UNIVERSITY OF THE WESTERN CAPE

Secure contactless mobile financial services with Near Field Communication

By

Adeola Oluwaseyi Poroye

A thesis submitted in fulfilment of the requirements
for the degree of Master of Science in the
Department of Computer Science, University of the Western Cape

Supervisor: Dr WD Tucker
Co-Supervisor: Mr MJ Norman

August 2011

Keywords

Banking the unbanked

Contactless smart card

Mobile-to-mobile money transfer

Mobile banking

Mobile financial services

Mobile payment

Near Field Communication

Security

Transaction cost

Usability

Abstract

This thesis presents the results from work with three prototypes that use Near Field Communication technology to provide secure contactless mobile financial services on mobile phones. Because of the challenges that hinder financial institutions from providing mobile financial services to the unbanked, the latter are forced to seek other forms of services that are often unsafe, inconvenient and expensive. The capacity of Near Field Communication to leverage the security features of the contactless smart card and the ubiquitous nature of the mobile phone can be used to provide such mobile financial services. The study used qualitative and quantitative research, and software engineering synthesis as the research methods. A focus group study identified some of the challenges faced, while a demographic survey helped to understand the target group: the unbanked. A preliminary payment survey using a personal computer emulator of mobile payment helped to determine if and how Near Field Communication was needed. Based on the results of our security attack study, we secured the short messaging service-based mobile banking application and then improved the security using Near Field Communication. The mobile banking application could not be tested in a real financial environment with actual users, so two new Near Field Communication-based prototypes were developed from the existing application to provide mobile payment and mobile-to-mobile money transfers. Security, usability and transaction cost were identified as the biggest challenges facing mobile financial services providers and the unbanked. The results showed that Near Field Communication can be used to resolve these challenges.

Declaration of authorship

I declare that *Secure contactless mobile financial services with Near Field Communication* is my own work, that it has not been submitted for any degree or examination in any other university and that all the sources I used or quoted have been indicated and acknowledged by appropriate references.

Full name .... Date: ....

Signed: ....

Acknowledgements

I would like to express my appreciation to the following people for their contributions towards the completion of the academic programme:

1. First and foremost thanks to the Almighty GOD for all that He has done for me. To Him alone is this glory forever and ever.

2. Dr. William D. Tucker, for the honour not only to work under his professional supervision and within his laboratory, but also for creating an environment conductive for research activities.

3. Mr. Michael J. Norman for his supervision, guidance, sound judgement and enthusiasm. Thank you Michael for being that angel. Thank you for all the periodic discussions, support and encouragement throughout the past two years. You are not only an excellent lecturer, but also a good friend.

4. I would like to appreciate my mum, dad, loving sisters and brothers and the entire extended family for their love, support, advice and patience. I thank you all.

5. I will like to thank Prof. and Mrs. Ogunniyi and family, my family and parents in South Africa. Thank you and may God continuously reward you.

6. I will like thank Prophet Temitope Balogun Joshua, my pastors and folks at SCOAN, Cape Town, South Africa. I would not have made this without your unconditional support. Your prayers, encouragement, enthusiasm and genuine caring attitude have done so much for me. Thank you for taking such good care. Emmanuel!!!

7. To all the members of Bridging Application and Network Group (BANG); thank you for your friendship, I am indebted to you all for your continued expertise, advice and encouragement. I am proud to have you guys as my friends.

8. I would also like to thank Telkom/Cisco/THRIP Centre of Excellence (CoE) that provided the necessary equipment and being my sponsor during these studies.

9. Last but not the least, I would like to thank Xiao Ping Hu who stood by me through the highs and lows of this period. I know how much it cost you, but thank you for everything. May God bless you.

Contents

List of Figures

List of Tables

Glossary

APDU	Application Protocol Data Unit: data exchange format a reader specified in ISO7896 to exchange data between and smart card chips.
API	Application Programming Interface
ATMs	Automated Teller Machines
CLDC	Connected Limited Device Configuration
CSCs	Contactless Smart Cards
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union is the specialised agency of the United Nations which is responsible for information and communication technologies.
ITU-T	is one of the three sectors (divisions or units) of the ITU; it coordinates standards for telecommunications. It is based in Geneva, Switzerland.
IVR	Interactive Voice Response
J2ME	Java 2 Platform, Micro Edition
JSR	Java Specification Requests
JSR 177	see also SATSA
JSR 257	A Java API standard defined to make use of the capability of the NFC functionality of the handset.
JVM	Java Virtual Machine

Kbps	Kilobits per seconds
M2M	Mobile-2-Mobile
MAC	Message Authentication Code
	A Message Authentication Code can be described as an encrypted checksum.
mbanking	Mobile Banking
mbps	megabit per second
MFS	Mobile Financial Services
MHz	Mega Hertz
MIDlet	is an application that uses the Mobile Information Device Profile of the CLDC for the J2ME environment.
mpayment	Mobile Payment
M-PESA	is a branchless banking service for Kenya.
MNO	Mobile Network Operator
MTN	Mobile Telephone Network
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP	NFC Interface and Protocol
OTP	One-Time-Password
p2p	Peer-2-Peer
	the 14 or 16 digits embossed on a bank or credit card
PCD	Proximity Coupling Device
PICC	Proximity Inductive Coupling Card
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POS	Point-Of-Sale
RF	Radio Frequency
RFID	RF Identification is a technology used to identify objects carrying RF transponders.
RMI	Remote Method Invocation
RSA	In cryptography, (stands for Rivest Shamir Adleman who first publicly described it) is an algorithm for public-key

	cryptography.
RTDs	Record Type Definitions Specification on how information like URI, SMS or plain text are encoded to fit into NDEF data containers.
SATSA	Security and Trust Services API A Java API standard defined in JSR 177 allowing a J2ME Application to access the SE of a mobile device.
SDM	Software Development Method
SE	Secure Element: is a Trusted Environment for storing sensitive data or applications.
SHA-1	In cryptography, Secure Hash Algorithm - 1 is a cryptographic hash function designed by the National Security Agency and published by the National Institute of Standard and Technology as a U.S. Federal Information Processing Standard
SP	Service Provider
SPSS	Statistical Package for the Social Sciences
SMAC	Standalone Mobile Application Clients
SMS	Short Message (or Messaging) Service
SIM	Subscriber Identity Module A smart card in a special form factor used in a mobile phone to authenticate the user against the network.
TDEA	Tripple Data Encryption Algorithm, see 3DES
URL	Uniform Resource Locator
UWC	University of the Western Cape
VM	Virtual Money
WAP	Wireless Application Protocol
Wizzit	is a provider of basic banking services for the unbanked
3DES	Triple Data Encryption Standard In cryptography, 3DES is the common name for the TDEA block cipher, which applies the DES cipher algorithm three times to each data block
X.509	In cryptography, X.509 is an ITU-T standard for PKI

Chapter 1

Introduction

This thesis presents the results from work with three prototypes that use Near Field Communication (NFC) technology to provide secure contactless Mobile Financial Services (MFSs) on mobile phones. In South Africa, the number of mobile phones has surpassed the number of bank accounts [41]. This creates both an opportunity and several challenges. The opportunity is that mobile phones may be a viable banking option for banking the unbanked members of the population, i.e. those without bank accounts or access to financial services. The major challenges are to provide security, improve convenience and lower transaction costs. A possible solution is to combine the security features of Contactless Smart Cards (CSCs) and the ubiquity of the mobile phone. This powerful combination can be traced to the latest member of the Radio Frequency Identification (RFID) family called NFC. Section 1.1 provides background on the related technology, Section 1.2 provides the motivation for the study, Section 1.3 introduces the research question and the overall approach, while Section 1.4 gives an outline of the rest of the thesis.

1.1 Background

The availability of automatic identification devices with technologies such as RFID and CSCs foster potential applications and business models [66]. Mobile phones are widespread and can support users in gaining access to various MFSs [27]. This study focuses on three technologies: RFID, CSC and NFC. Technological innovations enable new and innovative solutions for the variety of problems in the MFS domain because they allow mobile phones to be used as convenient and secure smart cards [86]. Section 1.1.1 provides an introduction to RFID, Section 1.1.2 addresses CSCs and Section 1.1.3 gives a brief account of NFC.

1.1.1 Radio frequency identification

The de facto barcode label is becoming inadequate to current and future requirements. While it is inexpensive, it has a low storage capacity and its inability to be reprogrammed requires a technically better solution for modern sophisticated processes such as providing security [45]. This section describes RFID and explains some of its applications.

RFID is a generic term for technologies that use radio waves to automatically identify people or objects [66]. The most common RFID method of identification is to store a serial number. This encoding is put on a microchip appended to an antenna. The chip and the antenna together form an RFID transponder, or designate. The antenna enables the chip to transmit information to a reader. The reader converts a radio wave, reflected back from the RFID tag, into digital information and passes that information on to computers that can make use of it [45]. General uses are to optimise logistics, solve out-of-stock problems and improve the supply chain [66]. The use of RFID offers reduced product size and reduced chance of counterfeiting [95].

1.1.2 Contactless smart cards

Today, the smart card is the most common form of electronic data-carrying device. Smart cards possess a contact strip, e.g. on bank cards and phone cards. However, a mechanical contact is often not practical because it subjects the contact strip to wear and tear.

The aim of CSC technology is to provide low-cost no-touch communication that offers acceptable levels of authentication, e.g. an encrypted channel for communication between the card reader and the smart card [4]. CSC technology contains microprocessor chips that support various security tools, including cryptography, to protect data transmitted between the card and the reader. A CSC is a proximity card because it operates at limited distances that vary from less than a millimetre to ten centimetres [4] [44]. The International Organisation for Standardisation /International Electrotechnical Commission (ISO/IEC 14443) is an international standard that defines how proximity cards are used for identification and the transmission protocols for communicating with it.

1.1.3 Near field communication

NFC is the latest in the family of RFID technologies. From a technological viewpoint, NFC is similar to RFID, since both use radio frequency (RF) to transmit data. Unlike its predecessors, NFC does not suffer from privacy issues and can be built into mobile phones [42] [60]. With the widespread use of mobile phones and their continuing growth potential, NFC-enabled mobile phones with available physical infrastructure, such as NFC tags, readers or devices, can become a potentially transformative technological innovation [75]. NFC operates in the 13.56 megahertz (MHz) spectrum and supports data transfer rates of 106, 216 and 424 kilobits per second (Kbps). An extension of up to one megabit per second (mbps) is expected [86]. The typical communication range of an NFC-device lies between two and four centimetres [60].

Two proximity coupling devices are of importance to NFC [59]: a Proximity Coupling Device (PCD) and a Proximity Inductive Coupling Card (PICC). The former uses a transmitter that reads ISO 14443 tags. An electromagnetic field is emitted from the reader, which inductively powers a tag/transmitter. The reader's communication with PICC involves the use of a load modulation scheme. The latter involves the use of a proximity reader to read or write to a transponder. ISO14443 tags do not have a power supply like a battery and are powered by the electromagnetic field of the reader.

NFC has two data formats [59]: NFC Data Exchange Format (NDEF) and Record Type Definitions (RTDs). The former is a data format to store information like a Uniform Resource Locator (URL), a Short Messaging Service (SMS) or plain text in a data container that could be stored on an NFC tag or exchanged over NFC [60]. One NDEF can store multiple RTDs [60].

An NFC device can operate in three modes from the application to the RF layer [60]: Peer-to-Peer (p2p) mode, read/write mode and card/tag emulation mode. In p2p mode, two NFC devices can carry out bidirectional communication to transfer arbitrary data. In read/write mode an NFC device acts as a PCD [60]. It can read and write data stored on an NFC-compliant passive transponder. Card emulation mode is a special smart card capability protocol for mobile devices. Thus, card emulation mode can, for example, enable payment or public ticket services.

People often face the complexities of setting up network connections between devices. This in part motivated the NFC Interface and Protocol (NFCIP-1) and its standardisation in ISO 18092. NFCIP-1 focuses on consumer electronics that use secure communication and, more importantly, on allowing people to expend less effort in configuring their networks [86] [10]. NFC Interface Protocol 2 (NFCIP-2) allows NFC to be compliant with physical infrastructure such as a FeliCa CSC system. FeliCa is a contactless RFID smart card system developed by Sony in Japan, primarily used for electronic money cards. NFCIP-2 is a bidirectional proximity coupling technology based on ISO 14443 and FeliCa standards.

1.2 Motivation

NFC offers a feasible MFS solution for a standard cellular handset, allowing the mobile phone to act as a CSC. Thus, the aim of this study is to explore NFC technology as a convenient and secure option for the unbanked with the capacity to perform financial transactions [86] [95]. This section uses the African context to motivate the exploration of this particular technology. Section 1.2.1 gives an account of MFSs in the South African context, Section 1.2.2 addresses mobile phone penetration in South Africa and Section 1.2.3 discusses the concept of "banking the unbanked".

1.2.1 Mobile financial services

In South Africa, there are 55 million people, of which 35 million are mobile users [69]. South Africa has a relatively sophisticated banking system where 36 banks are competing to serve a total of 20 million customers via nearly 3,000 branches and 17,000 Automated Teller Machines (ATMs) [69] [12]. This environment is highly regulated, while new entrants have changed banking paradigms. This section briefly examines two new innovative entrant payment services for the unbanked: M-PESA in Kenya and Wizzit in South Africa [12].

Kenya's largest Mobile Network Operator (MNO), Safaricom (a part of Vodafone), launched M-PESA. The M-PESA concept enables a mobile phone owner to move money swiftly, securely and directly across to another mobile phone user. The customer does not require a bank account, but simply registers with Safaricom for an M-PESA account [38] [27]. A customer buys electronic money at a Safaricom outlet, follows the instructions (similar to loading airtime onto a cell phone) and is able to load electronic money that can be used for M-PESA money transfers. M-PESA is now available in South Africa.

Wizzit allows users to perform phone-to-phone payments using SMS [39]. Users can also pay bills, buy airtime, transfer money, buy subscriptions, and achieve full transactional and informational banking via their mobile phones [39]. A companion Wizzit MasterCard-branded debit card may also be used for making purchases. The MasterCard may be used for making withdrawals from ATMs and receiving cash back from stores in the Wizzit network.

Wizzit makes it convenient for geographically isolated customers to exchange physical cash for mobile currency. Customers without access to banks can deposit cash at any post office and receive an immediate credit to their account. In South Africa, an MFS such as Wizzit offers a straightforward model for serving under-banked or unbanked clients and can target locations where traditional bank branches may not be economically viable [39].

1.2.2 Mobile phone penetration in South Africa

The African continent has the highest ratio of mobile to total telephone subscribers of any world region in the world and has been dubbed “the least wired region in the world” [31]. Africa is also the region with the highest mobile cellular growth rate [26]. Growth over the last five years averaged around 50% per year [41]. In emerging economies the mobile phone is anticipated to leapfrog the Personal Computer (PC), much like mobile cellular connection leapfrogged the fixed line [26].

In South Africa, mobile penetration is about 83% [26]. Wireless access has allowed communication to reach rural areas that previously had no network coverage [41]. About 52% of the population lives in areas with wireless reception. This growth of mobile phone use will continue to rise. In contrast, the use of a fixed landline is rare, because most people have to travel some distance to reach a landline. South Africa also has problems such as cable theft that makes it difficult and expensive to offer such services [41].

1.2.3 Banking the unbanked

The call to provide MFSs to bank the unbanked is compelling. Besides the demand for convenience by consumers, there is a need for access to MFSs by those with limited access to traditional forms of banking [24] [14]. The benefit extends to creating opportunities that offer cost-effective services by optimising existing infrastructure and minimising further investments in expensive infrastructure, while also opening up potential revenue streams and employment opportunities for corporate organisations [5].

MFSs in developing countries are still unpopular when compared to physical cash payment. The recent steady growth of mobile phone access is gradually providing a platform for offering MFSs to those in need of them [84]. Previously, the vast majority of the unbanked population have had to find alternative ways of making payment transactions [27]. These alternatives are increasingly unsafe and inconvenient. South Africa has a deep mobile phone penetration that has exceeded bank account ownership. It remains a challenge to find ways to bank the unbanked [24]. There are many mobile networks in communities across South Africa, most of which are in places where the unbanked population resides. Such coverage offers MFSs as a feasible option for banking the unbanked [38] [24].

Ondrus and Pigneur observed successes with Mobile Payment (mpayment) in Asia [75]. There have also been successes in some European countries. Ondrus and Pigneur remark that mobile phones are ready for RFID technology, as demonstrated by the ubiquity of proximity and contactless payment systems deployed in Asia. These make mpayment very convenient, safe and cost-effective and have many more benefits over other technologies [75]. A major challenge is in the aggregate dependence on locally closed networks. This problem stems from the non-existence of ratified global standards for deploying MFSs, and so it remains a proprietary solution. The challenge could be met by NFC. With more NFC-enabled devices forming interoperable platforms for multiple consumer applications, more opportunities are being created [75] [86].

1.3 Research question and overall approach

Technology provides the opportunity to avoid or resolve some MFS challenges, such as CSCs having security features that deal with security challenges; RFID improving and optimising services in the services industry; and NFC offering an intuitive, simple and safe way to use a mobile phone like a CSC. In particular, applying NFC to MFSs for banking the unbanked remains, by and large, an unanswered question. An ideal system should be usable and secure, and trade-offs between usability and security pose major challenges for system designers [9].

