payments has direct effect on the *trust* of using NFC enabled m-payments.	Accepted
H_{10}: *Perceived risk* of using NFC enabled m-payments has direct effect on the *perceived security* of using NFC enabled m-payments.	Accepted
H_{11}: *Perceived Security* of using NFC enabled m-payments has direct effect on the *attitude towards* of using NFC enabled m-payments.	Rejected
H_{12}: *Perceived Security* of using NFC enabled m-payments has direct effect on the *intention of use* of using NFC enabled m-payments.	Accepted
H_{13}: *Perceived Cost* of using NFC enabled m-payments has direct effect on the *attitude towards* of using NFC enabled m-payments.	Rejected
H_{14}: *Perceived Cost* of using NFC enabled m-payments has direct effect on the *perceived usefulness* of using NFC enabled m-payments.	Accepted
H_{15}: *Perceived Cost* of using NFC enabled m-payments has direct effect on the *intention* of using NFC enabled m-payments.	Accepted
H_{16}: *Trust* on NFC enabled m-payments has direct effect on the *perceived security* of using NFC enabled m-payments.	Accepted
H_{17}: *Trust* on NFC enabled m-payments has direct effect on the *perceived ease of use* of using NFC enabled m-payments.	Rejected
H_{18}: *Trust* on NFC enabled m-payments has direct effect on the *perceived usefulness* of using NFC enabled m-payments.	Rejected
H_{19}: *Prototype application* has a direct effect on the *perceived ease of use* of using NFC enabled m-payments.	Accepted
H_{20}: *Prototype application* has a direct effect on the *perceived usefulness* of using NFC enabled m-payments.	Accepted
H_{21}: *Prototype application* has a direct effect on the *intention to use* NFC enabled m-payments.	Accepted

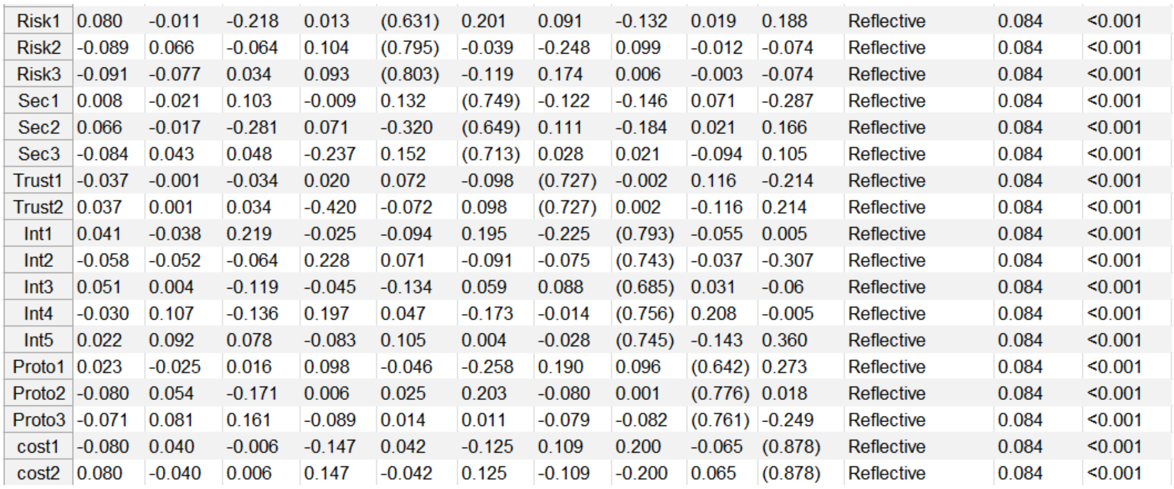
H_{22}: *Prototype application* has a direct effect on the *attitude towards use* of NFC enabled m-payments.	Accepted

The convergent validity and reliability of the model was also evaluated by examining the factor loading, Average Variance Extracted (AVE) and Cronbach's alpha. Figure 9-3 and Figure 9-4 shows that all factor loading are more than 0.5 with a P value of at most 0.04 which is acceptable. There are no crossing loading above 0.5, therefore the model has good discriminant validity. All the measurement items are reflective because they affect the latent variable.



	attitude	useful	ease	advant	risk	security	trust	intentio	prototyp	cost	Type (as defined)	SE	P Value
Att1	(0.703)	0.061	-0.095	-0.18	0.073	-0.097	0.388	0.160	0.092	0.004	Reflective	0.084	<0.001
Att2	(0.799)	-0.045	0.027	-0.054	0.242	-0.036	-0.142	-0.098	0.094	0.121	Reflective	0.084	<0.001
Att3	(0.812)	0.078	0.269	0.050	-0.168	0.158	0.056	-0.182	-0.181	0.207	Reflective	0.084	<0.001
Att4	(0.636)	0.015	-0.271	0.203	-0.008	-0.049	-0.325	0.177	0.010	-0.421	Reflective	0.084	<0.001
Usef1	0.093	(0.671)	-0.045	0.010	0.078	0.067	0.046	-0.329	-0.384	0.160	Reflective	0.084	<0.001
Usef2	0.051	(0.780)	-0.204	0.096	0.247	-0.403	-0.012	0.050	0.138	-0.044	Reflective	0.084	<0.001
Usef3	0.069	(0.760)	-0.237	-0.081	-0.017	0.021	-0.055	-0.048	-0.001	-0.266	Reflective	0.084	<0.001
Usef4	0.052	(0.621)	0.132	-0.336	0.006	0.258	0.216	0.113	-0.041	0.110	Reflective	0.084	<0.001
Usef5	-0.047	(0.691)	0.355	0.187	-0.281	0.075	0.192	0.195	0.053	0.026	Reflective	0.084	<0.001
Usef6	-0.192	(0.755)	0.229	0.032	0.034	0.228	-0.601	0.219	0.191	0.329	Reflective	0.084	0.002
Usef7	-0.005	(0.741)	0.025	-0.064	0.037	-0.012	-0.099	-0.031	0.13	-0.052	Reflective	0.084	<0.001
Ease1	0.044	-0.020	(0.854)	0.032	0.198	-0.053	0.014	-0.162	-0.097	0.106	Reflective	0.084	<0.001
Ease2	0.094	-0.120	(0.814)	0.062	0.098	-0.075	0.027	-0.165	-0.083	0.148	Reflective	0.084	<0.001
Ease3	0.154	0.029	(0.612)	-0.517	0.328	0.093	-0.402	-0.151	-0.128	0.206	Reflective	0.084	0.040
Ease4	-0.014	0.033	(0.818)	0.010	-0.143	0.061	0.029	0.185	0.101	-0.176	Reflective	0.084	<0.001
Ease5	-0.024	0.133	(0.718)	0.060	-0.343	0.161	0.022	0.285	0.108	-0.076	Reflective	0.084	<0.001
Relat1	0.020	0.065	-0.062	(0.714)	-0.083	0.072	0.264	-0.595	-0.201	0.200	Reflective	0.084	<0.001
Relat2	-0.007	-0.050	0.283	(0.698)	-0.283	0.039	0.163	0.135	-0.024	-0.016	Reflective	0.084	<0.001
Relat3	-0.155	0.021	0.117	(0.634)	-0.080	0.364	-0.308	-0.025	0.149	-0.021	Reflective	0.084	<0.001
Relat4	-0.002	0.051	-0.110	(0.882)	0.036	-0.320	-0.035	0.368	0.146	-0.141	Reflective	0.084	<0.001
Relat5	-0.237	0.069	-0.236	(0.738)	-0.018	-0.140	-0.059	0.098	-0.116	-0.014	Reflective	0.084	<0.001

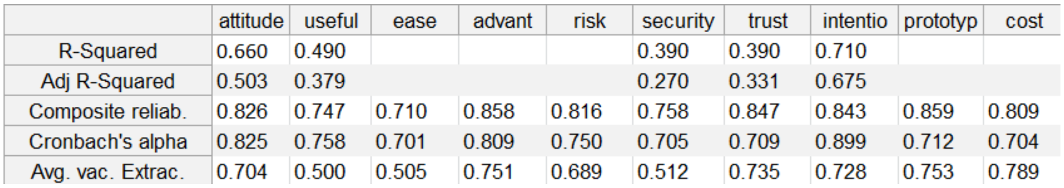
Figure 9-3: Combined loadings and cross-loadings



Risk1	0.080	-0.011	-0.218	0.013	(0.631)	0.201	0.091	-0.132	0.019	0.188	Reflective	0.084	<0.001
Risk2	-0.089	0.066	-0.064	0.104	(0.795)	-0.039	-0.248	0.099	-0.012	-0.074	Reflective	0.084	<0.001
Risk3	-0.091	-0.077	0.034	0.093	(0.803)	-0.119	0.174	0.006	-0.003	-0.074	Reflective	0.084	<0.001
Sec1	0.008	-0.021	0.103	-0.009	0.132	(0.749)	-0.122	-0.146	0.071	-0.287	Reflective	0.084	<0.001
Sec2	0.066	-0.017	-0.281	0.071	-0.320	(0.649)	0.111	-0.184	0.021	0.166	Reflective	0.084	<0.001
Sec3	-0.084	0.043	0.048	-0.237	0.152	(0.713)	0.028	0.021	-0.094	0.105	Reflective	0.084	<0.001
Trust1	-0.037	-0.001	-0.034	0.020	0.072	-0.098	(0.727)	-0.002	0.116	-0.214	Reflective	0.084	<0.001
Trust2	0.037	0.001	0.034	-0.420	-0.072	0.098	(0.727)	0.002	-0.116	0.214	Reflective	0.084	<0.001
Int1	0.041	-0.038	0.219	-0.025	-0.094	0.195	-0.225	(0.793)	-0.055	0.005	Reflective	0.084	<0.001
Int2	-0.058	-0.052	-0.064	0.228	0.071	-0.091	-0.075	(0.743)	-0.037	-0.307	Reflective	0.084	<0.001
Int3	0.051	0.004	-0.119	-0.045	-0.134	0.059	0.088	(0.685)	0.031	-0.06	Reflective	0.084	<0.001
Int4	-0.030	0.107	-0.136	0.197	0.047	-0.173	-0.014	(0.756)	0.208	-0.005	Reflective	0.084	<0.001
Int5	0.022	0.092	0.078	-0.083	0.105	0.004	-0.028	(0.745)	-0.143	0.360	Reflective	0.084	<0.001
Proto1	0.023	-0.025	0.016	0.098	-0.046	-0.258	0.190	0.096	(0.642)	0.273	Reflective	0.084	<0.001
Proto2	-0.080	0.054	-0.171	0.006	0.025	0.203	-0.080	0.001	(0.776)	0.018	Reflective	0.084	<0.001
Proto3	-0.071	0.081	0.161	-0.089	0.014	0.011	-0.079	-0.082	(0.761)	-0.249	Reflective	0.084	<0.001
cost1	-0.080	0.040	-0.006	-0.147	0.042	-0.125	0.109	0.200	-0.065	(0.878)	Reflective	0.084	<0.001
cost2	0.080	-0.040	0.006	0.147	-0.042	0.125	-0.109	-0.200	0.065	(0.878)	Reflective	0.084	<0.001

Figure 9-4: Combined loadings and cross-loadings continued...