The cost of MFS transactions can influence consumer adoption should the cost be passed on to customers [61]. We consider the total cost to constitute the price and the transactional cost [52]. The typical transaction cost includes the time and effort needed to locate and pay for a good or service. While existing card payments are suitable for most purchases, their transaction costs are too high for the unbanked [52]. Thus, the main research question of this study: ***"How can Near Field***

Communication be used to support mobile financial services?". This research question raise three other questions based on the challenges identified in the previous section:

- How can NFC be used to secure MFSs?
- How can NFC be used to improve the usability of secure MFSs?
- How can the trade-offs between usability and security be balanced to minimise transaction costs in NFC-based MFS systems?

To answer these research questions, we built NFC-based prototypes and conducted a background study, security attack results and two user studies. The background study involved three research activities: a focus group, a demographic survey and a preliminary survey. The focus group activity consisted of seven participants who were all students or non-academic staff at the University of the Western Cape (UWC). This activity took place in the last week of February 2009. It took the form of a round-table discussion during which questions and ideas were posed and respondents' answers where recorded. Sampling was random, but not representative. The demographic and preliminary surveys had a different set of 20 students from rural areas as participants. Sampling was random, but not representative. Data collection employed both quantitative and qualitative methods. In this study, a Personal Computer (PC) simulation of an NFC payment application was built to support experimentation in the laboratory.

In following an incremental model and based on the requirements gathered from the background study from using the NFC payment emulator application, we designed and developed an Mobile Banking (mbanking) application called NFCbankme. NFCbankme allows the user to perform simple banking transactions that include transfers, information requests such as balance checking, and withdrawal and deposits. When this application was completed, our request to perform the actual user testing in a live banking environment was rejected by all the banks we approached. We therefore performed no user testing on this particular system. Security attack tests were performed using NFCbankme within a laboratory environment.

In a bid to continue with the project, we rebuilt NFCbankme into two different prototypes based on mpayment and Mobile-to-Mobile (M2M) money transfer: NFCpayme and NFCme2u. The former made use of the balance-checking protocol from the NFCbankme prototype while the latter used the money transfer protocol from the NFCbankme prototype.

In both user studies I and II, NFCpayme and NFCme2u prototypes were used to support the studies. For both users studies we added 20 additional participants, making the total number of participants 40. These 20 new participants were made up of temporary migrant workers from rural areas in South Africa that had come to the Western Cape to seek work. The user studies focused on security, usability and transaction cost.

1.4 Thesis outline

The rest of this thesis is organised as follows:

Chapter 2 discusses related work dealing with secure contactless MFSs using NFC. The section on MFSs explains mbanking services, mpayment solutions and M2M money transfer systems. The section on CSCs discusses the characteristics and features of CSCs, standards and compatibility for contactless payment systems. The section on NFC addresses RFID, characteristics and features of NFC, standards and compatibility, and implementation approaches.

Chapter 3 presents the research design and methodology for this work. It identifies the research gaps, presents the research questions, explains the research approach and lays out the experimental design.

Chapter 4 explains the design and implementation of three NFC-based MFS prototypes: NFCbankme, NFCpayme and NFCme2u. Separate sections on each prototype presents an overview and discuss requirements for the design, architecture, the protocol and implementation.

Chapter 5 presents an analysis of the results background study, security attack tests, and user studies I and II. The results presented show how we use NFCbankme and NFCme2u to study security, NFCpayme and NFCme2u to study usability, and NFCpayme to study transaction cost.

Chapter 6 concludes the thesis with a discussion of conclusions, recommendations and the future work that is needed.

Chapter 2

Related work

This chapter discusses work related to secure contactless MFSs using NFC. Section 2.1 introduces work related to MFSs, including mbanking, mpayments and M2M money transfer systems. Section 2.2 describes work related to CSCs, including standards, technologies, Application Programming Interfaces (APIs) and their connection to payment services. Section 2.3 addresses work related to NFC, tracing its evolution from RFID, with technical specifications and APIs. Section 2.4 summarises this chapter.

2.1 Mobile financial services

MFSs encompass a broad range of financial activities that consumers engage in or access using their mobile phones [91]. There are three main forms of MFS offerings: mbanking, mpayment and M2M money transfer, which describe distinct but sometimes overlapping sets of products [25] [5]. Users find mbanking valuable because of the inherent time and place independence and the overall efficient effort-saving qualities. With mpayment, a mobile device is used to carry out payment transactions in which money is transferred from payer to receiver with or without an intermediary [61]. M2M money transfer involves transferring money via international or national remittance hubs from or to a real bank account or a mobile wallet [90]. These three forms of MFSs are themselves subsets of the broader domain of electronic banking, electronic payment and electronic money transfer, respectively [81]. This section addresses each topic in terms of three main themes: categorisation schemes, trade-offs between security and convenience, and how technology contributes to relevant research solutions. There are also three minor themes: timing, cost and usability.

2.1.1 Mobile banking services

Mbanking is defined as the provision and availability of banking and financial services via mobile telecommunication devices [91]. Usually, mbanking is a solution for customers with existing bank accounts to get connected to their bank or financial institution over a mobile network [70]. Mbanking offers customers ways to check balances and view transactions on a mobile device. Customers can also carry out credit or debit card management, which can be adopted for unbanked customers. Such solutions offer customers access to financial services via a mobile wallet [81]. For many customers, mbanking presents a delicate balance between a conceptually powerful opportunity (to be able to transact any time, anywhere) and practical challenges (such as menu sequences presented on a small screen and the need to use tiny buttons) [32] [9].

Mbanking schemes can be categorised into three types based on bank-related services: mobile accounting, mobile brokerage and mobile financial information services [91]. Mobile accounting involves the use of non-informational banking services that are specific to a particular account, such as remittance facilities and access administration [93]. Mobile brokerage refers to transactions such as buying and selling financial instruments [93]. Mobile financial information services refer to banking and financial services that are of a purely informational nature relating to either one's own bank account (s) or market developments [93].

An alternative categorisation of mbanking uses two models: the additive model and the transformative model [81] [43]. The former model considers the mobile phone as merely another channel to an existing bank account. The transformational model considers the financial product linked to the use of the phone as targeted at the unbanked, who are largely low-income earners [81].

Some mbanking platforms offer services, such as money transfers, which are considered forms of payment. Some mpayment products are so closely linked to bank accounts as the source of funds that they also presume mbanking functions [70] [36]. From the user's perspective, mbanking services may be active, such as client-driven account inquiries and transfers, or passive, such as automatic low-balance notifications. Mbanking mirrors both online banking and traditional high street banking in developed nations where most people have bank accounts. It is provided predominantly by banks, as they extend their customer services to mobile phones [37].

In terms of security associated with mbanking, Kreyer et al. defined security to include the integrity, authorisation, authentication, confidentiality and non-repudiation of transactions, and the issue of subjective security from the viewpoint of the customer [47]. Kreyer et al. view convenience to include ease and comfort of use, as well as the attainment of concrete benefits through such use [47]. According to Nie and Hu, a convenient, efficient and effective mbanking service has been a key determinant for customers when deciding to take up or continue with mbanking [73]. Security is fundamental to the success of mbanking development [73].

Customers using mbanking should gain increased convenience, access and the opportunity to easily detect account problems such as insufficient funds [75] [65] [67]. When compared to internet banking, mbanking can appear much more secure and user-friendly. Users tend to have a more personal attachment to their mobile phones than to their PCs [24]. This relationship leads to better protection of the physical security of the mobile phone. This also portends to the usage and lifestyle of mobile phone users, since there are more users of mobile phones than of the internet [61].

Mbanking employs many channels to deploy services, such as SMS, Interactive Voice Response (IVR), Wireless Application Protocol (WAP) and Standalone Mobile Application Clients (SMAC). SMS is the most prevalent channel [24]. SMS-based mbanking has proven to be very feasible, given that the SMS service enjoys wide support among mobile phones [40] [53]. In South Africa, the use of SMS-based cellular phone banking is gradually growing among banked customers, but is less pronounced in the unbanked market [23]. According to Donner, SMS technology is the most popular and cost-effective service suitable for mbanking in developing countries [23]. However, security remains a huge concern [9]. Services such as gaining access to one's account balances and statements, upgrading one's overdraft instantly, making and managing investments, and making payments and transfers are all provided via cellular phone banking.

SMS-based mbanking services can be operated with both push and pull messages [40]. Push messages are those that the bank sends out to a customer's mobile phone without the customer initiating a request for the information [53]. Such messages include mobile marketing and the use of a One-Time-Password (OTP). Pull messages are those that are initiated by the customer via a mobile phone for the purposes of obtaining information from or performing a transaction with a bank account [40]. Such messages include account balance enquiries and requests for current information, such as currency exchange rates and deposit interest rates on deposits.

In terms of timing associated with performing the MFS transaction, mbanking services are valued by users because of the inherent time and place independence, and overall effort-saving qualities [62]. Many mbanking services simply reproduce banking services already available online, with similar benefits for financial institutions. Such services enhance customer satisfaction and loyalty, along with increased account activity and related fee income, without the operational costs associated with bricks-and-mortar banking [62].

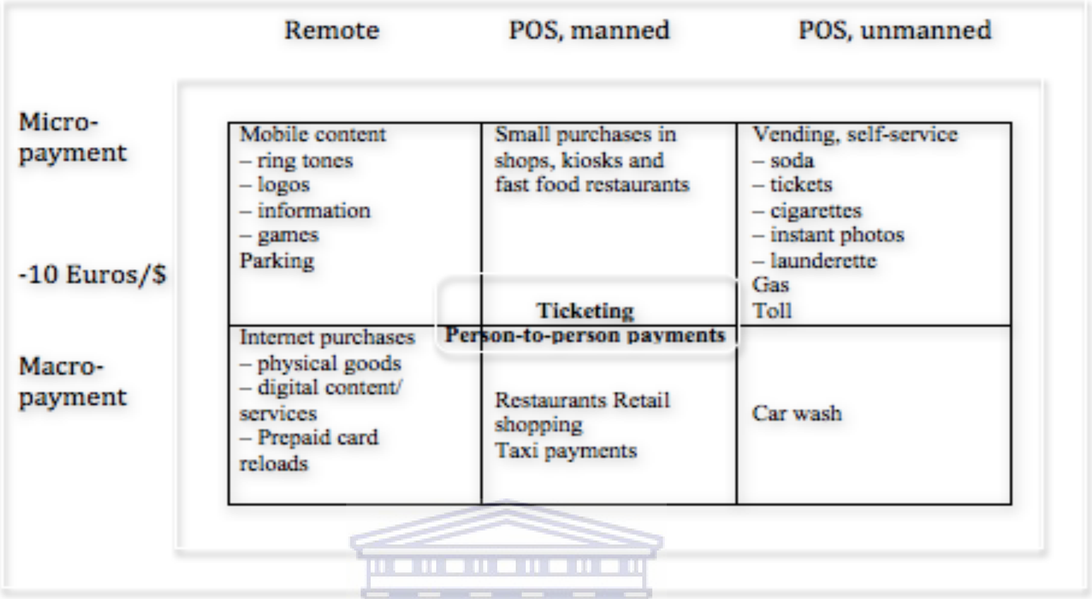
In economics, the term ‘transaction cost’ is used to refer to any cost, money, time, effort or other adverse effects associated with the task that incurred in the process of making an economic exchange [52]. The simplicity of a financial transaction is very important. In a study done by Mallat, the usage of SMS for MFSs is criticised because message formats are often complicated and slow to key in [61].

It is important that mbanking service systems strive to be usable and secure [52]. Raising the security level of a system may have an unfavourable effect on the system such as making its use more cumbersome and less efficient [9]. Similarly, bypassing or ignoring security features to making using the system easier often proves detrimental [9]. The less security-related activities interfere with user actions, the more likely users are willing to use security systems [52]. This trade-off between security and usability is proving to be a challenge for many mbanking systems [9]. The usability and security of a system have been shown to be sensitive to similar vulnerabilities during the design, development and testing stages of a system [9]. Usability and security are often shown to be in conflict in security features of a system or products [52].

2.1.2 Mobile payment solutions

Mpayment enables customers to make credit card and bill payments anytime, anywhere, from either a bank account or a mobile wallet [92]. Compared to cash and/or CSCs, mpayments have the advantage of not necessarily being tied to a physical Point-Of-Sale (POS), allowing more flexibility over their manner of use [52]. Furthermore, mpayments can involve the purchase of both physical and digital goods [22].

Mpayments are commonly categorised into micro- and macro-payments, with the distinction between the two occurring at approximately ten euros or their equivalent [62]. Mpayments are further subdivided into remote and proximity payments, depending on whether the transaction takes place at the POS or remotely via an electronic network (refer to Figure 2.1). The most obvious differences between proximity and remote mpayments have to do with speed and convenience. The use of NFC-based proximity mpayment eliminates third-party payment processes or accounts. Proximity mpayment data is linked directly to a payment card issued to the consumer by a trusted financial institution [4].



	Remote	POS, manned	POS, unmanned
Micro-payment	Mobile content – ring tones – logos – information – games Parking	Small purchases in shops, kiosks and fast food restaurants	Vending, self-service – soda – tickets – cigarettes – instant photos – launderette Gas Toll
-10 Euros/$		Ticketing Person-to-person payments	
Macro-payment	Internet purchases – physical goods – digital content/ services – Prepaid card reloads	Restaurants Retail shopping Taxi payments	Car wash

Figure 2.1 **Mpayments framework**
This figure illustrates the distinction between micro- and macro-payment and also direct access. P2p payments sometimes overlap with the different types of payments as seen in this diagram.
Source: [4] [62] [47]

Remote mobile micro-payments enable the purchase of mobile content and/or services such as news, games, tickets and location-based services [62]. Mobile micro-payments at unmanned POSs include buying soft drinks or items from vending machines and making payments at self-service stations [62]. Mobile micro-payments at manned POSs include small purchases at shops, kiosks and fast-food restaurants [62]. Proximity payments involve the use of short-range messaging protocols such as Bluetooth, RFID and NFC to pay for goods and services over short distances [92].

Two types of mpayment can be based on the validation of tokens exchanged: offline and online [47]. Offline mpayment involves no third party during the mpayment procedure and the tokens exchanged between the two transacting parties can be verified without external help [92] [62]. A typical example is an electronic voucher (eVoucher) transferred in mobile wallets [92]. On the other hand, online mpayment assumes that in an mpayment procedure, the tokens exchanged can be verified by contacting an trusted external trusted entity [47] [16].

Security and convenience are suggested as the key drivers for the growth of MFSs [62]. Consequently, to increase adoption, mpayment solutions must show clear advantages in terms of speed and convenience over traditional payment options [15] [63]. Transaction speed and convenience have often been cited as the main benefits in terms of cashless payment [63]. In addition, the complexity of an mpayment service and the extra effort required of customers are strong barriers to adoption by consumers. Mobile phones tend to have small physical or virtual keyboards and can be quite tedious and challenging for data entry [63] [51]. Tasks such as filling out forms and typing in credit-card numbers are difficult on a mobile phone.

Security challenges have shown to be a significant factor affecting mpayment [51]. Some technologies used to support mpayments have inherently weak security. For example, SMS is vulnerable to snooping, spoofing, message interception and social--engineering-based bypasses of security measures [51]. As a consequence, if a consumer were to lose a handset configured for mpayment and the thief uses the stolen phone to make purchases, a carrier may force the victim to pay for any unauthorised charges.

Mpayment systems come with risks that threaten to undercut and hamper industry growth [63]. The challenge exists for MFS providers to balance convenience and security to ensure that both users and providers are fully protected against fraud and data theft [51]. Massoth and Bingel argue that NFC is a good choice for mpayment with regard to speed, security and usability, and stands to be the most likely candidate for an mobile commerce (mcommerce) killer application in the near future [63].

In recent years, the methods of providing mpayment services have multiplied, including SMS, voice, WAP and NFC [16]. It has been noted that contactless technology has a high ease of use in comparison to other technologies [51]. Ease of use suffers from voice callback for set up and can be problematic with SMS--based and infrared-based systems. Bluetooth provides solutions that are easier to use than infrared, but are not as convenient as NFC [51]. The two technologies that have emerged as leaders, each with distinct benefits and limitations, are SMS and NFC. Other emerging technologies include those that make use of mobile phone web browsers, Bluetooth or downloaded software. Unlike NFC, these other technologies are similar to SMS-based approaches in not requiring special hardware [95] [63]. In contrast to NFC, SMS-based mpayment systems employ a text-messaging protocol to exchange transaction data via brief instructions transmitted to payment providers that in turn process the respective transactions.

Kungpisdan et al. proposed a secure account-based payment protocol that is suitable for wireless networks [48]. This protocol employs symmetric-key operations, which require lower computation for engaging parties than existing payment protocols [48]. It also satisfies transaction security properties provided by public-key-based payment protocols. Formal analysis shows that it achieves the goals of payment protocols [48]. Additionally, vital financial information is not required to be sent during transactions, which results in in greater security.

A number of different costs are associated with mpayment. These includes, usage of energy, availability, compatibility and data. New Bluetooth products that have low-energy consumption such as Bluetooth 4.0 compare favourably with NFC products. NFC devices consumes less energy than Bluetooth devices, but when NFC is compared to infrared or Bluetooth technology, it is more expensive and limited in supply. NFC is capable of communicating with other devices such as connecting two Bluetooth devices. In contrast, low-energy Bluetooth devices are able to synchronise with classic Bluetooth devices, but not with other devices, as in NFC. Bluetooth usage at mobile terminals is very costly, however, with the highest costs incurred by IVR- and SMS-based solutions [63].

Ben-Asher et al. observed user behaviour concerning the trade-off between security and usability [9]. To obtain empirical data, Ben-Asher et al. developed a controlled research environment for studying a user's tendency to take precautionary actions as a function of the trade-off between system usability and the level of security the system provides. Ben-Asher et al.'s work shows that the likelihood of an attack clearly affected participants' behaviour. Furthermore, participants who were more frequently exposed to security threats tended to adjust the security level more often, especially when initially using the system. When the likelihood of a threat was low, participants adjusted the security level less and they actually remained largely at the initial and default security levels [9].

2.1.3 Mobile-to-mobile money transfer systems

M2M money transfer involves international or national remittance hubs and a real bank account or a mobile wallet [90]. Remittance by mobile is mostly about sending money from source to destination and may also include the payment of utility bills or wages, which sometimes overlaps with mpayment [88] [68]. A key driver for M2M money transfers, especially in developing economies, is demand from people without bank accounts. Thus, M2M is offered via mobile wallet services from mobile operators [11]. These services unify MFSs and M2M money transfer services into one offering and, worryingly for financial institutions, the service provider (SP) does not have to be a bank.

One way to classify M2M money transfer is based on the authentication procedure: symmetric or asymmetric [22]. Symmetric authentication involves both parties having the knowledge of a secret key. Asymmetric authentication is when each party possesses both public and private keys. To enforce transaction semantics, Balan et al. combine two protocols [7]: the atomicity protocol employed in NFC payment systems and the electronic wallet protocol. The atomicity protocol employs a two-touch payment protocol, where both initiator and the target must touch their phones twice to complete the transaction [8]. In the first touch, certificates are used to exchange identification information for the purposes of mutual authentication and to establish a transient secure shared key that protects the transaction against relay attacks and external tampering. In the second touch, a signed payment message is sent from the payers wallet, which is then verified by the payee's wallet and, if the verification is successful, the balance is updated. To complete the transaction in the second touch, an electronic receipt is sent back to the payer's wallet.

With regard to security and convenience, Taghiloo et al. propose a solution that can hold a user's payment information, provide digital certification to identify the user and send the information to speed transactions [90]. The consumer benefits because his/her information is encrypted against piracy and because some wallets will automatically input information at the merchant's node and can give the consumer the option of paying with digital cash or by cheque [90]. Balan et al. offer a compromise of using the security in 'mFerio' transactions processes and the security in the communication channel. In addition, Balan et al. argue that a good user protocol is worthless if tokens and/or the communication channel fail [7]. Similarly, a highly secure token is no better either if user protocols permit payments to the wrong party [7].

Dominikus et al. propose a protocol to secure their mCoupons systems against attack. These attacks include: issuing the same mCoupons multiple times, issuing one's own mCoupons, the manipulation of mCoupons to stay valid even after they have been issued, reproducing valid copies of mCoupons and cashing them in [22]. The mCoupons system of Dominikus et al. makes use of NFC without online access for client and issuer, secured by standard cryptographic means. A time-variant challenge-response authentication technique is employed to prevent attackers from listening in to the communication between the two parties in during authentication process.

Regarding M2M money transfer service technologies, both domestic and international remittances are shifting from traditional providers to wireless carriers that are able to compete for consumer market share on the basis of technological ubiquity and lower-cost services [47]. Mobile technologies have been shown to drastically lower the cost of remittances, as they remove the need for physical points of presence and ensure, a timely and secure method of transaction. The concept of e-cash has been shown to be extremely attractive to low-income users in particular [90].

Taghiloo et al. propose a new approach to digital wallets based on mobile devices without the need to exchange physical money or communicate via a banking network [90]. A digital wallet is a software component that allows a user to make an e-payment in cash (such as a credit card or a digital coin) and hides the low-level details of executing the payment protocol that is used to make the payment [90].

Pering et al. exploit the use of gestures that connect two devices to implement M2M money transfers [80]. Want et al. consider the use of RFID to bridge the gap between physical objects with virtual representations or computational functionality via various types of tags [94]. Balan et al. employ NFC for secure wireless communication due to its clear conceptual mode, convenience and speed, and inherent security as a result of proximity [7]. Furthermore, their mFerio system requires user authentication and makes use of the Secure Element (SE) [7]. This enables hardware-enforced security and, in combination with a secure monetary token, it met the requirements of being tamper-proof, impossible to replicate and resilient to theft [7].

When considering authentication algorithms, asymmetric authentication uses a private key to encrypt or sign a message and a public key to verify the encryption or signature [22]. This method is more time- and power- consuming, but has an easier key management process. In implementing monetary exchanges, Balan et al. use the Even-Goldreich-Yacobi protocol, because it is less tolerant of security compromises and requires fewer changes (mainly an extension for atomicity criteria) to be made than the mFerio [7].

In terms of transaction cost, the use of Rivest Shamir Adleman (RSA) contributes significantly to overheads, resulting in unsatisfactory timing. To avoid an extra level of overheads, a counter-based mechanism rather than a digital-coin-based mechanism is preferred [7]. In contrast, symmetric authentication has a complicated key management process and if the key of one party is compromised, the whole system is insecure and requires a new distribution, which can be costly. In addition, it is suited for cases where all the systems are under the control of a central coordinator [22].

The downside of a counter-based mechanism is its reliance on an SE. However, cellphones are equipped with an SE that makes it suitable for mFerio. Again, the two-phase commit protocol method that manages a distributed atomic transaction requires all the tasks to be distributed between only two nodes: buyer and seller [90]. The seller node can act as the coordinator of a distributed transaction to simplify the protocol [90]. Taghiloo et al. modify, the two-phase commit protocol to perform atomic transactions between two nodes, removing the extra overhead of a two-phase commit protocol.

Usability, among other things, is concerned with the user's psychological acceptance of the system [9]. Thus, a well-designed security mechanism requires more effort when it in use than when it is not being used [9]. Considering that the context of use is highly important to users, especially when they are under pressure to complete an activity, they will be tempted to cut corners. Consequently, Balan et al. propose an NFC-based mobile p2p payment application as an alternative to cash-based transactions, without the need for some back-end payment server, which will be usable and secure in terms of actual implementation and user perception [7].

2.2 Contactless smart cards

The term 'contactless technology' applies to short-distance communication between two devices that are not physically connected [79]. This permits a range of services to be developed. CSCs are smart cards that operate without making physical contact. They do not need to contact a reader or be read or swiped in a special slot [29]. Emerging areas for CSC applications include payment of transportation fares and toll fees, POSs, retail stores, electronic passports and visas [83].

2.2.1 Characteristics and features of contactless smart cards

A CSC is often employed in applications that require the protection of information or secure transactions [83]. Unlike contact smart card technology, CSC has an RF interface that makes it convenient when reading at a short distance [79]. The growing popularity of the CSC is due to its ability to offer fast and convenient transactions on mobile devices [92].

The contactless capability is built into a tiny RFID tag in the card. The intent is to provide the user with greater convenience by speeding checkout or authentication processes [66]. An important feature is that the CSC is passive; it does not have an independent power source such as a battery [29]. In addition, by using RFID, the card derives all of its power from the energy emitted though the card reader's RF transmission [83]. A possible handicap to CSC is that the architecture of a payment process is completely local with no front-end processing [43]. What is more, given that no Graphical User Interface (GUI) exists, the user depends fully on the host to provide the appropriate interface for a transaction.

A CSC has internal memory with a similar level of intelligence to that of a secure micro-controller [44] [29]. This enables a CSC to securely store and access information. In addition, a CSC can perform security functions such as encryption and decryption and carry out intelligent interaction via RF using a contactless reader [29]. A CSC can depend on NFC to send stored data on the smart card to host devices equipped with NFC readers. An example is the Sony FeliCa card, one of the most successful CSCs [43]. This CSC is able to represent prepaid credit by storing integer counters, and the reader can decrement the amount of available credit via a secret-key-sharing protocol.

2.2.2 Standards and compatibility

To handle security of information and communication, CSC technology is based on international standards like ISO/IEC 14443 that can restrict reading distance to centimetres [4]. A good number of CSC applications are standardised under ISO/IEC 14443, which specifies the RF signal interface, and initialisation and anti-collision protocols for the wireless interconnection of closely coupled devices [49] [83]. ISO/IEC 14443 operates at 13.56 MHz, with a bit-rate of 106Kbps and is designed for a range of 10 cm. ISO/IEC 14443 defines cards (always passive, A or B) and readers (always active, A and B) [4] [60]. Any ISO/IEC 14443 card (A or B) is capable of supporting communication from any initiating NFC device [11] [60]. Similarly, any ISO/IEC 14443 reader can start a communication with any NFC device (at 106 Kbps) [4]. Also, ISO/IEC 14443 uses the terms 'proximity coupling device' (reader) and 'proximity integrated circuit card' [95] [79].

2.2.3 Security and trust services application programming interface

There are two security and trust services (SATSA) communication API packages: SATSA-Application Protocol Data Unit (APDU) and SATSA-java card remote method invocation (RMI). The APDU is the communication unit between a reader and a card. The structure of an APDU is defined by the ISO 7816 standards [17] (refer to Section 2.2.3). Together with the generic connection framework SATSA provides an API that allows Java 2 Platform, Micro Edition (J2ME) applications to communicate with an SE such as a JavaCard, universal subscriber identity module or a security token smart card [17]. There are also two optional SATSA security packages: SATSA-Public Key Infrastructure (PKI) signature service API and SATSA-CRYPTO Cryptographic API. Both enable the security APIs to manage digital signatures and user credentials (digital certificates) and to perform cryptography operations [64].

The interface that enables access to the SE at the application layer is provided by the Java Community Process Program, which standardises using the features of an SE [60]. This API is called SATSA API for J2ME Java Specification Request (JSR) 177 and has four packages: a set of cryptographic functions; an API for handling PKI; Java Card RMI in J2ME for calling a remote JavaCard object method and for communicating with the SE via an APDU [57] [46]. The RMI package for JavaCards can only be used if the SE runs a JavaCard operating system (OS). In contrast, the SATSA-APDU package is used for communication with the SE, regardless of how the SE is implemented in the device. As long as the smart card chip is able to process the APDU, this API can be used [17].

A MIDlet is an application that uses the mobile information device profile of the Connected Limited Device Configuration (CLDC) for J2ME. A MIDlet application can use the APDU interface to communicate with applications on a smart card using the APDU protocol [17]. ISO 7816-4 defines the APDU protocol as an application-level protocol between a smart card and an application on the device. There are two types of APDU messages: command and response [17]. Command APDUs are sent to smart cards by J2ME applications; response APDUs are the messages received from smart cards.

2.2.4 A contactless payment system

These technological solutions are based on ISO 14443, standard, Sony FeliCa technology, RFID tokens and NFC systems [4] [49]. 'Osaifu-Keitai' is Japanese for 'wallet phone', which is an mpayment system developed by NTT DoComo in Japan [52]. It is a comprehensive alternative to both cash and credit cards that offers a range of services by including several payment applications on the same device. FeliCa is a contactless RFID smart card system developed by Sony, and is primarily used in electronic money cards and supports many CSCs [52]. Devices supporting Osaifu-Keitai are embedded with a FeliCa integrated circuit chip. Osaifu-Keitai allows users to have access to the same services on the same phone anywhere. It provides very fast payment without the need to count out change or provide a signature.

Osaifu-Keitai can top up store-value applications by accessing an online credit card or bank account via a cellular network. Automatic top-up from online credit occurs once the value falls below a required threshold [52]. A drawback of Osaifu- -Keitai mobile phones is that users cannot afford to lose them. Privacy is also another issue, as users are warned not to use their mobile phone in every possible payment situation. These drawbacks may suggest that users are more likely to make incorrect payments than when using physical cash. For instance, a user holding a mobile phone at a POS may be too concerned about loosing or being robbed of the mobile phone rather than focusing on entering the right inputs into the mobile phone it [52].

2.3 Near field communication

Many different variations of contactless technology exist today [63]. NFC is of significant interest to MNOs [16]. NFC is designed to operate over very short distances, typically less than four centimetres, and to provide a fast, simple and secure means for the user to use a range of contactless services with their mobile phone [63]. Thus, mobile NFC is a combination of contactless services with mobile telephony [86]. Unlike contactless payment tags, NFC devices can be linked to mobile wallets that grant accesses to multiple accounts or cards [90]. Although limited by definition to local (proximity) transactions, NFC technology can also be used to top up prepaid mobile accounts at merchant load stations (outlets), for mpayment services and/or to facilitate in-person M2M transfers between two users with NFC-enabled devices [11].

2.3.1 Radio frequency identification

During World War II, RFID was used by the Allied forces to identify aircraft as either friend or foe [29]. The reasons for the recent rapid and escalating use of RFID technology include the advanced miniaturisation of chips and component devices; the constant decrease in price,which makes the use of RFID economically viable in ever-increasing areas of application; and the establishment of widely accepted standards [14] [74]. RFID systems generally have an antenna and a transceiver in a reader and a tag (also known as a transponder). The antenna transmits a signal to the tag that activates the transceiver using radio frequency waves, to the tag then transmits data back to the antenna [74] [13].

The latest trend within the RFID family of technologies is a more sophisticated proximity card. Advanced proximity cards can be standardised and embedded in mobile devices. The NFC proximity standard creates new possibilities as NFC readers can be built into mobile phones. As a consequence, NFC is an extension of RFID [75]. However, RFIDs have been shown to be vulnerable to threats such as denial of service attack, replay attack, lack of forward secrecy and privacy concerns. As RFID gains popularity, security- and privacy-related issues raise more concerns [96].

2.3.2 Characteristics and features of near field communication

The characteristics and features of NFC mostly derive from combining the functionalities of an RFID reader device and an RFID transponder in an integrated circuit [95]. NFC is restricted to a range of four centimetres, whereas RFID has the ability to transmit beyond a few metres. This restriction in range makes NFC an inherently more appropriate technology in terms of security [95]. NFC-enabled devices can communicate with one another and with any existing RFID infrastructure, such as readers and CSCs [92].

The NFC standard defines two different modes of communication [16]: active and passive. The active mode has both devices generating an RF signal on which the data is carried, whereas the passive mode has only one NFC device generating an RF field [2]. The passive NFC device, which is the target, uses a technique called load modulation to transfer the data back to the primary device or initiator [2]. As a result, no energy is required for reading out data stored and when it is switched off, the device still works. This feature can be employed for CSC applications.

NFC uses two different codings to transfer data. If an active device transfers data at 106 kbps, a modified Miller coding with 100% modulation is used [60] [72]. Otherwise, Manchester coding is used with a modulation ratio of 10% for all other cases.

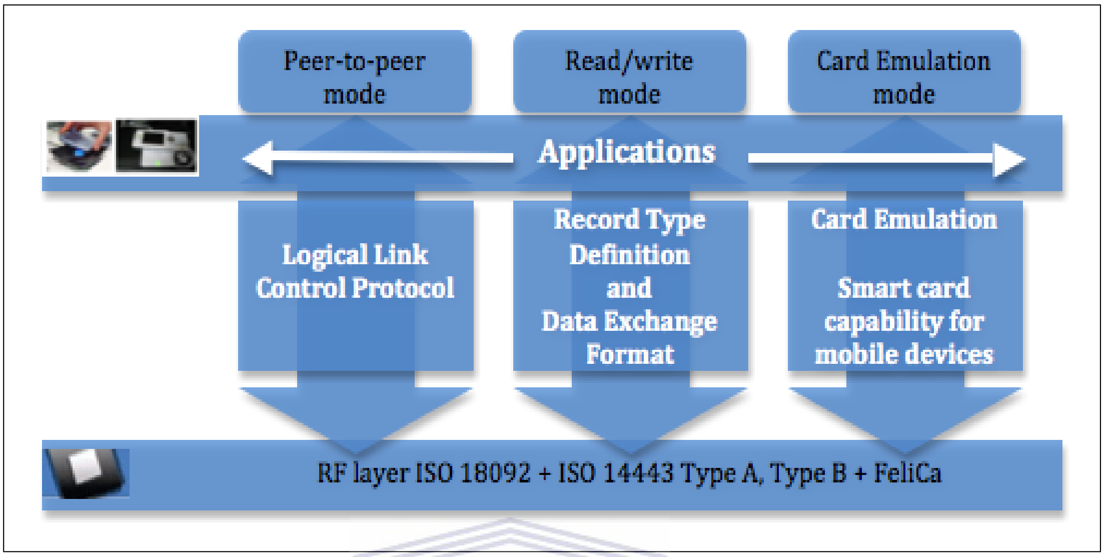

Peer-to-peer mode
Read/write mode
Card Emulation mode
Applications
Logical Link Control Protocol
Record Type Definition and Data Exchange Format
Card Emulation
Smart card capability for mobile devices
RF layer ISO 18092 + ISO 14443 Type A, Type B + FeliCa

FIGURE 2.2 **NFC communication modes**
NFC technology is compatible with existing contactless infrastructure. Mobile devices that have an NFC interface can operate in three modes: emulating smart cards, acting as a reader terminal (when the NFC enabled device reads a passive RFID tag) and realising p2p communication (both communicating devices are in active mode, sending messages to and receiving them from to each other).
Source: [95]

An NFC-enabled device can have three modes of operation (refer to Figure 2.2) [16] [95]: p2p mode, read/write mode and card emulation mode. The p2p mode involves two NFC devices exchanging data and this is standardised in ISO 18092 [16]. For instance, it is possible to transfer data such as electronic business cards or digital photos between two NFC-enabled devices by 'touch', i.e. by bringing the two NFC-enabled devices close to each other. In the read/write mode, NFC devices are able to read NFC tag types, such as an NFC smart poster tag. In card emulation mode, an NFC device is enabled to emulate an NFC tag and an ISO/IEC 14443- or FeliCa-compatible smart card, thus appearing to an external reader much the same as a typical CSC. In card emulation mode, it enables an NFC device for contactless payment or as an electronic ticket.