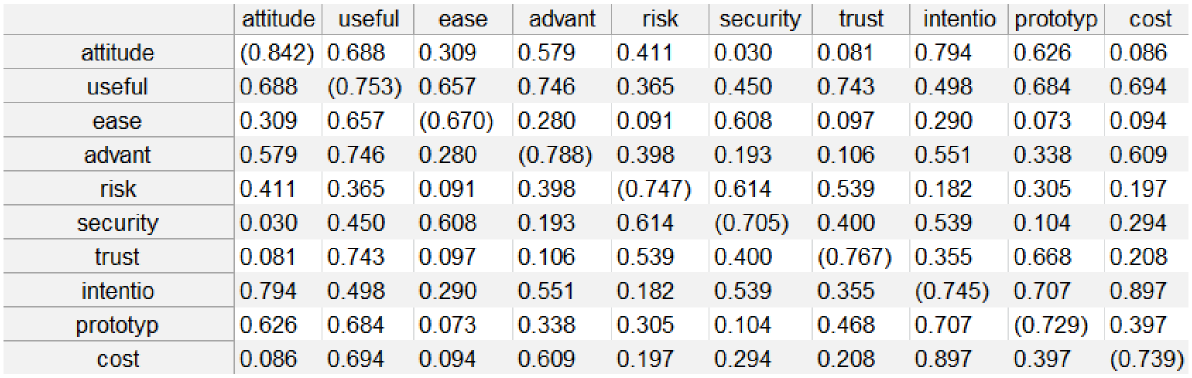
The requirement of the SEM is that the Cronbach's alpha should be at least 0.70 (Cronbach 1951). For the latent variables measurements' mean, standard deviation and cross-loadings see APPENDIX B - The mean, standard deviation, Cronbach's alpha and loadings of the measurements. Figure 9-5 shows that for all latent variables Cronbach's alpha are greater than 0.7 and this makes it reliable. The minimum recommended value for the AVE is 0.5 and Figure 9-5 shows that all the latent variables exceed the minimum recommended value (Hair, Black, Babin, & Anderson, 2010).



	attitude	useful	ease	advant	risk	security	trust	intentio	prototyp	cost
R-Squared	0.660	0.490				0.390	0.390	0.710		
Adj R-Squared	0.503	0.379				0.270	0.331	0.675		
Composite reliab.	0.826	0.747	0.710	0.858	0.816	0.758	0.847	0.843	0.859	0.809
Cronbach's alpha	0.825	0.758	0.701	0.809	0.750	0.705	0.709	0.899	0.712	0.704
Avg. vac. Extrac.	0.704	0.500	0.505	0.751	0.689	0.512	0.735	0.728	0.753	0.789

Figure 9-5: Latent Variables Coefficients (for all correlations P<0.01)

Figure 9-6 shows the correlations among the latent variables. The diagonal elements were all greater than 0.7 and were higher than the correlations with other variable.



	attitude	useful	ease	advant	risk	security	trust	intentio	prototyp	cost
attitude	(0.842)	0.688	0.309	0.579	0.411	0.030	0.081	0.794	0.626	0.086
useful	0.688	(0.753)	0.657	0.746	0.365	0.450	0.743	0.498	0.684	0.694
ease	0.309	0.657	(0.670)	0.280	0.091	0.608	0.097	0.290	0.073	0.094
advant	0.579	0.746	0.280	(0.788)	0.398	0.193	0.106	0.551	0.338	0.609
risk	0.411	0.365	0.091	0.398	(0.747)	0.614	0.539	0.182	0.305	0.197
security	0.030	0.450	0.608	0.193	0.614	(0.705)	0.400	0.539	0.104	0.294
trust	0.081	0.743	0.097	0.106	0.539	0.400	(0.767)	0.355	0.668	0.208
intentio	0.794	0.498	0.290	0.551	0.182	0.539	0.355	(0.745)	0.707	0.897
prototyp	0.626	0.684	0.073	0.338	0.305	0.104	0.468	0.707	(0.729)	0.397
cost	0.086	0.694	0.094	0.609	0.197	0.294	0.208	0.897	0.397	(0.739)

Figure 9-6: Correlations of Latent Variables

9.4 Findings

As shown in Chapter 6, we initially had 22 hypotheses but we remained with 15 after model fitting. One of the findings of the research was that *perceived usefulness* is a major key for determining the adoption of the m-payment. The customer's perception of *risk* directly affects the *perceived security* of the m-payment application and this negatively affects the intention by the customer to adopt the m-payment application. The results also revealed that *perceived ease of* *use* has a significant effect on *perceived security*. The *intention to use* m-payments is increased also by *relative advantage*, *perceived ease of use* and *trust*. The negative effect of perceived cost shows that from the participants' point of view, perceived cost is one of the most important predictors of the *attitude towards using* NFC enabled m-payment as well as the intention to use the system.

The data analysis also revealed that the following factors need to be taken into consideration when dealing with factors that affect the adoption of NFC enabled mobile payments:

- Security of the m-payment application as perceived by the customer. The analysis showed that the ease of use of the application turns to bias the participant's security perception.

- *Perceived risk* has a negative effect on both *perceived security* and *trust* and in turn trust has a significant effect on perceived security. The effect of trust on security can either be negative or positive depending on the customer's perception on risk.

- Relative advantage - clearly inform the customers about the benefits of using the m-payment application.

- Trialability – the application needs to be available to customers on trial basis; this will enable the test the application without being committed to it. Trialability influences *ease of use*, *attitude towards use* and *intention to use*.

- Ease of use should not lead to the compromise of the security of the m-payment application

9.5 Discussion

The research has shown that *perceived ease of use* is strongly correlated to both *perceived usefulness* and *perceived security*. There is a strong correlation between *perceived usefulness* and *attitude to use* the m-payment. Another strong correlation exists between *attitude to use* and *intention to use* the m-payment application. There was a significant negative influence of *perceived risk* on *trust*; the participants who thought that the contactless m-payment were risky tend to also think that it was not useful and secure. This led to a negative influence on both *intention to use* and the *attitude towards using*. The results showed that NFC enabled m-payment are easy to use and that consumers are willing to adopt them. From this research we saw that consumers are willing to adopt the m-payment as long as they can first test the payment application in order to understand how it works. The key element that can hinder the adoption of m-payments is perceived risk and cost. We found that most consumers perceive m-payments as being risky because they do not understand the functionary of the m-payment and its security structure. We recommend that if any stakeholder wants to offer an NFC enabled m-payment, they should educate the customers on the payment application and the technology that supports it.

The results obtained in this research shows that *perceived usefulness* of NFC enabled m-payment is affected also by *trust* and *relative advantage*. The findings show that *perceived risk*, *trust* and *perceived security* are relevant in determining the adoption of NFC enabled m-payments. *Trialability* is also an important factor in determining the acceptance of this kind to payment as shown by the relevance of the prototype. The results also confirms the TAM as shown by the contributions of *perceived ease of use* on *perceived usefulness* and also the contributions of both *perceived ease of use* and *perceived usefulness* to *attitude towards use*.

Through this research we also found that *perceived usefulness* had an insignificant effect on the *intention to use* the m-payment. The data analysis showed that the major determinants of acceptance of NFC enabled m-payment are *perceived ease of use*, *perceived usefulness*, *relative advantage, perceived risk*, *perceived cost*, *perceived security* and *trust*.

The data that was collected showed that 75% of the people received money once a month and those who had bank accounts chose the bank they use depending on the bank charges. The data analysis also showed that the participants found NFC technology to be easy to use. The data analysis also showed that *trust* and *perceived risk* have significant negative effect on *perceived security*.

Our results showed that perceived cost has a negative direct effect on both *attitude towards use* and *intention to use*. This means that the stakeholder offering the NFC enabled m-payment must ensure that the cost of carrying out a transaction is affordable and that there are affordable NFC enabled mobile devices on the market. *Relative advantage* is the strongest determinant of both *perceived usefulness* and *attitude towards use*. The benefits of the NFC enabled m-payments needs to be clearly highlighted to the consumers.

We had expected *perceived risk* to have a negative effect on the *attitude towards use* of NFC m-payment but upon data analysis we found that its effect on *attitude towards use* was insignificant and that it was positively correlated to *perceived security*. The reason for this might be because the benefits of NFC payments enticed the participants to the payments application regardless of its associated risks.

In chapter 3, under the related work section in the research done by Mallat (2007) the following were identified as some of the factors that affect the adoption of m-payments: relative advantage, cost, and trust. These factors were also taken into consideration in this research as well. The same effect that cost, trust and relative advantage had on the adoption of m-payments in Mallat's research is the same effect that was observed in this research.

The research also included the investigation of consumer acceptance of NFC enabled m-payment in MRA. Based on this Chapter for OBJ6a, the factors that affect consumer adoption of NFC enabled m-payments in MRA are:

- Perceived ease of use
- Perceived usefulness
- Perceived cost
- Perceived Security
- Perceived Risk
- Relative advantage
- Trust
- Attitude towards use
- Intention to use
- Trialability

The analysis of the model showed that the prototype had effect on perceived usefulness, attitude towards use and intention to use. Trialability was put in place of the prototype application because the prototype application was put initially to allow the participants to try out and experiment with the application in order to understand how it works. This shows that the consumers need to be able to try out the application before they can use. Most consumers are reluctant to adopt a new payment method without knowledge on how it works.

For OBJ6b, the key determinants of the adoption of NFC enabled m-payments as shown by the finding are:

- Intention to use
- Attitude towards use
- Relative advantage
- Perceived usefulness

9.6 Limitations

Most of the participants were not familiar with the mobile devices that were being used, this made the testing take more time and due to time constraints we could only do the testing with 79 people. Some of the participants were happy with testing the application and giving verbal feedback but were not willing to fill in the questionnaire. Since our sample size was small, this might have affected the outcome of our analysis. One of the limitations of the results is that the research was conducted using a single area and this limited the research sample as well. A broader sample from different MRAs might produce different results. As in any research that involves data collection there may be error which might have been caused by the inherent bias of the participants.

10 CONCLUSION

10.1 Introduction

The purpose of this research was to explore the feasibility of using NFC enabled m-payments in the MRAs of South Africa by carrying out a feasibility study of the technology. The feasibility study included carrying out a SWOT analysis, developing an NFC enabled m-payment application and investigating the factors that affect user adoption of NFC enabled m-payments. The development and testing of the prototype m-payment showed that it practical and feasible to develop an m-payment that is enabled by NFC. Usability testing to the application showed that NFC is usable and efficient.

The research also showed that consumers can adopt any m-payments due to a number of reasons. Some of the reasons include: convenience of m-payments, increased functionality, relatively fast transactions. The lack of other banking and payment alternatives has also been realised as a contributing factor to m-payment adoption. These factors were taken into consideration on the development of the proposed architecture. This chapter concludes the research by looking at factors that affect the adoption of m-payment in MRA; and standards and regulations that affect e-money in South Africa. In this chapter we also propose a business model and an architecture that is suitable for MRAs and concludes by giving some recommendations.

10.2 Proposed Business model and Architecture

This research acknowledges that m-payments depend on the business model used and the relationship between the business model used and the environment in which the mobile payment application will be launched. This section takes a closer look at the different types of Business Models that have been identified in past research and identifies the best choice from those business models for the marginalized rural areas.

The success of proximity mobile payment heavily depends on the collaboration of the stakeholders and this collaboration also affects the business model that will be adopted by the involved stakeholders. Currently the countries that have successfully adopted m-payments have

adopted any one of the following three models: mobile network operator centric; financial institution centric; and third-party operator centric. All these three models have been successful in different countries: the third party centric in China, the MNO centric in Japan and both the MNO centric and the financial institution centric in Korea (Lu et al., 2011). The major problem with the MNO centric model and the financial institutions is that they are restricted to their own customers and this is solved by the third party centric model especially if the MNOs and the financial institutions do not want to cooperate (Lu et al., 2011). The third-party operator centric provides "intermediary mobile payment services by integrating the functions of the MNOs' communications network with the financial institutions' payment accounts" (Lu et al., 2011).
The marginalized rural areas are usually either unbanked or underbanked. These people usually receive money once a month and most of them cannot afford to keep a bank account because of the bank charges. These factors were taken into consideration in the proposed model.

10.2.1 Limitations of the Business Models

From literature, the major problem with the MNO centric model and the financial institutions is that they are restricted to their own customers (Lu et al., 2011) and this is solved by the third party centric model especially if the MNOs and the financial institutions do not want to cooperate. The model that is adopted by a country or an area depends on both the customers who will be using the system and the dominating stakeholders in the area.

10.2.2 Proposed Model

The technologies that have been used to carry out m-payments are for skilful mobile users and are complex to be used by users who have no knowledge or limited knowledge of the technology. We are proposing NFC which is touch-based to be used as the m-payment technology to accommodate all consumers.

The interviews carried out in this research showed that the customers who have bank accounts would adopt m-payment it is offered by either the MNO or the bank while those without bank accounts are desperate enough to settle for any method as long as they have access to their money at the end of the day. The easiest way to offer an m-payment service will be to integrate the m-payment service with the existing banking and money transfer services. In South Africa Vodacom is already offering M-PESA, while MTN is offering MTN mobile money, the banks are offering cardless services and there is also WIZZIT (WIZZIT Bank, 2012) which is offering mobile banking to the unbanked at very low prices. This shows that the infrastructure for m-payments is already in place. The only need is a business model that suits people in the MRA. One of the characteristics of the consumers in MRA is their low income. The business model should therefore insure that the transaction costs that will be paid by these consumers are affordable to them. This can be done by reducing the number of stakeholders who are involved in the business model. The business model should serve both the unbanked and underbanked without forcing the unbanked to open a bank account that they cannot afford to maintain or the banked to open a mobile money transfer account if they are comfortable using the banks.

Another important factor that needs to be considered when it comes to m-payments is the mobile devices that will be used to carry out the transaction. This is where the mobile device manufactures come in to play. The mobile device manufacturers play an important role because for the consumers to carry out m-transactions they need mobile devices that are well suited for their environment, in this case MRA. The data collected for the TAM as well as the focus groups interviews showed that the cost of NFC enabled mobile devices was a major concern for the consumers. The consumers expressed that they need a mobile device that is cheap and has a long battery life. Our data analysis showed that most of the participants owned low-end mobile devices (i.e. feature phones) that offer basic functionalities.

The storage location of the secure element (SE) is also very important. As discussed in chapter 5, there are three possible locations for the SE: the mobile device, the Micro SD card and the SIM card. Mobile devices are ruled out as SE storage with the fundamental aim of trying to minimize the number of stakeholders involved in the m-payment to reduce transaction fees. We are proposing that the only role that the mobile device manufacturers play is only to provide the suitable mobile devices. Therefore in the context of MRA, the SIM card and Micro SD card can be used as a SE in order to provide both the unbanked and the banked with secure storage. This means that if the bank or WIZZIT is offering the m-payment service, they can use the Micro SD card as their secure element and this eliminates the need to use the MNO’s SIM’s card.

Based on the above discussions, the MNO, the bank or mobile banks like WIZZIT can offer m-payments independent of each other. The business model we are proposing for m-payments for MRA consist of the following stakeholders:

- MNOs
- Traditional banks
- Mobile banks
- Mobile device manufacturers (the only role that will be played by the OEMs is to provide the suitable devices.

These stakeholders do not have to go into partnership but can offer the m-payment individually and this will reduce the transaction fees that the customers will pay.

As discussed in chapter 1, being unbanked includes the inadequacy of people to meet the bank's criteria to open a bank account or their inability to access to banking facilities. These people may not be able to benefit from m-payments if there are being offered by the banks only, this is why we have proposed that the individual stakeholders offer their own m-payment. With the involved stakeholders offering their own m-payment, issues of interoperability of the payment applications arise. In order not to burden the merchants with more than one POS to accommodate all the customers, the stakeholders need to collaborate and ensure that they come up the m-payments applications that are interoperable.

On the issue of POSs, we identified that most of the merchants in the MRA are informal shops that are usually operated by family. These shops do not pay tax and cannot afford to buy equipment that is required for m-payments. Hence we are proposing that the merchants use their mobile device to receive m-payments. The following section gives the detailed architecture of this proposal

10.2.3 Proposed Application Architecture

The merchants in the MRA are usually unregistered and hence do not pay tax. The merchants operate very small shops that are usually owned and run by families. As such, this negatively impacts m-payment systems adoption by the merchants because they cannot afford to buy the required hardware for m-payments due to lack of funds. This research noted that merchants cannot afford to pay high transaction fees and expensive hardware thus negatively affecting their adoption of m-payments in MRA. Hence this architecture does not include the contactless reader other expensive m-payment hardware.

Figure 10-1 shows the proposed architecture for the MRA m-payment application. As we have already identified that most MNO have penetrated the MRA, the mobile network can be used by both the banks and the MNOs in conducting the m-payment.

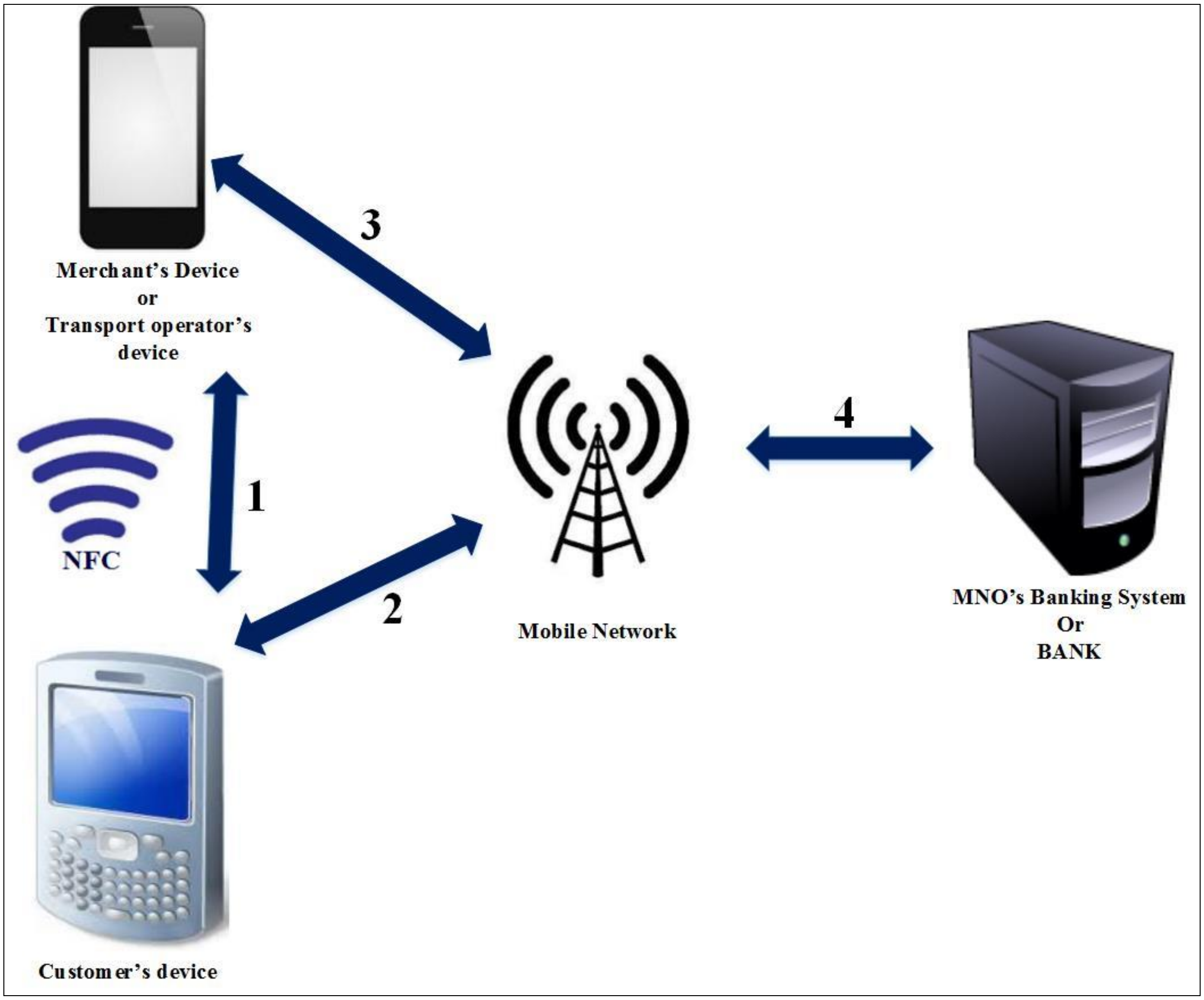


Figure 10-1: Proposed payment architecture

In this architecture the customers can own an account with either the bank or the MNO's banking system. We are also proposing that the customers use the m-payment to pay for their transport fares well as shown in Figure 10-1. During a payment transaction the customer receives the banking information of either the merchant or the transport operator using the NFC technology as shown by arrow 1 (or the customer can send his/her banking details to the merchant or transport operator) and sends the transaction information to the bank or MNO’s bank as shown by arrow 2 in Figure 10-1. The banking system receives the banking information (arrow 4) and carries out the transaction and sends the transaction outcome (arrow 4) to both the customer and the merchant or transport operator (arrow 2 and arrow 3 respectively).