These three NFC modes are based on ISO/IEC 18092 NFC IP-1 and ISO/IEC 14443 CSC standards. P2p mode is defined for device-to-device link-level communication and is not supported by contactless communication API [59]. Read/write mode is compliant with ISO 14443 and FeliCa systems and it enables applications for the transmission of NFC Forum-defined messages [95]. Although this is not secure, it is supported by a contactless communication API [59]. Card emulation mode allows an NFC-enabled device to act as a standard smart card. This mode is secure and supported by a contactless communication API [59].

The transfer of data in NFC is based on an inductive coupling at a frequency of 13.56 MHz [11]. Any NFC transaction requires two parties: an initiator sending the data and a target receiving the information [11]. The transfer speed is negotiated between the initiator and target and the data transfer is half-duplex, since at any point in time only one of the devices is in sending mode, while the other is in receiving mode [2] [95]. Consequently, the receiving device draws powers off its RF and will only listen to data sent over RF by the sending device [60].

2.3.3 Standards and compatibility

ISO/IEC 18092 is an RFID standard that shares similar applications with CSC systems. This standard is designed for larger devices like cellphones, PDAs and laptops and led to the emergence of NFC-enabled handsets [11] [4] [72].

The NFCIP-2 standard defines a gateway mechanism between ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 18092 interface standards [11] [95]. The following features of NFCIP devices are of interest: they have additional communication channels such as WiFi and global positioning system (GPS); they have convenient and powerful programming interfaces; and, finally, they are capable of acting both as a reader and as a tag [45] [95].

2.3.4 Contactless communication application programming interface

JSR 257 defines a standard API for contactless communications with RFID/NFC tags or bar codes At the moment, it is supported by many mobile phone vendors. This specification defines the J2ME Optional Packages for contactless communication [11][86]. JSR 257 is used to provide a small amount of information to applications from some other medium such as links to content and identifiers for services. It also allows the user to to discover and exchange data with contactless targets such as NDEF tags, RFID tags and external smart cards [34] [95]. The NDEF tag is a data packaging format specified by the NFC Forum to exchange information between an NFC device and another NFC device or with an RFID tag.

Thus, the contactless communication API provides a connection to any physical target that supports NDEF [76] [95].

RFID tags require connecting to a web page by scanning an RFID or a visual tag (bar code) in the corner of a movie poster, or calling a friend by touching an RFID tag that contains the appropriate phone number these are two of the use cases that contactless communication API enables [76] [95]. Thus, this API provides a mechanism to discover contactless targets and communicate with them [95].

External smart cards are able to communicate with this API because of the discovery mechanism. In addition, communication with ISO 14443-compliant smart cards is executed using APDU commands. A device that contains RFID hardware is capable of emulating a CSC to an external reader device. Consequently, this feature is called card emulation mode. For example, with transportation tickets, the device contains, for example, bus tickets and the external reader in the bus reads one ticket from the device [95]. For these situations, the API provides a notification to the application that the SE in the device has been accessed via the RFID hardware.

2.4 Summary

MFSs involve mbanking, mpayment and M2M money transfers, and these three sometimes overlap. For each MFS, this chapter has discussed issues pertaining to security, usability and transaction cost. SMS is widely supported on most mobile phones, but many SMS-based MFS issues are still unresolved. CSC provides the possibility of securing MFS transactions, and the associated standards were presented. The API that helps to develop the CSC-based MFSs using ISO/IEC 14443 was discussed. It was suggested that NFC technology is more suitable than SMS in terms of the added security and convenience that it offers. NFC technology, which is an extension of RFID, can enable a mobile phone to act as a CSC. The characteristics, features, standards, and compatibility of CSCs and NFC were addressed. The SATSA and contactless communication API are libraries for the CSC and NFC, respectively. These APIs provide the needed support classes for developing MFS software.

Chapter 3

Research design and methodology

The main challenges facing MFSs are security, usability and transaction cost. Section 3.1 of this chapter expounds on the challenges discussed in Chapter2. Section 3.2 poses the research questions, while Section 3.3 addresses the research approaches that are used. Section 3.4 lays out the experimental design including sampling, data collection and analysis. Section 3.5 discusses data-editing and -coding, validity and reliability procedures. Section 3.6 presents the ethical considerations affecting the research and Section 3.7 concludes the chapter with a summary.

3.1 Challenges for mobile financial services

Two themes permeate the related work: security and usability. These themes are often at cross-purposes with one another. This section explores how technologies impact on the provision and perception of security and usability/convenience for MFSs. It follows that a transaction cost becomes attached to the amount of user effort put into using a particular MFS system. This section thus examines the related work with respect to security and usability, the resulting transaction costs.

According to Donner, SMS technology is the most popular and cost effective service suitable for mbanking in developing countries [23]. In South Africa, the use of SMS-based cellular phone banking is gradually growing, although it is less pronounced in the unbanked market [23]. The major concern is security [9]. SMS is supported on nearly all mobile phones and as such, most phones can support SMS-based mbanking [28] [54]. Security limitations persist in the Global System for Mobile Communications (GSM), which is an important data transmission medium used in the delivery of SMS messages, thus indicating the security flaws inherent in such a system [77] [16].

Barkan et al. explain that the lack of data integrity in the GSM is a shortcoming [8]. The A5 algorithm is an important mechanism for authenticating a handset on a mobile phone network. This algorithm has been reversed engineered. The A5/1 variant has experienced three attacks in Europe, while the A5/2 variant was broken in less than 24 hours [82] [8] [19]. A similar problem exists with two other algorithms: the encryption algorithm for authentication, and the cipher key generation algorithm. The former is referred to as A3 and the latter as A8. These two algorithms are together known as COMP128, which is still being used in a vast number of SIMs. COMP128 was broken by Wagner and Golberg in a day [19].

In another study, Al-Tawil and Akrami explain security issues surrounding SMS itself [3]. According to Al-Tawil and Akrami, during the initial phase of SMS development, security concerns such as mutual authentication, non-repudiation and confidentiality were not considered. As a result, the end-to-end security later became a challenge, in terms of the ability of service provider personnel to gain access to plaintext SMS messages stored in the SMS centre. Beside encryption between the mobile station and the base transceiver station, there is no end-to--end security. Therefore, there is a possibility of altering a sender's message field to a different alpha-numeric string [19].

Certain security features and/or characteristics qualify an MFS system as having an acceptable level of security [16]. These features include making it impossible to reuse payment information in a bid to counterfeit or replicate the payment system's VM (or monetary representation), ensuring that any form of tampering with or alteration to the payment system's VM status renders it permanently unusable, and prohibiting the tracing if a particular payment transaction to participants in the transaction from within the system in order to enforce privacy by way of strong anonymity. In addition, cryptographically storing VM inside the phone makes the system resilient to theft [6]. A roll-back transaction of all or nothing that properly defines transactions semantics can be enforced. In essence, any interruption during a transaction should result in the cancellation of the entire transaction. This will provide strong assurance that a transaction's semantics are upheld.

Ghron et al. follows a user-centred approach via prototyping and usability tests for an NFC-based virtual ticketing application. They obtain a balance between the information reduction required by the user and the increase of application flexibility [32]. From Ghron et al.'s point of view, the application service will not only be less complex, but also less expensive and as a consequence, this will translate into more convenience for a broad community of users [32]. Donner states:

> *"Even the simplest handsets have features buried deep in menu structures. If navigating an m-banking/m-payments interface is difficult for experienced mobile users with bank accounts, even greater is the difficulty for first-time users in the developing world, many of whom will have only been using a mobile for a year or two"* [25].

Cheng et al. argue, that most trials only use NFC-enabled handset as a CSC, which does not really reveal the true potential of NFC technology [18]. Aigner et al. show that the user's attitude to the system is based on the very intuitive usability of NFC, by simply touching NFC targets with a mobile device for picking up and cashing in of mCoupons [22] [55]. Therefore, it is important to study the different interaction mechanisms that offer varying trade-offs between security and usability [9]. According to Ben-Asher et al., little empirical data is available on user behaviour regarding the trade-offs between security and usability [9].

The effort associated with the security and usability of an MFS system can be considered as a transaction cost – such costs include, any cost in terms of money, time, effort and/or other disutility that contributes to the total cost of service [9] [52]. The amount of money involved in a given payment transaction might influence the willingness of how much effort and/or distraction is associated with the security and confirmation processes that a user is prepared to accept [52] [9].

From section 2.2.4, it was clear that Osaifu-Keitai introduces new security problems and risks. Thus, these problems might prove to be far more costly than those resulting from the use of physical cash payments and there is the fear of losing the Osaifu-Keitai mobile phone. Transaction cost analysis suggests that cryptographically secured e-cash accessible via NFC interfaces is most suitable for small-value purchases [52] [63]. Nevertheless, the appropriate level of security would be a balance between the costs as a result of security implementation and costs due to the risks of not implementing security [52]. Consequently, finding a balance between usability and security in implementing NFC-based MFS system can help minimise overall transaction costs.

3.2 Research questions

As previously indicated in the introduction, the main research question that this study answers is: ***"How can Near Field Communication be used to support mobile financial services?"***. This research question can be broken into several questions based on the challenges identified in the previous section:

- How can NFC be used to secure mobile financial services?
- How can NFC be used to improve the usability of secure mobile financial services?
- How can the trade-offs between usability and security be balanced to minimise transaction costs in NFC-based MFS systems?

3.3 Research approach

The overall approach was to develop and test out three MFS prototypes that are built with NFC to achieve CSC functionality with mobile phones. The aim was to explore the research questions on security, usability and transaction cost. A software development method (SDM) was supported by quantitative and qualitative methods to include user feedback.

3.3.1 Qualitative methods

Qualitative methods are used when there is a need to know how things happen and how they are related. Such methods provide the research with in-depth insight into the issues being researched. The main methods of data collection include focus groups and in-depth interviews [89] [30].

MFSs are a relatively new research area and there is little previous empirical work on the subject. A qualitative approach using focus groups was chosen to explore consumer adoption of MFSs [61]. Focus groups are a form of group interview using group interaction as part of the method [61]. This method can be used to examine what people think, how they think and why they think what they do. Previous research has demonstrated the feasibility of using this method to study innovative mobile services [61]. The strength of focus group interviews lies in the group dynamics and interaction that provide researchers with in-depth perspectives on the topic under discussion.

Qualitative research methods afford subjects the opportunity to give much richer answers to questions put to them by the researcher and may provide valuable insights that might have been missed if any other method is used. There is also a strong case for using qualitative research methods to complement quantitative methods [20]. This thesis reports on the use of focus group interviews, surveys, questionnaires, semi-structured interviews and observations to collect data.

3.3.2 Quantitative methods

Quantitative research is concerned with counting and measuring things, and producing estimates of averages and differences between groups [71]. The methods and techniques tend to specialise in quantities; the numbers come to represent values and levels of theoretical constructs and concepts. Such representation extends to the interpretation of the numbers and is viewed as providing strong scientific evidence of how a particular phenomenon works [87].

Quantitative methods often employ surveys using a structured questionnaire that contains predominantly closed-ended or forced-choice questions [33]. They have fixed response options and are have less capacity to provide in-depth insights, but supply more breadth of information across a large number of cases. Statistical tests are used for conducting the analysis. The general research approach employed in this study involves the use of laboratory experiments with end users. The data collection techniques used are surveys and interviews. We used the Statistical Package for the Social Sciences (SPSS) for carrying out data analysis.

3.3.3 Software engineering method and synthesis

The research process involved building prototypes to explore the issues of security, convenience and transaction cost. Both qualitative and quantitative methods helped to do so this. An exploratory prototyping process was employed, where an initial prototype was developed and fine-tuned in a sequence of stages towards a final system.

Figure 3.1 illustrates the model employed. A cycle is one sequence of a complete set of stages, as can be seen in a waterfall model [50]. Our experimental design employed multiple prototypes to elicit user feedback and experimental data. In Section 3.4.1, a simple prototype (emulator) is described. It was evaluated quickly and then redesigned based on the requirement analysis.

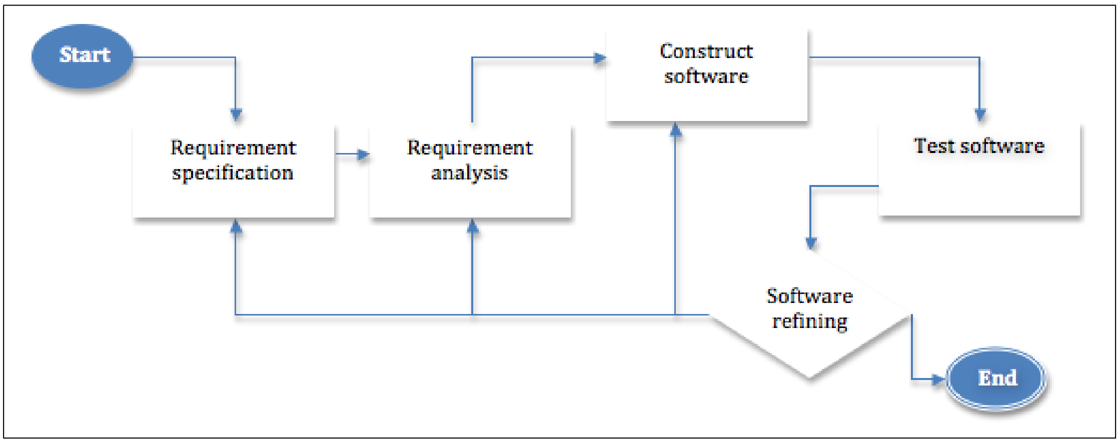


FIGURE 3.1 **The proposed software engineering method**
Exploratory prototyping comprises five steps, and an incremental model was used. The specification and analysis of requirements provided the overall objectives of the system and their individual functions. The software was written and the functions were tested against the requirements. If problems were encountered during this next phase, another prototyping cycle occurred, which could include another sequence of steps, until the development was stopped.

The requirement specification was used for the prospective prototype system. The prototype specification considered both the user's and designers point of view. This involved the examination of related systems and paying attention to the drawbacks of existing research and commercial systems in other to identify the challenges (see Section 3.1). In this step, an analyses of the requirement specifications were analysed and maps were drawn to connect them with the three NFC prototypes. In the software construction stage, the results obtained during the requirement analysis were incorporated into the implementation process.

Once the implementation of the software phase was completed, the software was tested from user and technical standpoints. The user was involved and user feedback was obtained. The main objective was to test the software with respect to security, usability and transaction cost. Based on the results obtained from testing the software, the original designs were adjusted and the implementation was re-constructed and tested once again with users.