The merchants can also act as agents to the MNOs and the customers can also collect their cash from the merchants. M-payments can benefit people that stay in marginalized areas by providing them with a payment method alternative to cash. The government can also benefit from m-payments because it causes the money that was in the informal sector to enter the formal market.

10.3 Recommendations

For any subsequent application, we recommend that the providers of the m-payment application take into consideration the following factors:

- The MNO have managed to penetrate into areas that banks have not reached (Adkins, 2013; Aker & Mbiti, 2010; Ondiege, 2010) and have a great customer base. Our data analysis showed that about 40 per cent of our participants are willing to use m-payments offered by MNOs.
- The banks have the trust of the customers and can lose their customers if they do not take advantage of m-payments.
- Knowledge of the income of the customers they are offering the m-payment to. People staying in marginalized rural areas cannot afford to pay high transaction fees because their income is very low but people in urban areas can overlook the transaction fee if the m-payment offers convenience.
- Customer’s perception of the technology that supports the m-payment and the provider especially in terms of trust
- The complexity and security of the technology that will support the m-payment
- The inclusion of other services in the m-payment that will generate revenue such as advertising.

- Convincing the merchants and the customers about the value of the m-payment over the existing payment system
- Educate the customer on the security of transactions channel and also the security that the application provides for the accounts.

The adoption of an m-payment application depends on both the merchants and the customers. These two stakeholders are in a catch-22 situation in most countries when it comes to m-payments. The customers are waiting for the merchants to offer m-payments while the merchants are waiting for the customers to adopt m-payments. For this problem we recommend that the stakeholder offering the m-payment should find out the m-payment that the customers want and their perception about the stakeholder offering the payment. Our data analysis showed that the customers will only adopt the m-payment if they trust the stakeholder offering it. The technology that supports the m-payment also affects the adoption of m-payment. Some technologies complicate m-payments and this will prevent the customers from adopting the m-payment. There is need to provide interoperability among different m-payments applications. This will enable customers to transfer money to each other using the peer-to-peer mode. The interoperability of m-payments should be cheap, easy, fast and secure to carry out transaction. This is the reason we are proposing NFC enabled m-payments for MRA. NFC offers ease of use to customers as it is touch based (Chidembo, 2009).

10.4 Summary of the handling and addressing of the research questions

Table 19 gives a summary of how the research questions have been addressed and handled. The recommendation and the proposed architecture given in this chapter are based on the findings of the whole research.

Table 19: How research questions have been addressed and handled

Research Questions	Research Objectives		Research Outcome
What are the strength, weaknesses, opportunities and threats of NFC enabled m-payments?	OBJ1	Undertake a SWOT analysis of the technology.	The answer to this question was provided in both Chapters 3 and Chapter 4. In Chapter 4, the research showed that the Strengths and Opportunities of NFC outweigh the weaknesses and threats of the technology.
What are the security issues of NFC as a payment technology?	OBJ2	Evaluate security issues	The security issues of NFC were covered under the Threats of NFC in Chapter 4. This section also showed that these issues can be minimized.
What are the consumer requirements for NFC enabled m-payments?	OB3a	Determine the knowledge of consumers on m-payments.	The answer to this question is found in Chapter 8 on requirements gathering.
	OBJ3b	Determine user requirement for an NFC enabled m-payment application	
How feasible is it to implement an NFC enabled m-payment application?	OBJ4	Determine the practicality of implementing an NFC enabled payment application	In Chapter 7 a prototype application was successfully implemented and it was tested in Chapter 8.
What are the factors that affect utilization of m-payments?	OBJ5	Deduce usability and user perception issues of m-payment applications	Chapters 3 covered the factors that affect the utilization of m-payments. We also found that the users perceived m-payments and NFC enabled mobile devices as expensive when we did data analysis in Chapter 9. In Chapter 3 we discovered mobile technologies other than NFC made m-payments complex.
Will the users accept an NFC enabled payment application?	OBJ6a	Determine factors that affect consumer adoption of NFC m-payments.	In Chapter 6, after intensive literature review, we came up with factors that affect m-payment and their associated hypotheses based on validated previous research. In Chapter 9 we carried out a data analysis on the data we collected in order to validate these factors and we rejected or accepted the hypothesis based on the statistical analysis.
	OBJ6b	Determine key determinants of NFC m-payment for MRA	
What are the NFC technology deployment strategies that can be adverted for MRA?	OBJ7	Give recommendation on the sustainable implementation framework for NFC applications in South Africa's marginalised rural communities.	Throughout this research we discovered many factors that affect the adoption of m-payment. In this chapter we came up with a proposed architecture and recommendations and this provides answers to this question and addresses its objectives.

10.5 Research Contribution

This research contributes to the research on m-payments enabled by the NFC technology. Even though the research was carried out in the context of MRA, the findings of this research can also be applied to customers in urban areas. Its contributions include:

- Major factors that affect the adoption of NFC enabled m-payments
- Mapping of the correlation between the technology acceptance and adoption factors, specifically for MRAs
- Validated hypotheses associated with factors that affect the adoption of NFC enabled m-payment
- Confirmed the feasibility of NFC for m-payments in MRAs
- A recommendation on the architecture and business models suitable for m-payments in MRAs
- Confirmed the practical implementation of an NFC enabled m-payment
- Recommendations for handling security issues associated by NFC technology
- A working NFC enabled prototype of an m-payment Android application

10.6 Future Work

In this research we presented NFC technology for user as a payment technology for consumers living in marginalized rural areas. The research showed that the technology offers ease of use and it is easy to deploy. NFC technology has many uses in mobile commerce which include advertising and marketing. Interoperability of m-payments among different application was suggested in this research and there is still need to carry out research on interoperability platforms of m-payments.

Another area that still needs research is the security issues that affect NFC technology. In this research, security issues were covered mostly using literature. There is need to carry practical tests on all the security issues and techniques for mitigating and addressing those security risks.

10.7 Conclusion

Mobile banking coupled together with m-payments has the potential revolutionize the lives of the unbanked and underbanked. For people staying in MRA this method avoids the necessity to travel long distances to go banks to collect cash if they adopt the method. The adoption of the m-payments depends on the merchants as well. The stakeholders need to involve the customers and the merchants in the development of the payment application for the application to be adopted. Lack of understanding of customer perception and motivation causes m-payments to fail (Rouibah, 2009). This can be avoided by carrying out research such as this one that looks at the factors that might affect the targeted customers from adopting the m-payment and address them before launching the payment application. Our data analysis showed that if the consumers trust the m-payment provider, they are not concerned with the issues of security. Another important point we identified from the focus groups is that consumers find it easy to adopt any form of m-payments application as long they understand its process and the technology that supports it.

The short communication distance that allows NFC devices to communicate increases security but does not eliminate security threats. The stakeholders offering the contactless m-payment has to ensure that the application and the personal data are stored securely on the mobile device and also that the application uses a secure channel during transaction. When it comes to payments methods, privacy, security, convenience, cost and usability are major concern for the customers. A survey done by Accenture South Africa showed that consumers in South Africa are willing to adopt m-payments as soon as they are rolled out (Accenture, 2014). According to Accenture the consumers need to be motivated to use m-payments and this can be done through rewards for usage (Accenture, 2014). The banking institutions need to take the initiative to offer m-payments to both the unbanked and banked for them not to lose revenue from m-payments and customers. Most people staying in MRA in South Africa depend on remittance send by relatives therefore they require a cheap payment method. An easy to use m-payment like the one enabled by NFC can benefit them because it can help them to save transport. The success of m-payments in most Asian countries is due to the fact that the Governments and influential MNO assisted in the development of the payment applications (Ondrus & Pigneur, 2007).

Lack of a suitable payment technology has been slowing down the development of mobile commerce. This can now be possibly overcome by NFC technology. The growth of m-payments heavily depends on the availability, accessibility, reliability, security, dependability, interoperability and acceptance of mobile wallet systems (Amoroso & Magnier-Watanabe, 2012). In conclusion m-payments are not going to reach mass adoption rates over night, like credits cards acceptance, it will take time for m-payments to be accepted. More still needs to be done in terms of educating customers and merchants, marketing, advertising and research before m-payments reach mass adoption in South Africa.

REFERENCES

Aamoth, D. (2011). How the New Google Wallet Mobile Payment System Works. *Time Magazine Techland*.

Accenture. (2014). *Driving the Adoption of Mobile Payments — What SA Consumers Want*.

Adkins, S. S. (2013). Ambient Insight Regional Report: The 2012-2017 Africa Mobile Learning Market.

Afanu, E. A. (2013). *Mobile Money Security:A Holistic Approach*. Lulea University of Technology.

Afful, F. E. (2013). Africa's mobile banking revolution: the poor now have access to financial services. Retrieved April 11, 2014, from http://mobilemoneyafrica.com/details.php?post_id=34

Ailisto, H., Matinmikko, T., Ylisaukko-oja, A., Strommer, E., Hillukkala, M., Wallin, A., … Salonen, J. (2007). *Physical browsing with NFC technology*. *VTT Tiedotteita Valtion Teknillinen Tutkimuskeskus* (p. 70). Retrieved from http://www.vtt.fi/inf/pdf/tiedotteet/2007/T2400.pdf

Aker, J. C., & Mbiti, I. M. (2010). Mobile Phones and Economic Development in Africa. *Center of Development Working Paper 211*.

Allah, M. M. A. (2011). Strengths and Weaknesses of Near Field Communication (NFC) Technology. *Global Journal of Computer Science and Technology*, *11*(3).

Al-ofeishat, H. A., & Rababah, M. A. A. A. L. (2012). Near Field Communication (NFC). *Interanational Journal of Computer Science and Network Security (IJCSNS)*, *12*(2), 93–99.

Amoako-Gyampah, K., & Salam, a. F. (2004). An extension of the technology acceptance model in an ERP implementation environment. *Information & Management*, *41*(6), 731–745. doi:10.1016/j.im.2003.08.010

Amoroso, D. L., & Magnier-Watanabe, R. (2012). Building a reasearch Model for Mobile Wallet Consumer Adoption: The case of Mobile Suica in Japan. *Journal of Theoretical and Applied Electronic Commerce Research*, *7*(1), 94–110.

Android Developers. (2014). Pausing and Resuming an Activity. Retrieved September 24, 2014, from http://developer.android.com/training/basics/activity-lifecycle/pausing.html

Anong, S. T., & Kunovskaya, I. (2013). M-finance and consumer redress for the unbanked in South Africa. *International Journal of Consumer Studies*, *37*(7).

Aziza, H. (2010). NFC technology in Mobile Phone next Generation Services. In *IEEE Second International Workshop on Near Field Communication*.

Bamasak, O. (2011). Exploring consumers acceptance of mobile payments – an empirical study. *International Journal of Information Technology, Communications and Convergence*, *1*(2), 173–185.

Bangor, A., Kortum, P., & Miller, J. (2009). Determinng What Individual SUS Scores Mean: Adding an Adjective Rating Scale. *Journal of Usability Studies*, *4*(3), 114–123.

Bankole, F., Bankole, O., Brown, I., & Cloete, E. (2012). Cell Phone Banking: Revisiting Predictors of Adoption in South Africa. In *AMCIS 2012 Proceedings*.

Barbuta, I., Dobrean, S., Gaza, M., Mihaila, M., & Screpnic, A. (2012). Mobile Payments Guide 2012: Insights in the worldwide mobile financial services market. *White Paper for THE PAYPERS*.

Bauer, H. H., Reichardt, T., Barnes, S. J., & Neumann, M. M. (2005). Driving consumer acceptance of mobile marketing: a theoretical framework and empirical study. *Journal of Electronic Commerce Research*, *6*(3), 181–191.

Benamati, J. S., Fuller, M. A., Serva, M. A., & Baroudi, J. A. (2010). Clarifying the integration of trust and TAM in e-commerce environments: implications for systems design and management. *IEEE Transactions on Engineering Management*, *57*(3), 380–393.

Benyo, B. (2009). Business Process Analysis of NFC-based Services. In *The 7th International Conference on Computational Cybernetics*. Palma de Mallorca, Spain.

Bevan, N. (1995). Human-Computer Interaction Standards. In *The 6th International Conference on Human Computer Interaction*. Yokohama.

Bose, & Shin, K. G. (2006). On mobile viruses exploiting messaging and Bluetooth services. In *The 2nd International Conference on Security and Privacy in Communication Networks*. Baltimore.

Brooke, J. (2013). SUS : A Retrospective. *Journal of Usabilty Studies*, *8*(2), 29–40.

Buchenau, M., & Suri, J. F. (2000). Experience prototyping. In *the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques* (pp. 424–433). ACM.

Cavoukian, B. A. (2012). Mobile Near Field Communication: Keep It Secure and Private. *Information Systems Security Association (ISSA)*, (August).

Chappell, D., & Jewell, T. (2002). *Java Web Services*. O'Reilly.

Chau, P. Y. K. (1996). An empirical assessment of a modified technology acceptance model. *Journal of Management Information Systems*, *13*(2), 185–204.

Chidembo, N. (2009). *EXPLORING CONSUMER ADOPTION OF NFC-ENABLED*. UNIVERSITY OF PRETORIA.

Chin, W. W., Marcolin, B. L., & Newsted, N. P. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, *14*(2), 189–217.

Chuttur, M. Y. (2009). Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. *Sprouts: Working Papers on Information Systems*, *9*(37).

Clark, S. (2012). NFC World. *NTT Docomo to take Japanese mobile wallet global*. Retrieved from http://www.nfcworld.com/2012/10/11/318353/ntt-docomo-to-take-japanese-mobile-wallet-global/

Coetzee, J. (2009). Personal or Remote Interaction? Banking the Unbanked in South Africa. *South African Journal of Economic and Management Sciences (SAJEMS)*, *12*(4).

Coskun, V., Ok, K., & Ozdenizci, B. (2013). *Professional NFC Application Development for Android*. John Wiley & Sons, Ltd.

CRONBACH, L. J. (1951). *Coefficient alpha and the internal structure of tests* (pp. 16 , 297–334). Psychometrika.

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008a). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, *7*(2), 165–181. doi:10.1016/j.elerap.2007.02.001

Dahlberg, T., Mallat, N., Ondrus, J., & Zmijewska, A. (2008b). Past, present and future of mobile payments research: A literature review. *Electronic Commerce Research and Applications*, *7*(2), 165–181. doi:10.1016/j.elerap.2007.02.001

Dahlberg, T., Mallat, N., & Öörni, A. (2003). Consumer acceptance of mobile payment solutions. In *The Second International Conference on Mobile Business* (pp. 211–218). Vienna.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 318–339.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man Machine Studies*, *38*(3), 475–487.

Deloitte. (2011). Dailing in: The future of mobile payments in Canada.

Deloitte. (2012). NFC and mobile devices : payments and more ! *White Paper*.

Dobson, P. J. (2002). Critical realism and information systems research: Why bother with philosophy. *An International Electronic Journal*, *7*(2). Retrieved from http://www.informationr.net/ir/7-2/paper124.html

Du, H. (2013). NFC Technology: Today and Tomorrow. *International Journal of Future Computer and Communication, 2*(4), 351–354. doi:10.7763/IJFCC.2013.V2.183

ECMA International. (2010). Ecma-386: NFC-SEC-01: NFC-SEC Cryptography Standard using ECDH and AES, *2nd Editio*.

ECMA International. (2013a). ECMA-385 NFC-SEC : NFCIP-1 Security Services and Protocol, (June).

ECMA International. (2013b). Standard Ecma-340: Near Field Communication - Interface and Protocol (NFCIP-1), *3rd Editio*.

ECMA International. (2013c). Standard ECMA-352: Near Field Communication Interface and Protocol-2 (NFCIP-2), *3rd Editio*.

Ergeerts, G., Schellekensy, D., Schrooyen, F., Beyers, R., De Kock, K., & Van Herck, T. (2012). Vision towards an Open Electronic Wallet on NFC Smartphones. *International Journal on Advances in Internet Technology, Vol 5 No 3 & 4*, *5*(3 & 4).

Eze, U. C., Gan, G. G., Ademu, J., & Tella, S. A. (2008). Modelling User Trust and Mobile Payment Adoption : A Conceptual Framework. *Communications of the IBIMA*, *3*, 224–231.

Ezell, S. (2009). Explaining International IT Application Leadership: Contactless Mobile Payments. *The Information Technology & Innovation Foundation*.

Fielding, R. (2000). *Architectural Styles and the Design of Network-based Software Architectures*. University of Califormia, Irvine, USA.

Ghag, O., & Hedge, S. (2012). A Comprehensive Study of Google Wallet as an NFC Application, *58*(16), 37–42.

Gillis, B., & Pillay, R. (2012). A review of payments interoperability in the Southern African Development Community region. *Journal of Payments Strategy & Systems*, *6*(2), 144–158.

Global Platform. (2009). Proposition for NFC Mobile: Secure Element Management and Messaging. *White Paper*.

Gottschalk, K., Graham, S., Kreger, H., & Snell, J. (2002). Introduction to Web services architecture. *IBM System Journal*, *41*(2), 170–177.

Granelli, F. (2011). An Overview on the status of Near Field Communication Technologies. *ICaST ICST's Global Community Magazine*, 4–5. Retrieved from http://icast.icst.org/2011/04/overview-status-near-field-communication-technologies

GSMA. (2011). M-Ticketing Whitepaper. Security Classification: Non-Confidential. *White Paper*.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis*. Upper Saddle River, New jersey: Pearson Prentice Hall.

Halaweh, M. (2012). Adoption Of Near Field Communication Technology For Mobile Payments In The UAE. In *European, Mediterranean & Middle Eastern Conference on Information Systems* (Vol. 2012, pp. 613–618). Munich, Germany.

Haselsteiner, E., & Breitfuß, K. (2006). Security in Near Field Communication (NFC) Strengths and Weaknesses. In *Workshop on RFID Security*.

He, Y. (2012). *A new approach to faster retail service and customer satisfaction: How NFC and RFID technologies may improve current retail business performance*. Lahti University of Applied Sciences.

Innovision Research & Technology. (2007). Near Field Communication in the real world - Turning the NFC promise into profitable , everyday applications Innovision Research & Technology plc. *White Paper*.

ISO/IEC 18092. (2013). INTERNATIONAL STANDARD ISO / IEC Telecommunications and information Communication — Interface and Protocol. *International Standard, Reference Number ISO/IEC 18092:2013(E), Second Edi*.

ISO/IEC 9241-11. (1998). Ergonomic requirements for office work with visual display terminals (VDT)s - Part 11 Guidance on usability. *EC 9241-14: 1998 (E)*.

Jack, W., & Suri, T. (2011). Mobile money: The economics of M-PESA. *National Bureau of Economic Research*, *w16721*.

Jackson, W. (2011). *Android Apps For Absolute Beginners*. Apress.

Jandebeur, J., & Schaeufele, A. (2013). SWOT Analysis of Near Field Communication Technology. *Academic and Business Research Institute Publication*.

Jenkins, B. (2008). Developing Mobile Money Ecosystems. *Washington, DC: IFC and the Harvard Kennedy School*.

Jovanovic, M., & Organero, M. M. (2011). Analysis of the Latest Trends in Mobile Commerce using the NFC Technology. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, (May), 1–12. Retrieved from Available from: http://www.cyberjournals.com/Papers/May2011/01.pdf. (Accessed 13 June 2012).

Keen, I. (2009). NFC Technology Overview. *NFC Forum White Paper*.

Khan, M. S., & Jain, A. (2013). STUDY OF EMERGING OPERATING SYSTEM GOOGLE ANDROID. *International Journal Of Advance Research In Science And Engineering (IJARSE)*, *2*(12), 66–72.

Kim, C., Mirusmonov, M., & Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in Human Behavior*, *26*(3), 310–322. doi:10.1016/j.chb.2009.10.013

KPMG International. (2007). Mobile Payments in Asia Pacific. *White Paper*.

Kumar, A. (2010). *Near field communication*. COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY.

Kumar, D., Gonsalves, T. a, Jhunjhunwala, A., & Raina, G. (2010). Mobile payment architectures for India. *2010 National Conference On Communications (NCC)*, (1), 1–5. doi:10.1109/NCC.2010.5430160

Kupukile, M., & Ncube, M. (2011). Competition and Efficiency in the Banking Sector in South Africa. *African Development Review*, *23*(1), 4–15.

Laukkanen, T., & Lauronen, J. (2005). Consumer value creation in mobile banking services. *International Journal of Mobile Communications*, *3*(4), 325–338.

Lawack-Davids, V. (2012). The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa. *Journal of International Commercial Law and Technology*, *7*(4), 318–327.

Liebenau, J., Elaluf-calderwood, S., Karrberg, P., & Hosein, G. (2011). Near Field Communications ; Privacy , Regulation & Business Models October 2011, (October).

Lightspeed Research. (2012). *Driving Value and Adoption of Mobile Payments — Consumers Want More*.

Linck, K., Pousttchi, K., & Wiedemann, D. G. (2006). Security issues in mobile payment from the customer viewpoint. In *14th European Conference on Information Systems (ECIS)*. Go¨teborg, Sweden.

Lu, Y., Yang, S., Chau, P. Y. K., & Cao, Y. (2011). Dynamics between the trust transfer process and intention to use mobile payment services: A cross-environment perspective. *Information & Management*, *48*(8), 393–403. doi:10.1016/j.im.2011.09.006

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science*, *35*(4), 572–585.

Madlmayr, G. (2008). *Managing an NFC Ecosystem*. *Near Field Communication Research*. Hagenberg.

Makina, D. (2013). Migration and characteristics of remittance senders in South Africa. *International Migration*, *51*(s1), e148–e158.