3.4 Experimental design

This section explains how the research was carried out. Several studies were conducted for this work, in this order: background, security attacks, and user studies I and II (Refer to Figure 3.2). We provide details on each study including prototypes, sampling, data collection and tests. In total, four prototypes were

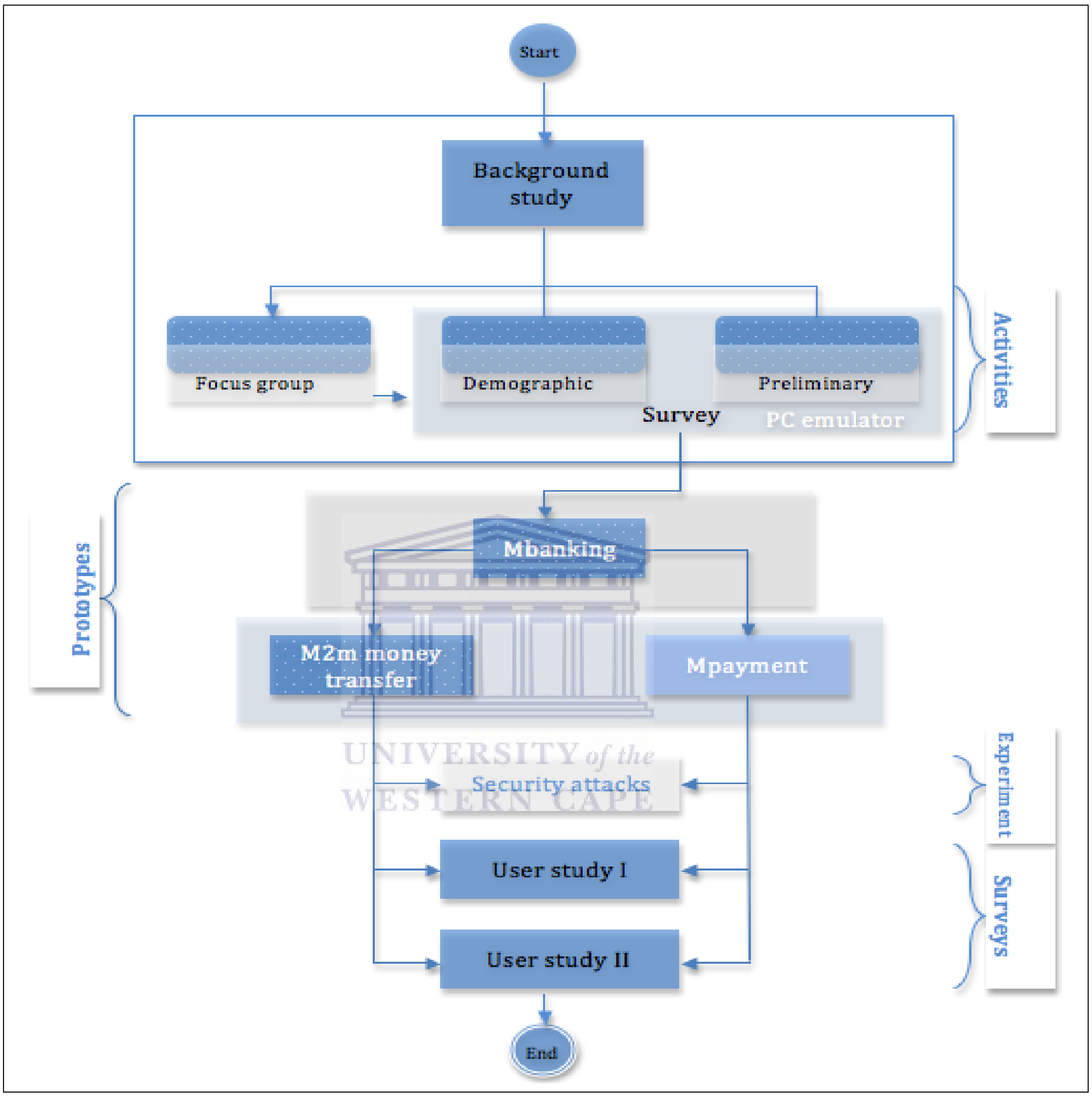


Figure 3.2 **Experimental design overview**
The figure illustrates the various research studies explained in this study. We began with a background study involving an initial focus group. Next, a demographic and preliminary survey was conducted. The next study involved the building of an mbanking prototype, which was later redeveloped into two other prototypes: mpayment and M2M money transfer. These two prototypes were then used to carry out two users studies in an incremental model. We also carried out security attacks on NFCbankme and NFCme2u prototypes.

built: a PC-based emulator for the demographic and preliminary activities during the background study, NFCbankme for mbanking, NFCpayme for mpayment and NFCme2u for M2M money transfer. The term ‘money’ here refers to VM on the phone. The last three prototypes were built after the background study was completed at the very beginning of the user studies. NFCbankme and NFCme2u were used to examine the security of MFS; the NFCpayme and NFCme2u were used to explore the usability of MFSs; and NFCpayme was used to evaluate transaction cost.

3.4.1 Background study

The background study consisted of three activities: a focus group study, a demographic survey and a preliminary survey (refer to Figure 3.3). The focus group study was carried out first. It laid the direction for the subsequent demographic and preliminary surveys. The purpose was to come up with ideas and information regarding the challenges MFSs faced in the community. Students from the UWC were randomly selected based on an open invitation on campus noticeboards a week before the actual study was conducted. The selection was not representative. The study took place for an hour on the 23rd of February 2009. Seven participants, the researcher and a hired research assistants were involved. The format for the focus group was session took that of a round-table discussion. Participants were also asked questions and the answers were recorded by both the researcher and the assistant. This activity was conducted in one of the conference rooms of the student residential hall on the UWC campus.

The demographic and preliminary surveys were conducted at the same time. The purpose of the former was to gather demographic information, while the latter was designed to discover if there was a need for NFC, in what ways NFC can be used, and factors and challenges that might influence users’ decisions. The intention was also to get a sense of the sample groups to target and to get feedback for the improvement of the subsequent study. These activities took place in March 2009. They activities were tailored towards a survey study. A PC-based simulation for a simple customer-merchant payment scenario using a mobile phone emulator was constructed to support the survey. The PC-based MIDlet emulator supported the study and users were able to interact and respond visually.

The sample consisted of 20 participants that were recruited by searching for students currently at UWC who where from rural areas. The ideal participant had social and economic ties with his/her rural household; and was often involved in payment or purchasing and the sending or receiving of money in one form or another to and/or from household members and/or acquaintances in rural communities. The first participant was randomly selected from among members of this group and then this person identified another participant, which in turn led to the next one, until we had the target number of participants.

This target number was based on the budget allocated for the study. The reason was that it was easier and less inexpensive to make use of this sample group. The participants were brought into a laboratory environment, the prototyped emulator was shown to them, and they were required to perform a set of simple tasks. Questionnaires on the laboratory experiment, were given to each participants to complete after the tasks were completed (refer to Appendix C). The feedback from these activities laid the foundation for the subsequent study. The next study involved the construction of prototypes.

3.4.2 Security attack study

The results of the background study informed the prototyping of NFCbankme. The results and challenges faced from studying the NFCbankme service led to the creation of two new MFS solutions: NFCpayme and NFCme2u. The NFCbankme prototype was initially an attempt to offset the constraints mentioned in Section 3.1 using SMS. This prototype was later re-constructed based on NFC. The attempt focused on developing a MIDlet application that would collect, processes and sends and receives messages via the hypertext transfer protocol (HTTP) or a GSM network to/from a bank server.

To ensure message integrity, message digest generated a secure message that was later sent to the bank server. Symmetric encryption was employed to ensure confidentiality, it required less computational overhead than either the asymmetric or PKI-based approach. The content was encrypted to maintain message integrity using a symmetric encryption algorithm that used an OTP known only to the customer and the server.

The NFCbankme prototype was tested in the bridging application and network group laboratory at the UWC. The NFCbankme solution was tested using the Kannel SMS gateway. The client-server test made use of a backend MySQL database. The transmission control protocol/internet protocol socket connection and Nokia 6131 emulator and phone were used.

The following tests were conducted on NFCbankme and the results are reported (refer to Chapter 5). A test using an OTP was conducted by attempting to generate a duplicate password. To ensure that the bank server was talking or listening to the right port, the Kannel (an open source WAP gateway that also works as an SMS gateway for GSM networks) was used.

The NFCbankme protocol encryption was based on existing security algorithms from GSM. A symmetric key encryption algorithm – AES from bouncy castle cryptography library, with a 128 bit key length – was used. Decrypting in the mobile phone was instrumented to record the time taken to accomplish tasks. The secure hash algorithm-I (SHA-I) algorithm was used to compute the message digest. Different alteration forms were performed on the messages digest bytes to see if a slight change, e.g. changing a single character, might produce a correct message or a different message digest. It was assumed that knowledge of the password was retained by the user. The symmetric OTP was only shared between the user and the bank server.

The use of the NFC interface with an SMS-based GSM network made a contactless authentication approach possible. Nevertheless, we used a PIN to provide authentication details to the receiver. It was presumed that the user would obtain the PIN when registering at the bank for his/her bank account number. The strength of the password selection strategy is determined the strength of the authentication.

Only unique OTPs were generated and stored in the server's database. A unique pair of the OTP and the sequence number that is used to encrypt the message was allowed for a single user. Consequently, the user could not deny not sending a message he/she had sent. In using the same sequence-password pair, the bank server was able to succeed in decrypt the encrypted data.

The security attack tests conducted included deliberately altering a portion of the content during transmission to cause a digest mismatch at the receiving end since a new digest was created. To test replay attack in a situation where a third party was in possession of the transmitted messages, we stored every received message in the bank server and performed security checks for the sequence number for a specific account identifier. The same message was retransmitted multiple times. Another test used was to attack the system armed with knowledge of the PIN and an invalid OTP.

In terms of the NFCpayme study, some basic activities take place inside an NFC mobile phone; remote transfer of data to the SE, reading data stored in the SE and sending it to the server. The Java software technology required for programming in the SE is called JavaCard. The NFCpayme is a cashless payment application, which requires installing a J2ME MIDlet and JavaCard application to simulate the SIM card that can be loaded with money to perform a purchase. The value is stored in the SE within the mobile phone. The complete NFCpayme prototype consists of contactless NFC-based mobile wallet application using JavaCard and a contactless reader.

An asymmetric authentication technique was used to replace the NFCbankmes symmetric authentication. Although symmetric authentication methods may achieve a similar task, complex key management makes them unattractive. Furthermore, once a key is compromised, all the entire communicating parties also sharing the same key are compromised, causing the entire payment system to fail. This informed the decision to use an asymmetric key with simple key management. It supports interoperability and it avoids existing security flaws that may arise because it uses a standardised protocol and algorithm [16] [35].

3.4.3 User studies

The discussion of the user studies in this section is organised as shown in Figure 3.3. The first prototype that was constructed was based on the outcome of the background study. This is the mbanking prototype we call NFCbankme. This prototype was expected to enable users to perform banking operations such as checking balances, and making withdrawals and deposita. It had client and server applications, with the client operating the NFC-enabled mobile device and the server expected to link with a bank server for testing. We were not able to find a bank that would allow us to test the system among actual users.

The solution was to redesign our ‘doing banking’ business case and develop two new prototypes. The first prototype, which we call NFCpayme, is based on the customer-merchant payment scenario from the background study, only that this time the prototype was the actual application rather than a PC-emulator. The second prototype, which we call NFCme2u, is based on money transfer systems such as the p2p payment systems. The construction of these two prototypes allowed us to proceed with the user studies. Two user studies were done in iterations: user study I and user study II. Both prototypes were used to support the user studies. For the second user study, the prototypes were refined to accommodate user feedback from using the prototypes in the first round.

The sampling methods for the two user studies were similar. The 20 participants from the demographic and preliminary surveys in the background study i.e. university students from rural areas, were retained for these studies. An additional 20 participants were added to make the total number of participants 40 for each user study. The extra participants were temporary internal migrant workers who had

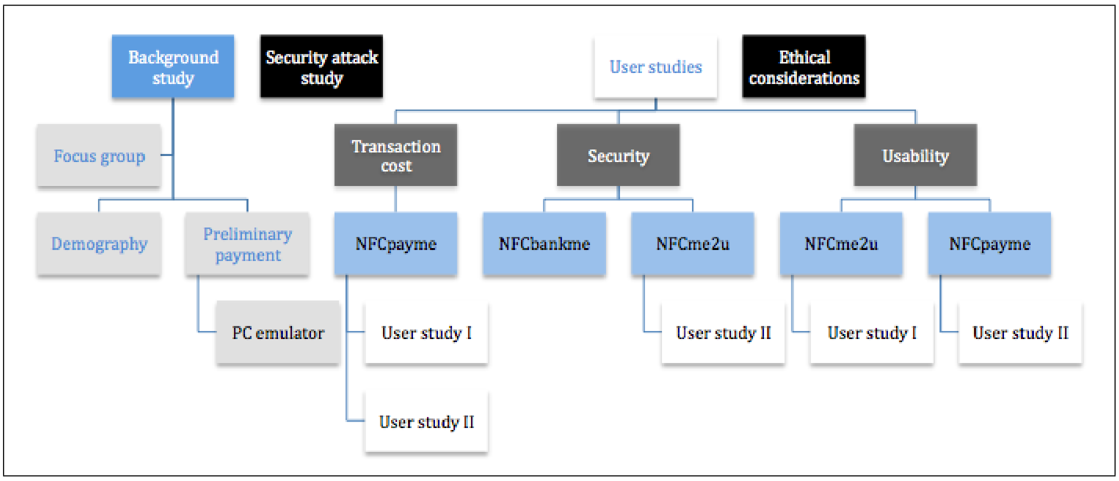


Figure 3.3 **Arrangement of discussions on the experiments**
The figure illustrate how the discussions on the background study, security attacks and user studies are arranged (see Section 3.4.3). These user studies involve discussions on security, usability and transaction cost issues (see Section 3.4.1). Four prototypes are explained in the figure: PC emulator, NFC bankme, NFCpayme and NFCMme2u are explained. Security attacks were mainly performed on NFCbankme prototypes on both with SMS only and SMS with NFC-based approaches (see Section 3.4.2). The figure also shows that discussions on the focus groups, and demography and preliminary surveys are provided (see Section 3.4.1): The ethical consideration for this experimental design are explained.

migrated to the Western Cape province in search of better economic opportunities for themselves and their rural households.

We refer to this new sample group of 20 as 'migrant workers'. Unlike the 20 rural students, the 20 migrant workers were identified in areas in Cape Town where most migrants are either searching for jobs or working. Samples were random, but not representative. Those selected were volunteers recruited to take part in this study as participants. The first user study was carried out in September 2009, while the second took place in June 2010. Each user study took a month to complete.

In both user studies, users were provided with a MIDlet on an NFC-enabled handset and asked to perform a set of tasks using the software (See Appendices C, D and E). A silent observer monitored the whole process. The observer was unknown to the participants and each participant was handed a questionnaire to complete at the end of the process. The questions were based on the experiments that had just been completed. The survey allowed the collection of user feedback data.

After the first user study, the prototypes were improved for the second user study based on the users' feedback. The first user study considered transaction cost and usability. The NFCpayme prototype was used to study transaction cost. The questions in the questionnaire focused on user perception of convenience, anxiety, completion time and predictable performance, and how much participants were willing to pay for using NFC. The usability study was supported by both the NFCpayme and NFCme2u applications.

We considered security using an NFCbankme prototype that was designed and developed based on the feedback from the background study and the challenges faced by MFSs identified in Section 3.1. Two protocols were constructed: check balance and money transfer, the former for simple banking transactions such as retrieving transaction details and the latter for sending and receiving money on mobile devices. The prototype was initially an attempt to offset the constraints discussed in section 4.1.5 and used SMS. It was later re-constructed by adding NFC to support security and usability. An NFC MIDlet client was used to collect, process, send and receive messages via HTTP and a GSM network to/from a bank server on a PC. The NFCbankme protocol encryption was based on existing security algorithms from GSM. The use of the NFC interface with an SMS-based GSM network allowed a contactless authentication approach to be possible. The NFCbankme solution was tested using the Kannel SMS gateway. The client-server test made use of a backend MySQL database.

In considering security using NFCme2u, we looked at two phases based on a set of user requirements from the background study and the challenges faced by MFSs identified in Section 3.1. In user study I, aspects of NFCme2u receipt features and authentication procedures were examined. In user study II, we considered the encryption, exchange of keys and overall security mechanism of NFCme2u. In the second user study, the security features of NFCme2u were implemented. System performance tests measured the time taken for security protocols to complete a transaction. The results of the security tests on NFCme2u are given in Section 5.2. Participants were given a questionnaire to complete at the end of each test. Participants were initially given a ten-minute Powerpoint presentation showing how NFCme2u is used. The task involved transferring money from one NFC phone to another.

When examining usability using NFCme2u in both user study I and II, we outlined the following set of user requirements for NFCme2u that we had gathered from the background study. These requirements were those of how easy the system was to use; how easy it was to learn; how fast it was to use, and its accuracy, predictable performance and availability. At the end of each test, participants were required to complete a short and a long questionnaire. In the former, simple questions using the Likert scale were asked on how easy they thought the tasks were, how confident they were during the experiments and whether the tasks were quick to complete. Users were asked to complete a NASA-TLX survey.

In user study I, the user interface as shown in Figure 4.3.5 was implemented on NFCme2u. The evaluation considered speed, ease of use and accuracy. In user study II, we tested the cognitive load of NFCme2u against the cash transactions by measuring their differences. The results of the usability tests on NFCme2u are presented in Section 5.3. Each participant took the experiment alone. The silent observer was at a distance pretending to also be participating in the experiment, but was actually monitoring the participants.

In user study II, NFCme2u was again tested with a similar setup, procedure system of data collection to that of user study I. Participants were required to perform eight tasks, four with NFCme2u and four with cash. Two use cases were examined using cash and NFCme2u: base and timed. The base case involved taking the baseline cognitive load results for cash and NFCme2u while the timed case set a time limit of 45 seconds on each task, which exerted more pressure on the participants to complete a task.

In user study II, an evaluation using NFCpayme to carry out an experiment was done. Three levels of security implementation for the payment scheme were adopted. These levels were ranked from the least to the most secure. This ranking also corresponded to with the least to the most effort required of the customers: automatic, light confirmation and strong authentication.

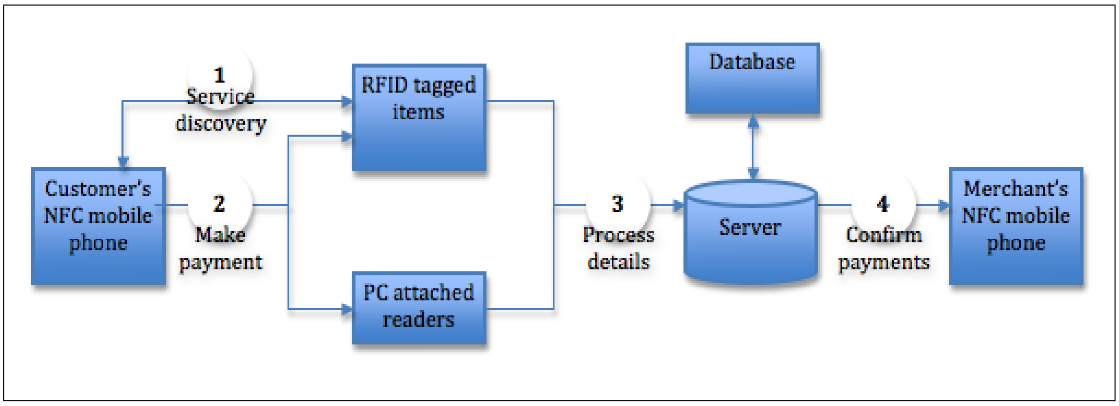


Figure 3.4 **NFCpayme sequence at kiosk**
Thus Figure illustrates a typical NFCpayme scenario between a merchant and a customer.