Mallat, N. (2004). Theoretical constructs of mobile payment adoption. In *The 27th Information Systems Research Seminar*. Scandinavia.

Mallat, N. (2007). Exploring consumer adoption of mobile payments – A qualitative study. *The Journal of Strategic Information Systems*, *16*(4), 413–432. doi:10.1016/j.jsis.2007.08.001

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*, 251 – 266.

Maroofi, F., Kahrarian, F., & Dehghani, M. (2013). An Investigation of Initial Trust in Mobile Banking. *International Journal of Academic Research in Business and Social Sciences*, *3*(9), 394–403.

Mas, I., & Morawczynski, O. (2010). Designing Mobile Money Services Lessons from M-PESA. *Innovations*, *4*(2), 77–91.

Massoth, M., & Bingel, T. (2009). Performance of different mobile payment serviceconcepts compared with a NFC based solution. In *IEEE Fourth International Conference on Internet and Web Applications and Services*.

Mccarthy, B., & Data, F. (2008). Mobile Payment : The Linchpin of the Mobile Commerce Economy.

McElligott, T. (2007). Near Field Near, But Mobeam Now. *Telephony*.

Minihold, R. (2011). Near Field Communication (NFC) Technology and Measurements. *White Paper for Rhode & Schwarz*.

Mkhumbuza, K. (2013). *Mobile Banking Capabilities Required to Serve the Unbanked Market in South Africa*. University of Pretoria.

Mobey Forum. (2011a). Business models for NFC payments. *White Paper*, 1–64.

Mobey Forum. (2011b). Business Models For NFC payments. *White Paper*.

Mobile Financial Services. (2011). Business Models For NFC payments. *Mobey Forum*.

Moggridge, B. (2007). *Designing Interactions* (pp. 643–735). The MIT Press.

Moore, J. F. (1996). *The Death of Competition: Leadership and Strategy in the Age of Business Ecosystems* (p. 26). New York, NY: Harper Collins.

Muriira, L. M., & Kibua, N. (2012). Near Field Communication (NFC) Technology : The Future Mobile Money Service for Kenya Peponet Technology Abstract. *International Journal of Computing and ICT Research*, *6*(1), 73–83.

Nambi, S. N. A. U., Prabhakar, T., & Jamadagni, H. (2012). Near field communication – applications and performance studies. *Wireless Networks and Computational Intelligence Communications in Computer and Information Science*, *292*, 1–10.

National Retail Federation. (2011). Mobile Retailing Blueprint. *White Paper*.

NFC Forum. (2008). Essentials for Successful NFC Mobile Ecosystems. *White Paper*.

NFC Forum. (2009). Logical Link Control Protocol Technical Specification NFC Forum. *White Paper,* (LLCP 1.0).

NFC Forum. (2011). Simple NDEF Exchange Protocol Technical Specification. *Technical Specification,* (SNEP 1.0).

NTT DOMOCO. (2011). DOMOCO Enriches Mobile NFC Ecosystem. *Mobility Domoco Newsletter*.

Ok, K., Coskun, V., Ozdenizci, B., & Aydin, M. N. (2011). A Role-Based Service Level NFC Ecosystem Model. *Wireless Personal Communications*, *68*(3), 811–841. doi:10.1007/s11277-011-0484-3

Ondiege, P. (2010). Mobile Banking in Africa: Taking the Bank to the People. *Africa Economic Brief*, *1*(8).

Ondrus, J., & Pigneur, Y. (2007). An Assessment of NFC for Future Mobile Payment Systems. *International Conference on the Management of Mobile Business (ICMB 2007)*, 43–43. doi:10.1109/ICMB.2007.9

Ozdenizci, B., Aydin, M. N., Coskun, V., & Ok, K. (2010). NFC Research Framework: A Literature Review And Future Research Directions. In *The 14th IBIMA International Business Information Management Conference* (pp. 2672–2685). Istanbul,TURKEY.

Patel, J., & Kothari, B. (2013). Near Field Communication - The Future Technology For an Interactive World. *International Journal of Engineering Research and Science and Technology*, *2*(2).

Patinge, S. A., & Soni, P. D. (2013). A Survey on Instant Message and Location Sharing System for Android. *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, *2*(10), 219–221.

Pavan, K. P., Sanjay, A., & Zornitza, P. (2012). Comparing Performance of Web Service Interaction Styles : SOAP vs . REST. In *2012 Proceedings of the Conference on Information Systems Applied Research* (pp. 1–24).

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce : Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, *7*(3), 69–103.

Pihlajamäki, A. (2004). Mobile Payments. In *Seminar on Networking Business*.

Pope, M., Pantages, R., Enachescu, N., Dinshaw, R., Joshlin, C., Stone, R., & Seal, K. (2011). MOBILE PAYMENTS : THE REALITY ON THE GROUND IN SELECTED ASIAN COUNTRIES AND THE UNITED STATES. *International Journal of Mobile Marketing Winter*, *6*(2), 88–105.

Raina, V. K., Pandey, U. S., & Makkad, M. (2011). Use of Mobile Transactions Payment Model in Customer Oriented Payment System using NFC Technology. *International Journal of Mathematical and Computer Sciences Vol.11,Part II*, *11*.

Rogers, E. M. (1995). *Diffusion of Innovations*. New York: Free Press, New York, NY.

Rogers, E. M. (2003). *Diffusion of innovations*. New York: Free Press.

Rouibah, R. (2009). The failure of mobile payment: Evidence from quasi-experiments. In *2009 Euro Americans Conference on Telematics and Information Systems* (pp. 1–7). ACM.

Sahin, I. (2006). DETAILED REVIEW OF ROGERS ' DIFFUSION OF INNOVATIONS THEORY AND EDUCATIONAL TECHNOLOGY-RELATED STUDIES BASED ON ROGERS '. *The Turkish Online Journal of Educational Technology - TOJET*, *5*(2), 14–23.

Sammarco, A. J. (2010). NFC Enabling Technology Enhancing Your Business Opportunities. *White Paper for DeviceSolution*.

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students* (Fifth edit.). Pearson Education.

Sauro, J. (2014). Measuring Usability with the System Usability Scale (SUS). *2011*. Retrieved June 15, 2014, from http://www.measuringusability.com/sus.php

Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, *9*(3), 209–216. doi:10.1016/j.elerap.2009.07.005

Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, *9*(3), 209–216.

Shin, D. (2008). Understanding purchasing behaviors in virtual economy: Consumer behavior of virtual currency in Web2.0 communities. *Interacting with Computers*, *20*(4), 433–446.

Shin, D. (2009). Towards an understanding of the consumer acceptance of mobile wallet. *Computers in Human Behavior*, *25*(6), 1343–1354.

Shon, T. H., & Swatman, P. M. C. (1998). Identifying effectiveness criteria on internet payment systems. *Internet Research*, *8*(3), 203 – 218.

Siau, K., Sheng, H., Nah, F., & Davis, S. (2004). A qualitative investigation on consumer trust in mobile commerce. *International Journal of Electronic Business*, *2*(3), 283–300.

Smart Card Alliance. (2007). Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure. *A Smart Card Alliance Contactless Payments Council White Paper*, (September), 1–39. Retrieved from http://www.mobiltarca.com/media/documents/smart-card-alliance-proximity-mobile-payments-leveraging-nfc-and-the-contactle.pdf

Smart Card Alliance. (2008). What Makes a Smart Card Secure? *White Paper*.

Smart Card Alliance. (2011). *The Mobile Payments and NFC Landscape: A U.S. Perspective* (pp. 1–53).

Smart Card Alliance Contactless Payments Council. (2007). Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure. *White Paper*.

Smith, M. L. (2006). Overcoming theory-practice inconsistencies: Critical realism and information systems research. *Information and Organization*, *16*, 191–211.

South African Reserve Bank. (2009). National Payment System Department Position Paper on Electronic Money Position Paper NPS 01/2009 Dated November 2009. *White Paper*, (November), 1–10.

Specification, T. (2006). NFC Data Exchange Format (NDEF) Technical Specification.

STRATEGY ANALYTICS INSIGHT. (2012). *Google Wallet Phones Off to a Slow Start in USA Summary*.

Strommer, E., Hillukkala, M., & Ylisaukko-oja, A. (2007). Ultra-low power sensors with near field communication for mobile applications. *International Federation for Information Processing*, 131–142.

Szmigig, I. T. D., & Bourne, H. (1999). Electronic cash: a qualitative assessment of its adoption. *International Journal of Bank Marketing*, *17*(4), 192–202.

Valentin, E. K. (2001). SWOT ANALYSIS FROM A RESOURCE-BASED VIEW. *Journal of Marketing THEORY AND PRACTICE*, *9*(2), 54–69.

Van der Heijden, H. (2002). Factors Affecting the Successful Introduction of Mobile Payment Systems. In *The 15th Bled Electronic Commerce Conference* (pp. 430–443).

Ventures. (2013). South Africa's Banked Population Now 75% – FinMark Trust. Retrieved April 11, 2014, from http://www.ventures-africa.com/2013/11/south-africas-banked-population-now-75-finmark-trust/

Viehland, D., Siu, R., & Leong, Y. (2010). Consumer willingness to use and pay for Mobile Payment Services. *International Journal Of Principles and Application of Information Science and Technology*, *3*(1).

WIZZIT Bank. (2012). WIZZIT Bank. Retrieved May 21, 2014, from http://www.wizzit.co.za/?q=node

Yang, S., Lu, Y., Gupta, S., Cao, Y., & Zhang, R. (2012). Mobile payment services adoption across time: An empirical study of the effects of behavioural beliefs, social influences and personal traits. *Computers in Human Behaviour*, *28*, 129–142.

Zang, M. Y., & Dodgson, M. (2007). A roasted duck can still fly away: a case study of technology, nationality, culture and the rapid and early internationalization of the firm. *Journal of World Busines*, *42*, 336–249.

Zea, O. M., Lekse, D., Smith, A., & Holstein, L. (2012). Understanding the current state of the NFC payment ecosystem : A graph- based analysis of market players and their relations. *Enfoque UTE*, *3*(2), 13–32.

Zmijewska, A. (2005). Evaluating Wireless Technologies in Mobile Payments-A Customer Centric Approach. In *The IEEE International Conference on Mobile Business (ICMB).*

Zmijewska, A., Lawrence, E., & Steele, R. (2007). Classifying m-payments – a user-centric model. In *The Third International Conference on Mobile Business, M-Business 2004.*

APPENDIX A - Latent Variables Measurements

Table 20: Measuring Attitude towards using NFC enabled m-payments

Measurement Item	References
Using mobile payment services is a good idea	Oh et al. (2003)
Using mobile payment services is wise	van der Heijden (2003)
Using mobile payment services is beneficial	Yang and Yoo (2004)
Using mobile payment services is interesting	Schierz *et al*, (2010)

Table 21: Measurements for Intention to use NFC enabled m-payments

Measurement Item	References
Given the opportunity, I will use mobile payment services	Davis (1989), Gefen et al. (2003)
I am likely to use mobile payment services in the near future	Venkatesh and Davis (2000)
I am willing to use mobile payment services in the near future	Schierz *et al*, (2010)
I intend to use mobile payment services when the opportunity arises	Schierz *et al*, (2010)
I will recommend m-payments to my family and friends	

Table 22: Measurements for Perceived Usefulness

Measurement Item	References
NFC enabled mobile payments are useful for making payments.	Bhattacherjee (2001)
Using NFC enabled m-payments simplifies making payments.	Devaraj et al. (2002), van der Heijden (2003)
Using NFC m-payments is a good idea	Oh et al. (2003)
M-payments services enable a faster usage of applications like person to person money transfer.	der Heijden (2003)
NFC m-payments adds variety to payment methods	
NFC m-payments provide a faster method of payment.	
Using NFC m-payments service is beneficial	Yang and Yoo (2004)

Table 23: Measurements for Perceived Ease of Use

Measurement Item	References
It is easy to learn to use the NFC enabled m-payment	
It is easy to master using NFC m-payments services	Bhattacherjee (2001), Davis et al. (1989)
The interaction with mobile payment services is clear and understandable	Taylor and Todd (1995), Venkatesh and Davis (2000)
It is easy to perform the steps required to use mobile payment services	Schierz et al 2010
It is easy to interact with mobile payment services	Schierz et al 2010

Table 24: Measurements for Perceived Risk

Measurement Item	References
The risk of an unauthorized third party overseeing the payment process is low	Luarn and Lin (2005)
The risk of abuse of usage information (e.g., names of business partners, payment amount) is low when using mobile payment services	Parasuraman et al. (2005)
The risk of abuse of billing information (e.g., credit card number, bank account data) is low when using mobile payment services	Schierz et al 2010
I think contactless m-payments transactions have potential risk	Wu et al 2005
I think contactless m-payments puts my privacy at risk	Wu et al 2005

Table 25: Measurements for Perceived Security

Measurement Item	References
Using a contactless m-payment application is financially secure.	
I would find mobile payment services secure in conducting my payment transactions	Schierz et al 2010
I am worried about the security of contactless m-payments.	

Table 26: Measurements for Trust

Measurement Item	References
I trust NFC as a payment technology contactless m-payments	
I trust that the m-payment application will protect my privacy	

Table 27: Measurements for Cost

Measurement Item	References
I think an NFC enabled mobile phone is expensive	
I think the transaction fee for carrying out contactless m-payment is expensive	

Table 28: Measurements for Prototype application

Measurement Item	References
The prototype helped me to understand contactless m-payments enabled by NFC	
The prototype gave me confidence in contactless m-payments	
The prototype application was easy to use	

Table 29: Measurements for Prototype application

Measurement Item	References
Contactless m-payments are convenient and effective.	
I believe contactless m-payments are quicker than using cash.	
I believe contactless m-payments will benefit me	
Contactless m-payments will help me save time	
I believe can benefit from contactless m-payments	

APPENDIX B - The mean, standard deviation, Cronbach’s alpha and loadings of the measurements

	Mean	Standard Dev.	α	Loadings
Att1	4.286	1.074	0.725	0.703
Att2	4.078	0.855		0.799
Att3	3.844	1.113		0.812
Att4	3.701	1.077		0.636
Int1	4.273	0.805	0.799	0.793
Int2	4.156	0.875		0.743
Int3	4.156	1.101		0.685
Int4	4.104	0.661		0.756
Int5	4.078	0.957		0.745
Usef1	4.000	0.743	0.758	0.671
Usef2	3.922	0.839		0.780
Usef3	3.857	0.838		0.760
Usef4	4.377	1.001		0.621
Usef5	3.987	1.019		0.691
Usef6	4.182	0.702		0.755
Usef7	4.000	0.858		0.741
Ease2	4.182	0.807	0.701	0.814
Ease3	3.526	1.026		0.612
Ease4	4.234	0.560		0.818

	Mean	Standard Dev.	α	Loadings
Relat1	4.156	0.762	0.669	0.714
Relat2	4.289	0.763		0.698
Relat3	4.338	0.700		0.634
Relat4	4.351	0.664		0.882
Relat5	3.909	0.934		0.738
Risk1	4.208	0.732	0.650	0.631
Risk2	3.571	1.031		0.795
Risk3	4.052	1.062		0.803
Sec1	4.052	0.724	0.705	0.749
Sec2	3.870	1.030		0.649
Sec3	3.779	1.034		0.713
Trust1	3.922	0.970	0.709	0.727
Trust2	3.737	1.112		0.727
Proto1	4.273	0.772	0.699	0.642
Proto2	4.039	0.733		0.776
Proto3	4.117	1.051		0.761
Cost1	3.650	0.980	0.780	0.830
Cost1	3.790	0.970	0.765	0.798

APPENDIX C – Questionnaire

University of Fort Hare
Together in Excellence

Department of Computer Science

By

Caroline Gurajena

I am conducting a research on Mobile Payments in the MRA Communities, South Africa. The research requires conducting interviews with various stakeholders including mobile phones users and shop owners. In this questionnaire there is no wrong or right answer. What is required is just your opinion on the asked questions. Your responses will be kept **Private and Confidential** and used for academic purposes only. Your co-operation will be highly appreciated.

SECTION A: BIOGRAPHICAL INFORMATION

1. Gender

Female	
Male	

2. Age

15 - 29	
30 - 45	
45 and above	

3. Education Level

Grade 9 and below	
Grade 12	
Certificate	
Diploma	
Degree	

SECTION B: BANKING INFORMATION

1. Do you have access to a bank (if your answer to this question is **NO** please proceed to question 6)?

Yes	
No	

2. How far is the nearest bank from where you live (in km)?
   …………………………………………

3. Do you have a bank account?

Yes	
No	

4. How often do you use a bank?

Weekly	
Monthly	
Rarely	

5. Why did you choose the bank that you use?
   ………
   ………
   ………

6. How often do you receive money?

Weekly	
Monthly	
Rarely	

SECTION C: TAM INFORMATION

For the next several questions, please choose a box that indicates how much you agree with the statement.

Attitude towards using NFC enabled m-payments

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Using NFC enabled mobile payment services is a good idea					
Using NFC enabled mobile payment services is wise					
Using NFC enabled mobile payment services is beneficial					
Using NFC enabled mobile payment services is interesting					

Intention to use NFC enabled m-payments

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Given the opportunity, I will use NFC enabled mobile payment services					
I am likely to use NFC enabled mobile payment services in the near future					
I am willing to use NFC enabled mobile payment services in the near future					
I intend to use NFC enabled mobile payment services when the opportunity arises					
I will recommend NFC enabled mobile payments to my family and friends					

Perceived Usefulness

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
NFC enabled mobile payments are useful for making payments.					
Using NFC enabled mobile payments simplifies making payments.					
Using NFC enabled mobile payments is a good idea					
NFC enabled mobile payments services enable a faster and easier usage of applications (money transfer).					
NFC enabled mobile payments adds variety to payment methods					
NFC enabled mobile payments provides a faster method of payment.					
Using NFC enabled mobile payments service is beneficial					

Perceived Ease of Use

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
It is easy to learn to use NFC enabled mobile payment application					
It is easy to perform the steps required to use NFC enabled mobile payment application					
I think an NFC enabled mobile payment application is complicated					
I think most people can learn to use NFC enabled mobile payment application quickly					
I did not need to learn anything before learning to use NFC enabled mobile payment application					

Relative Advantage

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
NFC enabled mobile payment are convenient and effective					
I believe contactless mobile payments are quicker than using cash					
I believe contactless mobile payments will benefit me					
Contactless mobile payments will help me save time					
I believe can benefit from contactless mobile payments					

Perceived Risk

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The risk of an unauthorized third party overseeing the payment process is low					
I think contactless m-payments transactions have potential risk					
I think contactless m-payments puts my privacy at risk					

Perceived Security

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Using a contactless m-payment application is financially secure.					
I would find mobile payment services secure in conducting my payment transactions					
I am worried about the security of contactless m-payments.					

Trust

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I trust NFC as a payment technology for mobile payments					
I trust that the mobile payment application will protect my privacy					

Cost

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think an NFC enabled mobile phone is expensive					
I think the transaction fee for carrying out contactless mobile payments is expensive					

Prototype application

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The prototype helped me to understand NFC enabled mobile payments					
The prototype gave me confidence in NFC enabled mobile payments					
The mobile prototype application was easy to use					