This level of difficulty or ease was informed by the degree of risk, amount of money involved and security confirmation that was necessary. The tasks were payment transactions and they involved checking balance and making a purchase using

	PIN	Menu	Proceed/ reset	Price or quantity	Proceed/ reset	Swipe to pay	Accept/ cancel	Receipt	Save/reject
Full authentication	Input PIN	Type input	Input PIN		Input PIN	✓	Input PIN	✓	Input PIN
Simple selection/part completion	Part completion	Simple selection MENU	X	Simple selection MENU	Part completion	✓	Click to accept	✓	Click to accept
Automatic	X	Default selection option	X	Simple selection MENU	X	✓	X	✓	Click to accept

Table 3.1: Security and usability trade-off table
This table provide details of stages involved in a payment transaction depicting three levels of distraction/convenience.

NFCpayme. The NFCpayme prototype set up had a server method that allowed communication to the mobile phone via HTTP and the phone method allowed the communication via the PC attached to an NFC reader (refer to Figure 3.4). Level one security involved inputting a PIN code and required user authentication at almost every major point in the transaction. The second level involved a simple part-completion technique, making selections and accepting confirmations from option menus. The idea behind the part-completion technique was to take the customer's password, randomise the position of each character and require fewer characters to be entered at login and different stages of the transaction by the customer (refer to Table 3.1).

Once the user had completed the set tasks by interacting with the NFCpayme system, the undertook a survey and a semi-structured interview using a questionnaire about each of the payment modes (refer to Appendices D and E). The questions focused on security, privacy, perceived convenience and reliability. The results for the time taken to complete each payment mode transaction were recorded. It was important that users provided information on the maximum amount they were willing to part away with using each of the payment mode.

We considered the transaction cost for both user studies, and improved the NFCpayme prototype based on the initial feedback. NFCpayme was rebuilt from the NFCbankme check/balance protocol. User study I was carried out based on the feedback obtained from the demographic and preliminary surveys, while user study II requirements were gathered from the first user study.

In the second user study, we also consider the NFCpayme solution. The environment in the laboratory experiment was set up to simulate a kiosk. There were five items with RFID tags attached to them, along with their information written on the tag. The tests for each user were done individually. Participants were shown a flash-based PowerPoint presentation explaining that the NFCpayme system provided an opportunity to demonstrate payment via NFC-enabled mobile phones and describing how to use the prototype. After a ten-minute training and preparation session, users were then asked to perform three sets of tasks on the NFCpayme system.

These tasks were to make a purchase using a services at a merchant kiosk, order the item and obtain proof of payment. These were done in three different modes: a strong authentication payment involving a PIN; a light confirmation payment involving the partial input of a PIN and requiring less authentication while purchasing the item (s); and an automatic payment done almost seamlessly and requiring very little authentication.

The equipment used include an NFC-based contactless reader connected to a PC-based server application and two NFC-enabled devices with the client application installed – one for the customer and another for the merchant (Nokia 6212 Classic and 6131 mobile phone, respectively). After completing these tasks, users were required to complete a survey that contained questions on perceived convenience, security, privacy and reliability. They were also asked about the largest amount they were prepared to pay to use the different interaction modes. The time taken by each participant to complete the transactions was recorded, as it was instrumented on the mobile phone.

3.5 Data editing and coding, validity and reliability procedures

This section presents more information on the data collection, validity and reliability procedures used. Certain key areas were considered during the process of checking and adjusting data: omissions, legibility, consistency, and reading for coding and storage. We used field editing by a field supervisor and in-house editing by a hired research assistant. It is important to state that data entry was done via a computer keyboard. The first frequencies printout from the survey was examined very carefully to detect wild values or other forms of mistakes. This was unlikely, but a possible occurrence might have been a respondents age being shown as 99; this may have been true, but may also have been a mistake.

All data were first captured into a Microsoft Excel 2007 spreadsheet before importing it into the SPSS. The check involved searching for missing system values assigned by the SPSS program or for input data and user-defined missing values that had been specified and SPSS considered to be missing. The data capture process was done three by three different data capturers and compared for any differences, which were then rectified.

The experimental studies considered how well a variable measured what it was supposed to, validity, how reproducible the measures were on a retest, and reliability. This process identified and assigned numerical representation or other character symbols to previously edited data. A variable was taken to be the classification scheme that could have several values, while values were the numbers or categorical classification representing individual instances of the variable that was being measured.

3.6 Ethical considerations

The principle of voluntary participation requires that people should not be coerced into participating in research. Similarly, the requirement of informed consent was considered. Essentially, this means that prospective research participants must be fully informed about the procedures and risks involved in the research and must give their consent to participate.

Consent forms were handed out to participants so that they could voluntarily decide whether to participate or not (refer to Appendix B for the consent form) [1]. Rural students participants who took part in the preliminary survey continued to participate in subsequent studies. The same migrant workers participated in both user studies. This provided continuity during the study. The identities of the participants were kept confidential, while the data collected were captured and stored in password-protected files.

Ethical standards also require the researcher not to put participants in a situation where they might be at risk of harm as a result of their participation. Harm can be defined as both physical and psychological [85]. Two standards were applied in order to help protect the privacy of research participants. Firstly, the researcher guaranteed that their participation was strictly confidential. For instance, personal details and responses to questions were not revealed to an outsider. Participants were assured that identifying information would not be made available to anyone not directly involved in the study. Secondly, the principle of anonymity essentially means that the participant should remain anonymous throughout the study – even to the researcher [30]. In our case, no real names were mentioned or recorded.

After the analysis of all data files, all files were discarded appropriately to avert any information leak. This step was taken to ensure that no physical or emotional harm came to participants, such as violation of their right to privacy by posing sensitive questions or revealing personal information. Participants were made to recognise that participation in the survey was a voluntary process that required the researcher to encourage participation without undue pressure on or coercion of the participants.

Justice requires a commitment to ensuring a fair distribution of the risks and benefits resulting from research [85]. Those who took on the burdens of research participation should share in the benefits of the knowledge gained. In addition, respect for communities "confers on the researcher an obligation to respect the values and interests of the community in research and, wherever possible, to protect the community from harm".

Even when clear ethical standards and principles exist, there will be times when the need to carry out accurate research threatens the rights of potential participants. No general set of standards can possibly anticipate every ethical circumstance. As a result, there needs to be a procedure that assured that the researcher considers all the relevant ethical issues in formulating his/her research plans. To this end, a research proposal was submitted to the Institutional Review Board of the researcher's institution and was approved [21].

3.7 Summary

This chapter explained the research design and methodology. Security, usability and transaction costs constitute challenges facing MFSs. The main research question is, "How can near field communication be used to provide mobile financial services?" This research question is broken down into several questions concerning security, usability and transaction costs, respectively. The research approach used qualitative, quantitative and software engineering and synthesis research methods. The experimental design addressed a background study, a security attack study, and user studies I and II. The background study considered three activities: a focus group, and demographic and preliminary payment studies. Focus group question--and-answer sessions, questionnaires, interviews, surveys and observations were used in the background study. Three prototypes were built: NFCbankme, NFCpayme and NFCme2u. The last two were used to explore usability. NFCbankme and NFCme2u were used to examine security, and NFCpayme alone was used to study transaction cost. Finally, the ethical considerations affecting the study were laid out.

Chapter 4

Prototype design and implementation

This chapter addresses the design and implementation of prototypes built to investigate the research questions, as explained in the previous chapter. Three prototypes were developed: NFCbankme, NFCpayme and NFCme2u. NFCbankme is an attempt to provide mbanking services such as checking balances and transferring money. NFCpayme deals with mpayment, while NFCme2u involves M2M money transfers. Each prototype is covered in a separate section and each section covers overview, requirements, architecture, protocol and implementation. Section 4.1 explains NFCbankme, Section 4.2 describes NFCpayme and Section 4.3 discusses NFCme2u. A summary section concludes this chapter.

4.1 Mobile banking prototype

NFCbankme used two different technologies: SMS and NFC. SMS helped provide basic MFS functionality. Then more requirements surfaced that led to employing NFC to bolster security and usability. The initial effort of building NFCbankme became a challenge. We could not test it with actual users, since we could not get a bank to provide the financial backend. In addition, our attempt at simulating a secured banking environment inside the laboratory environment failed. It was too laborious and we could not complete the software to allow for user testing. We later modified aspects of the NFCbankme prototype into two simpler prototypes: NFCpayme and NFCme2u. Even though we could not test NFCbankme on actual users, we reused much of the code for the other prototypes. Therefore, this section details the design and implementation of NFCbankme. Section 4.1.1

presents an overview of NFCbankme, Section 4.1.2 gives the requirements for the system, Section 4.1.3 describes its architecture, Section 4.1.4 explains the protocols considered for it, while Section 4.1.5 gives some implementation details for NFCbankme, including screenshots.

4.1.1 Overview

Assume a situation where an SMS is sent via the GSM network to a remote bank server, which in turn communicates with a backend database that is located in the SMS centre. A reply via the same route is received on the user's mobile device. An additional instance may emerge in which the SMS is later used for payment, whether remote or proximity. This can take place at a teller's computer terminal at the bank or a terminal that offers customer service. This creates an opportunity for using mobile phones for banking contactlessly. We assumed an overall picture that integrated the mobile and contactless domain and then provided a use case scenario. We envisaged the use of an NFC-enabled device with SMS and NFC capabilities (refer to Figure 4.1).

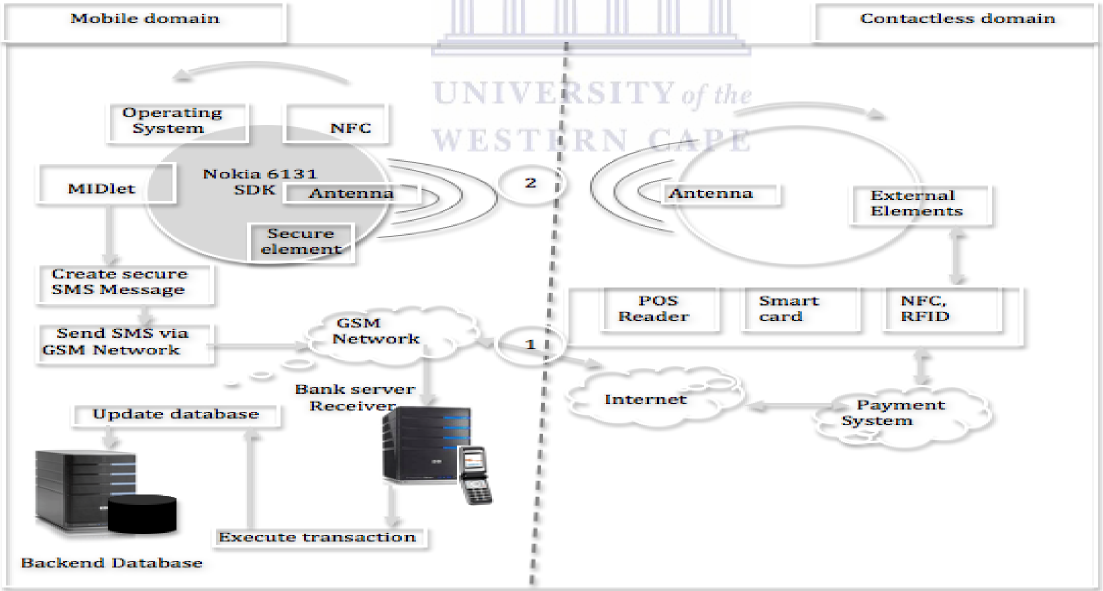


FIGURE 4.1 **Interfacing a GSM operating environment with NFC**
This diagram illustrates the operating environment for an NFC-enabled device. This consist of two parts: mobile and contactless. The mobile part comprises the GSM network and cellular phone side, while the NFC contactless part consists of the contactless reader and network infrastructure capabilities.

A MIDlet on the phone can handle SMS from the GSM network. The mobile phone has an antenna that generates and senses RF-fields for contactless communication.

The antenna of a contactless reader also generates an RF eld for reading data from an NFC-enabled phone. The POS reader application requests data from the mobile phone and processes it. The internet represents and provides the service offerings. The GSM network can be operated by any MNO and connectivity is via SMS to the mobile phone and also via the internet to content providers. The mobile phone has both GSM and NFC capabilities. In testing NFCbankme, this prototype utilises the use of the Kannel SMS gateway, an open source WAP, and an SMS gateway to send SMS in binary code via the internet to the destination mobile phone and port.

4.1.2 Requirements

The following is a summary of the requirements for NFCbankme and it can be divided into three categories: functionality, usability and security. The functionality and security categories constitute the functional requirements of the system, while the non-functional requirements are those in the usability categories. In terms of functionality, NFCbankme must be able to send and receive SMS, support contactless communication, place orders, make purchases and perform service discovery. In considering the usability aspect, the requirements are to have a user-friendly GUI, fast SMS, as few clicks as possible to perform a task, ease of use, convenience, small effort to accomplish the task and availability of use.

With regard to security, the system should detect reused VM; avert compromising data by using an SE, thus ensuring that message integrity is upheld; and maintain the validity of the transmitted message. The confidentiality of the information and VM must be ensured, as well as restrictions on the accessibility and dissemination of information. It is important to determine whether someone or something is, in fact, who or what he/she/it is declared to be. Thus, the process must be authenticated. Another requirement is to ensure non-repudiation, i.e. that the sender of the message cannot later deny having sent it and that the recipient cannot deny having received it.

4.1.3 Architecture

The high-level conceptual view shown in Figure 4.1 has two parts: mobile and contactless. The mobile part comprises the GSM network and cellular phone and the contactless part consists of the NFC contactless reader and network infrastructure capabilities. A MIDlet is initiated almost instantly when the phone receives an incoming SMS. The Java environment can handle the SMS from a GSM network. Once initiated, it extracts and processes the data content of the SMS. The connection between the mobile and the contactless domain, i.e. the Internet, is the gateway that allows the content provider to deliver the service and bill MNO subscribers using the service (see the circled figure 1 in Figure 4.1). The contactless link between the two antennas on either side of the broken line represents communication via NFC (see the circled figure 2 in Figure 4.1).

In applying NFC to support SMS mbanking, we assumed a scenario that involves a customer, the NFC-enabled mobile phone with an SE and some VM. Firstly, a customer places an order for VM to be topped up on his/her mobile phone. Secondly, an SMS with the VM is sent to the customer's mobile phone. Thirdly, the customer receives the SMS and saves it onto the SE of the mobile phone. The VM can then be used by presenting the mobile phone with the SE containing the VM to the contactless reader/POS for buying goods. From this scenario, the second and third steps are discussed in this thesis. Step two covers the delivery of the SMS via the GSM network and the use of symmetric authentication. The third step concerns getting data from the SMS to the SE and employs the asymmetric authentication approach (see Figure 4.1).

4.1.4 Protocol

This section describes two cryptographic key approaches: symmetric and asymmetric authentication. The former is implemented between the mobile phone and the GSM system via NFC and SMS. The latter is implemented for communication between the mobile device and the contactless domain using NFC and the internet.

A symmetric cryptographic key approach is used to enforce the security of the message sent between NFCbankme on the mobile phone and the GSM system. For messages to be transmitted in a secure manner over the GSM network, an SMS structure is required such that each eld represents the GSM message structure parameters (refer to Figure 4.2). In managing the key, two tasks that make use of the key generation technique are employed: 'check balance' and 'money transfer' tasks, both of which involve the use of a random generator. The response message from the bank's server is encrypted with derived keys from the customer's data using algorithms.