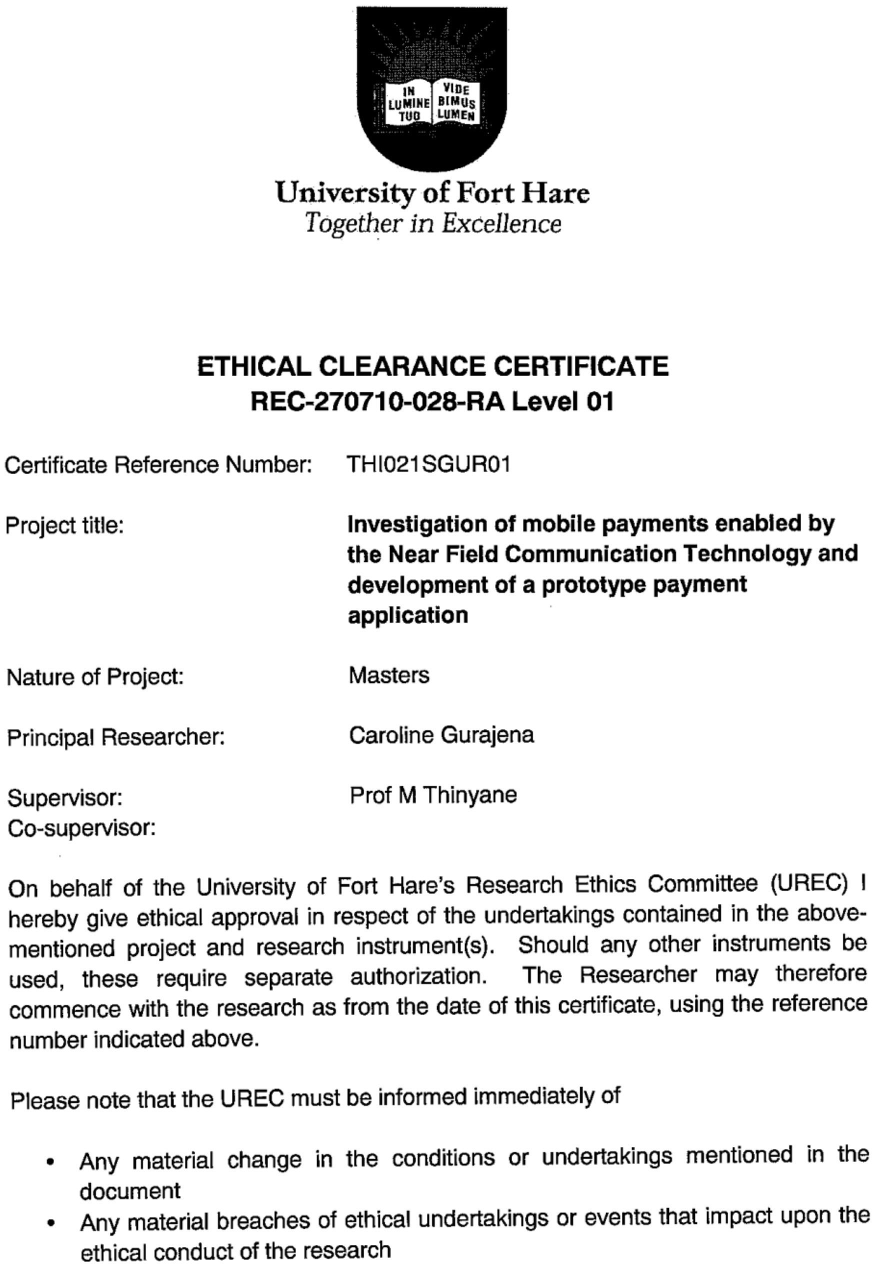
APPENDIX D – SOAP WSDL

```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Generated by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is Metro/2.3
(tags/2.3-7528; 2013-04-29T19:34:10+0000) JAXWS-RI/2.2.8 JAXWS/2.2 svn-revision#unknown.
-->
<definitions targetNamespace="http://simulated.banking.net/"
name="SimulatedBankingService" xmlns="http://schemas.xmlsoap.org/wsdl/"
xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:tns="http://simulated.banking.net/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsp1_2="http://schemas.xmlsoap.org/ws/2004/09/policy"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <types>
    <xsd:schema>
      <xsd:import namespace="http://simulated.banking.net/"
schemaLocation="SimulatedBankingService_schema1.xsd"/>
    </xsd:schema>
  </types>
  <message name="transferRequest">
    <part name="parameters" element="tns:transferRequest"/>
  </message>
  <message name="transferRequestResponse">
    <part name="parameters" element="tns:transferRequestResponse"/>
  </message>
  <message name="transfer">
    <part name="parameters" element="tns:transfer"/>
  </message>
  <message name="transferResponse">
    <part name="parameters" element="tns:transferResponse"/>
  </message>
  <message name="balance">
    <part name="parameters" element="tns:balance"/>
  </message>
  <message name="balanceResponse">
    <part name="parameters" element="tns:balanceResponse"/>
  </message>
  <message name="get_details">
    <part name="parameters" element="tns:get_details"/>
  </message>
  <message name="get_detailsResponse">
    <part name="parameters" element="tns:get_detailsResponse"/>
  </message>
  <message name="check_payment">
    <part name="parameters" element="tns:check_payment"/>
  </message>
  <message name="check_paymentResponse">
    <part name="parameters" element="tns:check_paymentResponse"/>
  </message>
  <message name="make_payment">
    <part name="parameters" element="tns:make_payment"/>
  </message>
  <message name="make_paymentResponse">
    <part name="parameters" element="tns:make_paymentResponse"/>
  </message>
  <message name="createAccount">
    <part name="parameters" element="tns:createAccount"/>
  </message>
  <message name="createAccountResponse">
    <part name="parameters" element="tns:createAccountResponse"/>
  </message>
  <portType name="SimulatedBankingService">
    <operation name="transferRequest">
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/transferRequestRequest"
message="tns:transferRequest"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/transferRequestResponse
" message="tns:transferRequestResponse"/>
    </operation>
    <operation name="transfer">
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/transferRequest"
message="tns:transfer"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/transferResponse"
message="tns:transferResponse"/>
    </operation>
    <operation name="balance">
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/balanceRequest"
message="tns:balance"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/balanceResponse"
message="tns:balanceResponse"/>
    </operation>
    <operation name="get_details">
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/get_detailsRequest"
message="tns:get_details"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/get_detailsResponse"
message="tns:get_detailsResponse"/>
    </operation>
    <operation name="check_payment">
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/check_paymentRequest"
message="tns:check_payment"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/check_paymentResponse"
message="tns:check_paymentResponse"/>
    </operation>
    <operation name="make_payment">
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/make_paymentRequest"
message="tns:make_payment"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/make_paymentResponse"
message="tns:make_paymentResponse"/>
    </operation>
    <operation name="createAccount">
```

```
      <input
wsam:Action="http://simulated.banking.net/SimulatedBankingService/createAccountRequest"
message="tns:createAccount"/>
      <output
wsam:Action="http://simulated.banking.net/SimulatedBankingService/createAccountResponse"
message="tns:createAccountResponse"/>
    </operation>
  </portType>
  <binding name="SimulatedBankingServicePortBinding" type="tns:SimulatedBankingService">
    <soap:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>
    <operation name="transferRequest">
      <soap:operation soapAction=""/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
    <operation name="transfer">
      <soap:operation soapAction=""/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
    <operation name="balance">
      <soap:operation soapAction=""/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
    <operation name="get_details">
      <soap:operation soapAction=""/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
    <operation name="check_payment">
      <soap:operation soapAction=""/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
    <operation name="make_payment">
      <soap:operation soapAction=""/>
      <input>
```

```
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
    <operation name="createAccount">
      <soap:operation soapAction=""/>
      <input>
        <soap:body use="literal"/>
      </input>
      <output>
        <soap:body use="literal"/>
      </output>
    </operation>
  </binding>
  <service name="SimulatedBankingService">
    <port name="SimulatedBankingServicePort"
binding="tns:SimulatedBankingServicePortBinding">
      <soap:address location="REPLACE_WITH_ACTUAL_URL"/>
    </port>
  </service>
</definitions>
```

APPENDIX E - Ethical Clearance



University of Fort Hare
Together in Excellence

ETHICAL CLEARANCE CERTIFICATE
REC-270710-028-RA Level 01

Certificate Reference Number:	THI021SGUR01
Project title:	**Investigation of mobile payments enabled by the Near Field Communication Technology and development of a prototype payment application**
Nature of Project:	Masters
Principal Researcher:	Caroline Gurajena
Supervisor:	Prof M Thinyane
Co-supervisor:	

On behalf of the University of Fort Hare's Research Ethics Committee (UREC) I hereby give ethical approval in respect of the undertakings contained in the above-mentioned project and research instrument(s). Should any other instruments be used, these require separate authorization. The Researcher may therefore commence with the research as from the date of this certificate, using the reference number indicated above.

Please note that the UREC must be informed immediately of

- Any material change in the conditions or undertakings mentioned in the document
- Any material breaches of ethical undertakings or events that impact upon the ethical conduct of the research

The Principal Researcher must report to the UREC in the prescribed format, where applicable, annually, and at the end of the project, in respect of ethical compliance.

Special conditions: Research that includes children as per the official regulations of the act must take the following into account:

Note: The UREC is aware of the provisions of s71 of the National Health Act 61 of 2003 and that matters pertaining to obtaining the Minister's consent are under discussion and remain unresolved. Nonetheless, as was decided at a meeting between the National Health Research Ethics Committee and stakeholders on 6 June 2013, university ethics committees may continue to grant ethical clearance for research involving children without the Minister's consent, provided that the prescripts of the previous rules have been met. This certificate is granted in terms of this agreement.

The UREC retains the right to

- Withdraw or amend this Ethical Clearance Certificate if
  - Any unethical principal or practices are revealed or suspected
  - Relevant information has been withheld or misrepresented
  - Regulatory changes of whatsoever nature so require
  - The conditions contained in the Certificate have not been adhered to

- Request access to any information or data at any time during the course or after completion of the project.

- In addition to the need to comply with the highest level of ethical conduct principle investigators must report back annually as an evaluation and monitoring mechanism on the progress being made by the research. Such a report must be sent to the Dean of Research's office

The Ethics Committee wished you well in your research.

Yours sincerely

Professor Gideon de Wet
Dean of Research

06 June 2014

APPENDIX F – Consent Form

University of Fort Hare
Together in Excellence

Ethics Research Confidentiality and Informed Consent Form

Please note:

This form is to be completed by the researcher(s) as well as by the interviewee before the commencement of the research. Copies of the signed form must be filed and kept on record

(To be adapted for individual circumstances/needs)

Our University of Fort Hare / Department is asking people from your community / sample / group to answer some questions, which we hope will benefit your community and possibly other communities in the future.

The University of Fort Hare / Department/ organization is conducting research regarding. **Mobile Payments in Marginalized Rural Areas**. We are interested in finding out more about **The Use Of Banking Facilities And Mobile Banking** We are carrying out this research to help **Major Stakeholder in the ecosystem of Mobile Payments enabled by Near Field Communication to come up with a payment solution that best suits people who live in the Marginalized rural areas of South Africa** (*adapt for individual projects*)

Please understand that you are not being forced to take part in this study and the choice whether to participate or not is yours alone. However, we would really appreciate it if you do share your thoughts with us. If you choose not take part in answering these questions, you will not be affected in any way. If you agree to participate, you may stop me at any time and tell me that you don't want to go on with the interview. If you do this there will also be no penalties and you will NOT be prejudiced in ANY way. Confidentiality will be observed professionally.

I will not be recording your name anywhere on the questionnaire and no one will be able to link you to the answers you give. Only the researchers will have access to the unlinked information. The information will remain confidential and there will be no "come-backs" from the answers you give.

The interview will last around **(15)** minutes *(this is to be tested through a pilot).* I will be asking you a questions and ask that you are as open and honest as possible in answering these questions. Some questions may be of a personal and/or sensitive nature. I will be asking some questions that you may not have thought about before, and which also involve thinking about the past or the future. We know that you cannot be absolutely certain about the answers to these questions but we ask that you try to think about these questions. When it comes to answering questions there are no right and wrong answers. When we ask questions about the future we are not interested in what you think the best thing would be to do, but what you think would actually happen. (*adapt for individual circumstances*)

If possible, our organization would like to come back to this area once we have completed our study to inform you and your community of what the results are and discuss our findings and proposals around the research and what this means for people in this area.

INFORMED CONSENT

I hereby agree to participate in research regarding **NFC enabled Mobile Payments**. I understand that I am participating freely and without being forced in any way to do so. I also understand that I can stop this interview at any point should I not want to continue and that this decision will not in any way affect me negatively.

I understand that this is a research project whose purpose is not necessarily to benefit me personally.

I have received the telephone number of a person to contact should I need to speak about any issues which may arise in this interview.

I understand that this consent form will not be linked to the questionnaire, and that my answers will remain confidential.

I understand that if at all possible, feedback will be given to my community on the results of the completed research.

……………………………..
Signature of participant **Date**:…………………..

I hereby agree to the tape recording of my participation in the study

……………………………..
Signature of participant **Date**:…………………..