In terms of the check balance task and a transaction where a single message is sent to the server (refer to Figure 4.2), the customer encrypts the request message m_1

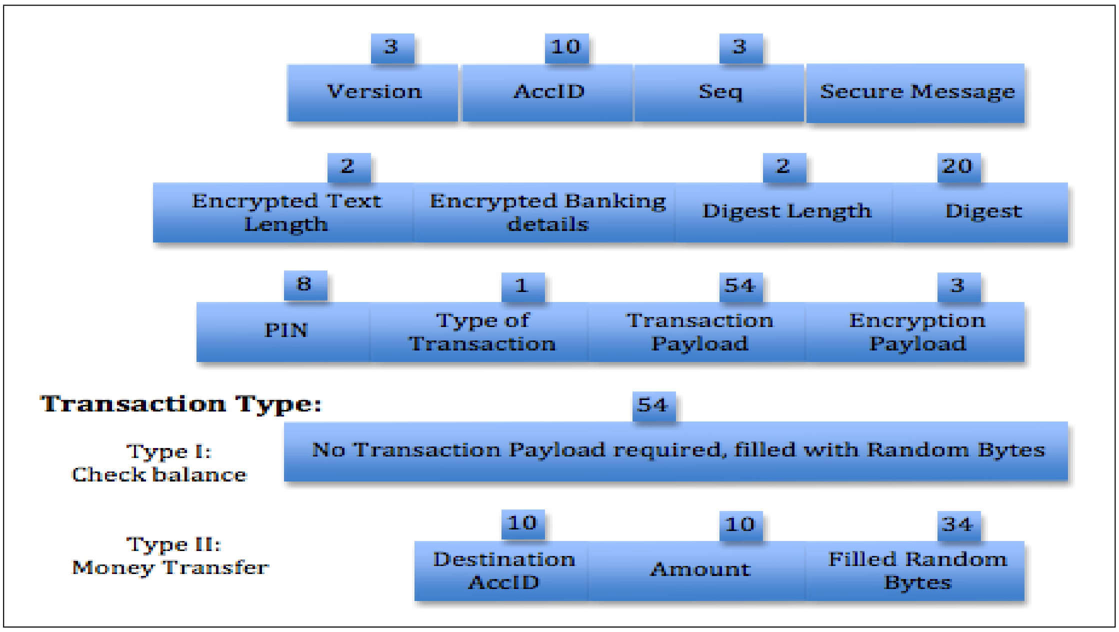


Figure 4.2 **Structure overview for a secure SMS message**
The minimum number of bytes required for each field in the message is placed directly above the field.
Source: [19]

with the OTP and a message digest on m_1 produced using a hash function H. C to denotes the bank NFC mobile client of the security protocol, while S to refers to the bank server side of the security protocol. E_{ks} implies the encryption with the OTP using the password generator. This leads to equations 4.1, 4.2 and 4.3.

$$M1 : C - S : E_{ks}[m_1], H[m_1] \tag{4.1}$$

$$M2 : S - C : E_{ActP}[< balance >] \ or \ [< Errormessage >] \ in \ plaintext. \tag{4.2}$$

$$Where \ m_1 = [ActID||TransactionType||SQ||PIN] \tag{4.3}$$

We consider a salt number to be a random number that is needed to access the encrypted data, along with the password [19]. If an attacker does not know the password, and is trying to guess it with a brute-force attack, then every password he tries has to be tried with each salt value. Salts are stored separately from passwords. Thus, the salt number denotes the salt value produced by the NFC mobile client or C and is used by the bank server and mobile client to produce the session key KS. KS is the symmetric session key shared by S and C. SQ is the sequence number of the password and Transaction Type represents a number that indicates the type of transaction selected. ActID represents the account identifier of C, and PIN represents the predefined personal identification of C.

The bank reply is E_{ActP}, meaning encryption using a concatenation of the user account identification, the salt number and a PIN. Once the reply arrives at C, the NFC mobile client is prompted to enter both the PIN and the account number before the message content can be accessed. This also means the derived keys are not stored, and so no storage space is used. Similar to the check balance account task the request to transfer money, the bank NFC-mobile client encrypts the request with the randomly generated password and the reply is the same as the check balance protocol reply from the bank. *M2* activates C by requesting the customer to enter the account identification and the PIN when accessing the messages.

In the money transfer task, a message is encrypted as SQ and sent to S by C and the payload represents the extra data for the transaction such as the transaction amount (refer to equations 4.4, 4.5, and 4.6). While E_{ks} refers to encryption using the OTP from the password generator, E_{ActP} implies an encryption using a concatenation of the customer salt number and PIN. H is the hashing function that creates message digest on m_2. The confirmation can take the form of a plain text message requesting that the user clicks to cancel a transaction that is about to launch within a few seconds. A reply message *M2* from the bank server starts such an application.

$$M1 : C - S : E_{ks}[m_2], H[m_2] \quad (4.4)$$

$$M2 : S - C : E_{ActP}[< confirmation >] \ or \ [< Errormessage >] \ inplaintext. \quad (4.5)$$

$$Where \ m_2 = [ActID||DestinationActID||payload||TransactionType||SQ||PIN] \quad (4.6)$$

The bank maintains a random password generator application that creates the sets of random passwords called OTPs and sequence number pairs. It is assumed that these sets of pairs are exchanged with the knowledge kept only between the user and the bank. Initially, the customer might have to physically come to the bank to obtain these sets of pairs in advance and/or subsequently have a secure communication that allows the customer to gain access to them. The sequence number is to prevents impersonation and replay attacks (refer to Figure 4.2) . The NFCbankme protocol uses a two-factor authentication strategy, and as such it uses two criteria that authenticate a user, i.e. something the user knows (such as the password) and something the user has (such as the NFC-enabled mobile phone).

An asymmetric cryptographic key approach is used to secure communication between the mobile device and the contactless domain using NFC and the internet

(Figure 4.1). Let the client's mobile device be the Initiator, while the teller/-cashier/agent outlet (AO) contactless reader acting as the issuer becomes the Target device [78]. A private and public key pair is generated by the Initiator. For initialisation, the Target is assigned a secret key K_I and the virtual SMS MIDlet is installed on the client's mobile device or, as is the case with most mobile phones, SMS comes pre-installed.

The client's mobile device stores the private key, and the public key is associated with the ID of the client's mobile device. This is done by having the public key transferred to the bank server, which doubles as the PKI server. While a registered AO has access to the PKI server, only authorised entities may modify all ID-public key association and the backend database. The AO must trust the PKI server and have access to it to be able to handle access to the client's public key.

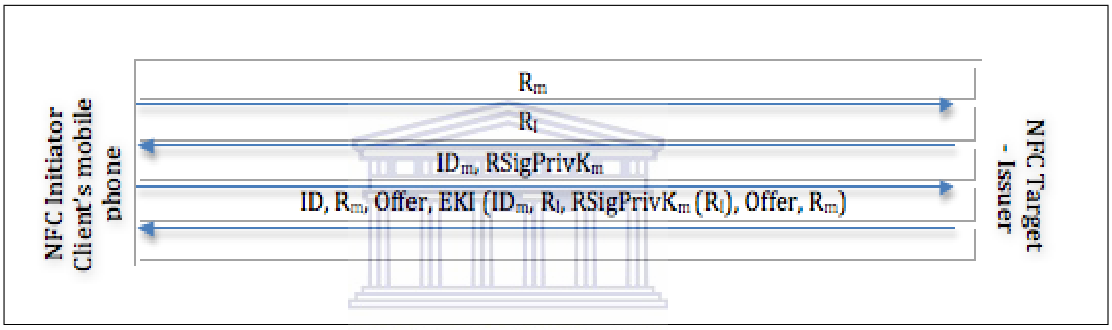


FIGURE 4.3 **Issuing the virtual SMS message**
The challenge for the client authentication is R_I, the issuer ID as ID, the information data is *Offer*, the secret key (issuer) is K_I, the AES result is EK_I, the challenge (mobile device) is R_M, the mobile device is ID_M, the private key (mobile device) is $PrivK_M$, and the signature using the private key is $SigPrivK_M$.

To use the protocol, the client interacts with the issuer by 'touching' it (see Figure 4.3). This action sends a request to obtain a valid virtual SMS, which is similar to an SMS top up message, which contains the challenge R_M for the issuer. A mutual authentication ensues in which the issuer also sends a challenge R_I to the client's mobile device. The client's mobile device signs this challenge using its private key $P_{RIV}K_M$. It sends the ID (ID_M) and the signature to the issuer. Although, the issuer at this time is unable to verify the signature, it attaches additional information data or *Offer* and the authentication to the challenge, and encrypts the input using AES. The valid virtual SMS message comprises the issuer's ID, the client challenge and the encryption result.

The client brings the VM message to the AO. The AO requires that the client's mobile device authenticate itself and, as a result, the AO sends a challenge R_C to the client (see Figure 4.4). The client's mobile device signs the challenge with its private key $P_{RIV}KM$ and sends back the result $SigP_{RIV}K_M(R_C)$ along with the ID_M to the AO. At this point, the AO will need the public key from the client's mobile device to verify the client's signature. For this reason, the AO contacts the bank server and sends the client's ID to the server, and the server responds with the appropriate public key $PubKey_M$. The AO uses the issuer's ID to obtain the

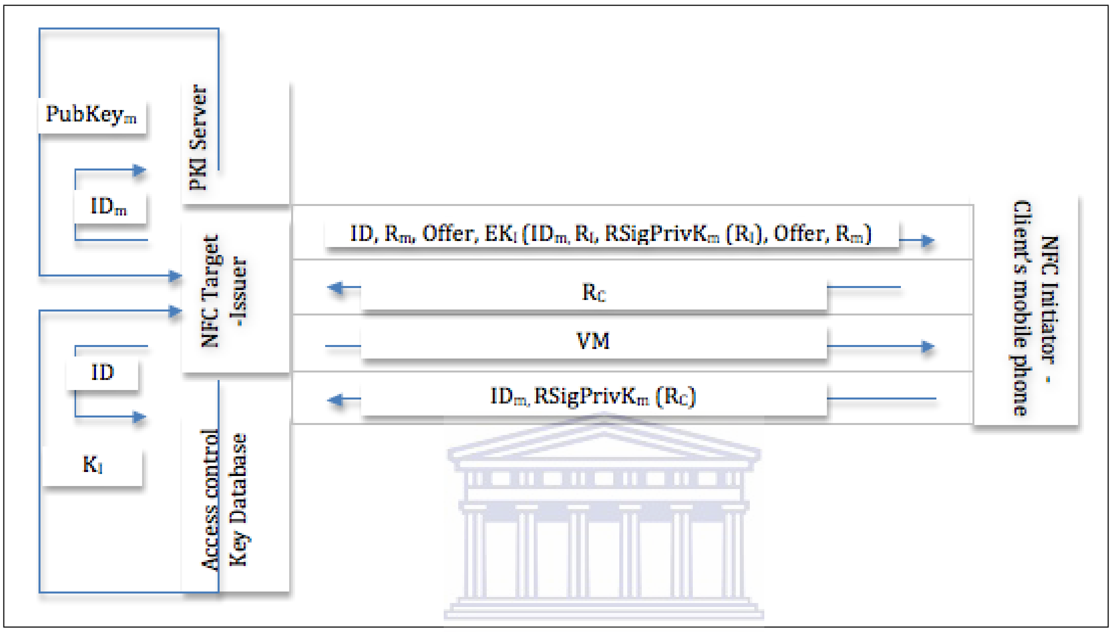

PubKeym
PKI Server
IDm
NFC Target -Issuer
ID
Kl
Access control Key Database
ID, Rm, Offer, EKl (IDm, Rl, RSigPrivKm (Rl), Offer, Rm)
RC
VM
IDm, RSigPrivKm (RC)
NFC Initiator - Client's mobile phone

FIGURE 4.4 **Retrieving the virtual SMS reply message**
All acronyms remains the same as in Figure 4.3; R_C becomes the challenge.

secret key k_I, decrypts the encrypted portion of the virtual SMS reply message and gets access to the client-authentication data exchanged when issuing the virtual SMS. The AO compares the IDs (ID_M) and uses the public key from the present client to verify the authentication data. For the AO to be certain that the virtual SMS message was issued for the current client, the IDs must be equal, while the signature $SignP_{RIV}K_M(R_I)$ must be verifiable with the current public key and the issuer's challenge in the virtual SMS message (R_I). The AO verifies that the challenges (R_M) inside the encrypted portion are the same as those outside it. If all security checks are successful, the AO sends the virtual SMS reply message to the client's mobile device.

4.1.5 Implementation

The connected limited device configuration (CLDC) is used, since it defines the characteristics of the mobile device we are using. The OS has Java Virtual Machine

(JVM) built into it and the CLDC defines the specification for this JVM and a set of Java-class libraries. The minimum software and hardware requirement are that the host OS can launch, select and remove applications from a device that has 32 kilobytes (kbytes) of volatile memory for runtime memory allocation and 128 kbytes of memory for JVM and CLDC libraries. The integrated development environment (IDE) is Eclipse Ganymede.

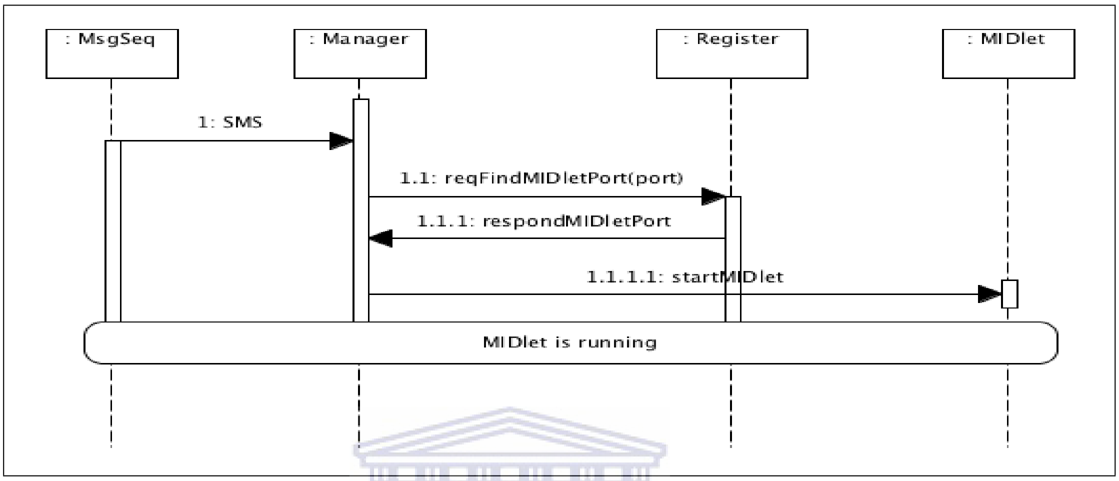


FIGURE 4.5 **MIDlet is started when an incoming SMS is received in the sequence diagram.**
The message sequence diagram (MsgSeq) in the mobile phone receives the SMS and the MIDlet is automatically initiated.

The OS of the mobile device receives the SMS and can initiate the MIDlet to start (see Figure4.5). The application manager receives the SMS in binary code sent to the mobile phone and finds the registered port destination address given by the SMS. If the port search is successful, it signifies that the MIDlet is ready to start. In this security setting, we require the account username and PIN to start the MIDlet. The JavaCard contains the JavaCard applet that reads/writes to the SE (refer to Figure 4.6).

At this point, the MIDlet reads the VM on the SE, so that the crediting/debiting of VM can take place (see Figure 4.7). The MIDLet can then process the data and send a writeAPDU containing the VM to the JavaCard application. The JavaCard application saves the VM and responds with a responseAPDU. In the case of the MIDlet reading the VM from the SE, this can occur in one of two ways. The MIDlet may receive a new VM or the user may want to check the balance of his/her VM. When the JavaCard is selected, a readAPDU is sent from the MIDlet with the address that it should read. The JavaCard application replies with the successful message.

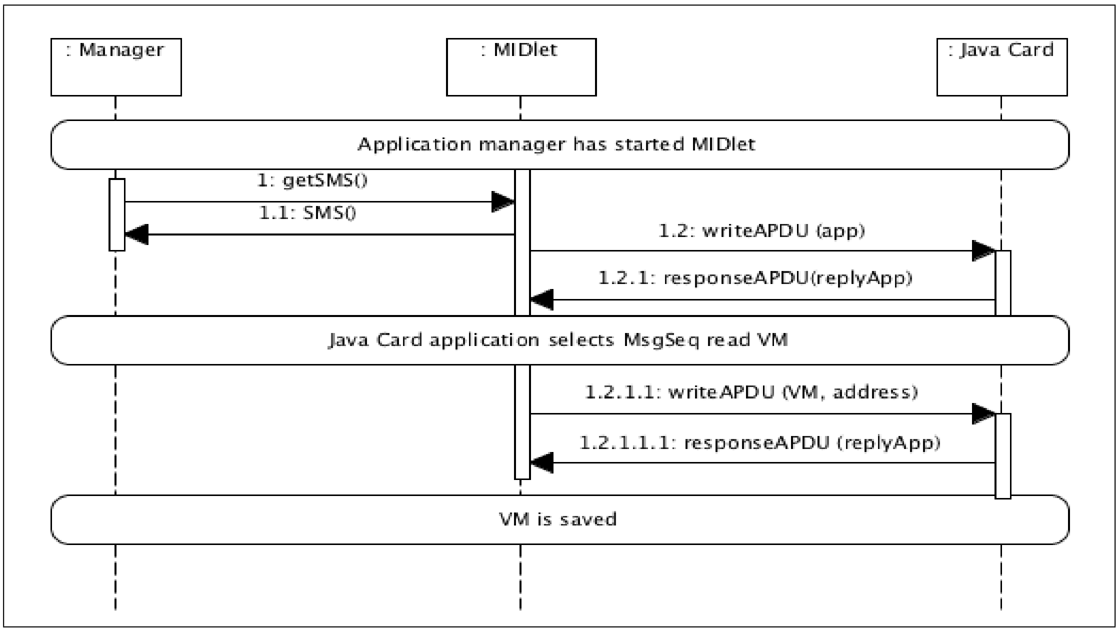

: Manager
: MIDlet
: Java Card
Application manager has started MIDlet
1: getSMS()
1.1: SMS()
1.2: writeAPDU (app)
1.2.1: responseAPDU(replyApp)
Java Card application selects MsgSeq read VM
1.2.1.1: writeAPDU (VM, address)
1.2.1.1.1: responseAPDU (replyApp)
VM is saved

FIGURE 4.6 **MIDlet saving VM SMS in the sequence diagram**
The application manager sends the SMS to the MIDlet, which extracts it and sends a selectAPDU to the JavaCard application. A responseAPDU is sent back from the JavaCard application to the MIDlet.

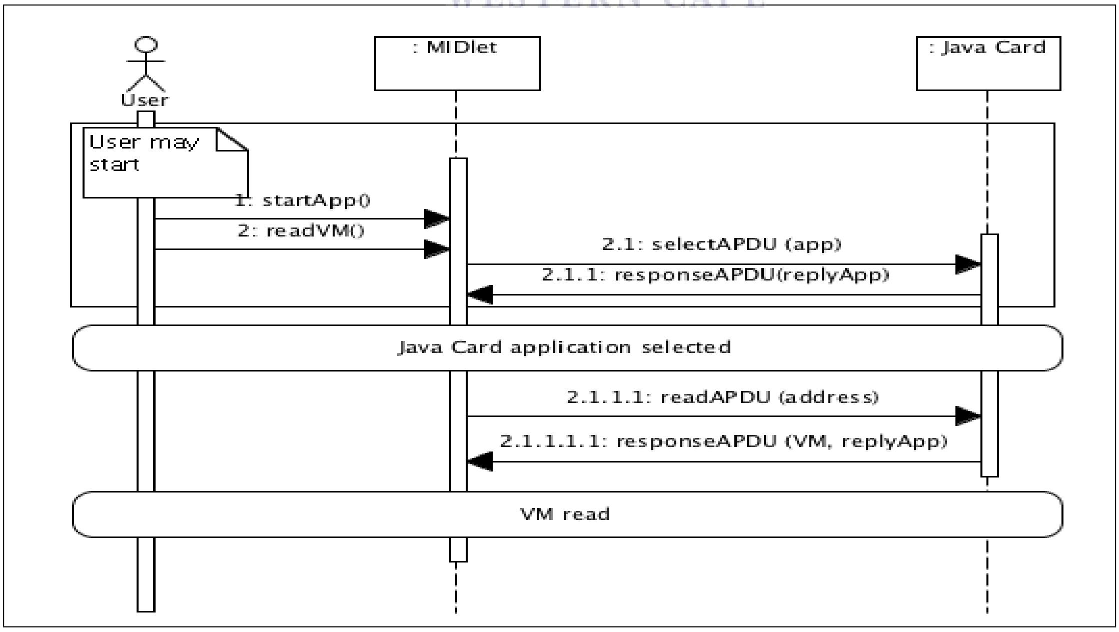
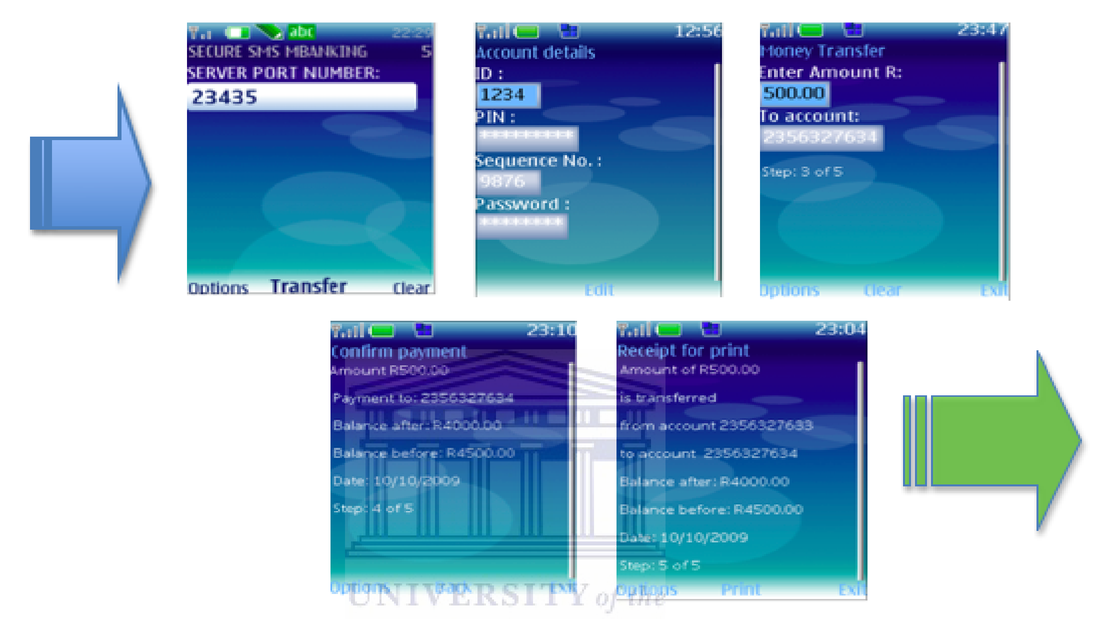

User
: MIDlet
: Java Card
User may start
1: startApp()
2: readVM()
2.1: selectAPDU (app)
2.1.1: responseAPDU(replyApp)
Java Card application selected
2.1.1.1: readAPDU (address)
2.1.1.1.1: responseAPDU (VM, replyApp)
VM read

FIGURE 4.7 **MIDlet reading VM SMS in the sequence diagram.**
The JavaCard application is selected by the selectAPDU(selApp) and the response –responseAPDU (replyApp) contains –returns the successful message.

The client puts the NFCbankme MIDlet on the mobile phone and launches the application to remotely perform an mbanking transaction. The mobile phone obtains the user input and generates the secure SMS message that includes the preset version bytes pattern and sends it to the server. If message integrity is upheld the server compares the owner's account PIN retrieved from the database and the one in the message. Once all the necessary security checks have been done, the server performs the requested transaction (see Figure 4.8 for the GUI).



SECURE SMS MBANKING

SERVER PORT NUMBER:
23435

Account details

ID :
1234

PIN :
****

Sequence No. :
9876

Password :
****

Money Transfer

Enter Amount R:
500.00

To account:
2356327634

Step: 3 of 5

Confirm payment

Amount R500.00

Payment to: 2356327634

Balance after: R4000.00

Balance before: R4500.00

Date: 10/10/2009

Step: 4 of 5

Receipt for print

Amount of R500.00

is transferred

from account 2356327633

to account 2356327634

Balance after: R4000.00

Balance before: R4500.00

Date: 10/10/2009

Step: 5 of 5

FIGURE 4.8 **Sequence of operation for NFCbankme**
The figure illustrates the sequence of operation in the NFCbankme mobile client application. The user enters the server port number, selects option one and the account information screen is shown and a secure SMS gateway is selected. The Money Transfer screen requires the transaction details to be entered. This brings up the Confirmation screen and the user selects the Pay option. The last screen displays the proof of payment and offers the option to exit or perform another transaction.

4.2 Mobile payments prototype

This section describes how NFCpayme allows a users to pay for items, check his/her balance and top up VM. The section shows how the proof of identity between parties is accomplished and provides an account of the underlying protocol to prevent possible attacks. Section 4.2.1 provides an overview of NFCpayme, Section 4.2.2 presents the requirements for NFCpayme, Section 4.2.3 provides the architecture of NFCpayme, Section 4.2.4 explains the protocol behind NFCpayme and Section 4.2.5 describes the implementation of NFCpayme, including screenshots.

4.2.1 Overview

The NFCpayme application is downloaded and installed on an NFC-enabled mobile device. The mobile device can then store and cash in VM via the application. The issuer equipped with an NFC interface is attached to a labelled RFID-tagged list of grocery products and can issue VM. The client with the mobile device touches the issuer and the VM equivalent of the price of the product is stored on the mobile device. It is possible for each client to have more than one mobile device, but this will amount to having more than one virtual identity. The client takes the VM topped up on the mobile device to the cashier (merchant or shop owner) payment terminal, which is also an NFC-enabled device, and cashes in the VM. The merchant verifies the validity of the VM and supplies the service or product (refer to Figure 4.9).

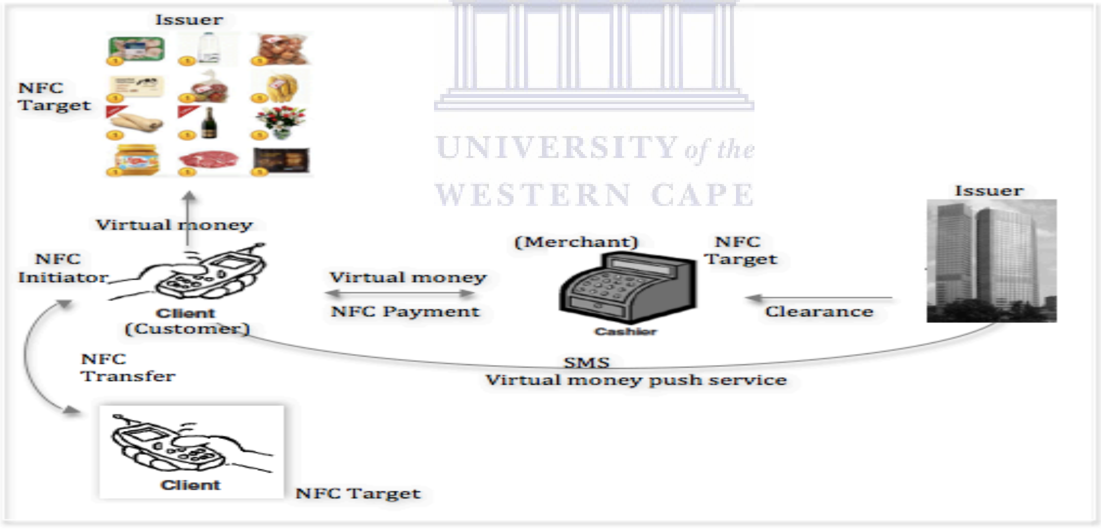


Figure 4.9**NFCpayme and NFCme2u systems**
This figures shows the structure of NFCpayme, which makes use of VM. The system comprises three parties: the issuer with an NFC interface that can be attached to an item on sale such as an RFID-tagged list of grocery products and/or a VM issuer; the customer with the NFC-enabled mobile phone; and the merchant, who also has an NFC-enabled device such as a payment terminal. This diagram also illustrates the NFCme2u concept between two NFC-enabled mobile phones. This interaction is explained in Section 4.3.4.

4.2.2 Requirements

Mobile payment systems are not immune to security attacks and must be protected [72]. A secured system of electronic VM should make an attack more expensive than the value an attacker could gain from a successful attack. Based on the discussion of mpayment solutions in Section 2.1.2, and the analysis of security issues raised in Section 3.1. NFCpayme assumes that it must be impossible for valid VM to be issued by an illegal party, for an illegal party to produce and cash in a valid copy of the VM, for VM already spent to be reused and for invalid VM to be made valid.

A client carrying a mobile handset uses the VM at a merchant payment terminal equipped with an NFC interface. The VM may be issued by an issuer. A client may have more than one mobile device; however, this will imply having more than one virtual identity. The client can approach the merchant POS and make payment with the virtual currency, and the merchant confirms the validity of the VM before supplying the service or goods. The system needs to handle certain security problems that may arise such as attackers reusing VM, attackers issuing virtual currency, VM remaining valid even after use, and attackers producing valid copies of VM and cashing them at the merchant POS.

The different entities involved in the various processes are the issuer, activator, client and merchant. Both the merchant and the issuer require an initialisation phase, and this requires enough computational power in terms of memory usage. The entity responsible for this is the activator. The activator is responsible for generating secret keys for the issuers, storing and distributing these secret keys in the databases of the appropriate merchants, and revoking and redistributing keys. In addition, it activates the merchant's access keys to the PKI server that manages the public keys of the client. The activator gives the merchant a certificate authority (CA), i.e. a trustworthy certificate, so that the merchant can do an offline verification. Used VM is stored in a database and the activator only provides access to the database for new merchant devices. The issuer is a passive NFC device, a CSC, an RFID tag or another NFC device, which means that the energy for the operation comes from the field of active NFC devices near the issuer [16]. 'Passive' means that the energy consumption of the tag is provided by the NFC initiator via the electromagnetic field, i.e. the tag itself has no battery or power source. The client mobile phone must be able to handle asymmetric authentication. Thus, it must have an NFC interface; private keys stored in the SE; and the required software for requesting, handling, and topping up and/or cashing in VM. Also, the merchant must be able to verify digital signatures and do AES computation, in this case by using the PC-based solution with online access.

4.2.3 Architecture

Figure 4.9 shows the client, merchant (affiliate) and issuer as actors. The VM is received from the issuer via SMS. This is then transferred from one client to another via NFC with proof of payment or an intermediate RFID tag. Payment is done by transferring the VM from the client device to the affiliate payment terminal. Clearance occurs over a secured network between the affiliate and the issuer. Once this is successful, a client may manage VM as he/she so chooses, e.g. checking the balance, history logs, etc.

The NFCpayme MIDlet is first code-signed to enable the OS to allow access to the NFCpayme JavaCard applet in the SE. This is signed with a CA to obtain the code-signing certificate that is used to digitally sign code and content [56]. The NFCpayme JavaCard applet is deployed to run on the secured hardware called the SE. The SE will only take new software from a trusted services manager (TSM) holding a private key, which allows authentication to the SE. This process will guarantee that the VM and other data in the SE is handled safely, and the NFCpayme JavaCard applet is securely deployed.

The MIDlet and applet are installed in the phone's OS and SE, respectively. The initialisation protocol as a result of the TSM establishing connection with the SE is executed by the issuer, triggering the public key of the issuer to be hard-coded into the SE, and subsequently generating an RSA keypair for the client mobile device in the SE. This client public key (RSA) registers with the issuer. The issuer generates the X.509 certificate for the client public key registered with it and sends it to the SE. This leads to the establishment of a network connection between the issuer and the client mobile device. This process is done only once [55] [58].

The next time VM is needed, the issuer generates signatures. The created VM is put into a byte array and encrypted for a destined SE. The result is sent via SMS to the cell phone number, which triggers the NFCpayme MIDlet to start and transfer the encrypted message to the SE, where it is decrypted. These processes are automated for the convenience of the client. Since each VM can be used separately, each is signed separately to prevent an illegal party from issuing valid VM. The process sets up the offline system. The structure of the VM comprises the ID of the VM, the amount, a status byte, and a 128 byte RSA signature by the issuer.

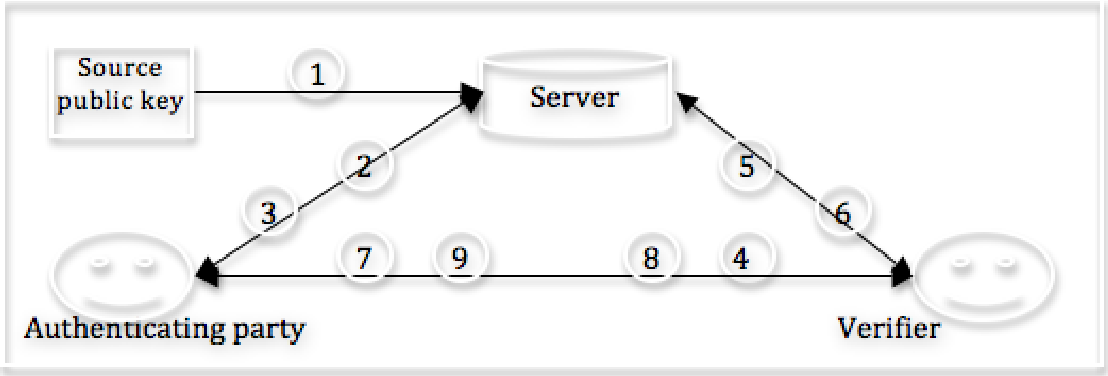


FIGURE 4.10 **The asymmetric approach for authentication using PKI**
The verifier can send a request to the server with the ID of the authenticating party to know how to contact the server and has to trust the integrity of the data stored. Furthermore, the transmission of the public key is secured such that the server can sign the transmitted data.
Source: [22]

To prove a party's identity to another, the knowledge of a secret key is shown. A challenge response authentication is used. First, a challenge is sent to the party willing to prove its identity, and this party returns a verifiable response before it is authenticated. Since asymmetric authentication is used, each party has a keypair consisting of a public and private key. The public key is used to verify each other's signatures, while a party is able to sign challenges using the private key. The steps are listed below and depicted in Figure 4.10.

1. The public keys of both parties are stored in the database.
2. The authenticating party then generates a public-private keypair.
3. The authenticating party transfers its public key and ID to the server.
4. The authenticating party sends its ID to the verifier.
5. The verifier sends the ID to the server.
6. The server responds with the corresponding public key.
7. Verifier sends challenge to the authenticating party.
8. The authenticating party signs the challenge using its private key.

9. Verifier then verifies the signature using the public key of the authenticating party.

Let us assume that client A wants to prove its identity to the merchant's POS party B. Party A begins authentication against party B by sending its ID, where ID is the identity that party A claims to possess. Subsequently, party B sends back a time-variant challenge R_B to A, and A demonstrates its knowledge of a private key K by authenticating itself. A does so by calculating a function F whose result depends on K and R_B. This result is then handed over to party B to verify the response and subsequently verify the identity of party A. An attacker logged into the communication between both parties may attempt to produce a second challenge without the knowledge of K. However, every challenge is time-variant and this makes the authentication protocol secure against the attack, e.g. replay attack. $A \longrightarrow B : ID \;\; ; \;\; B \longrightarrow A : R_B \;\; ; \;\; A \longrightarrow B : F_K(R_B)$.

4.2.4 Protocol

The NFCpayme involves various stages (refer to Figure 4.9): client-to-client, an affiliate payment terminal, and the issuer-to-beneficiary. Assume an issuer – a passive NFC target embedded in a food poster that could be used in a fast-food restaurant. The target's secret keys are stored in a database and the merchants have access to this database for the verification of VM. Additionally, privileges and/or access control is defined in order to restrict knowledge of the secret keys to only authorised merchants, and authenticating the merchants is required.

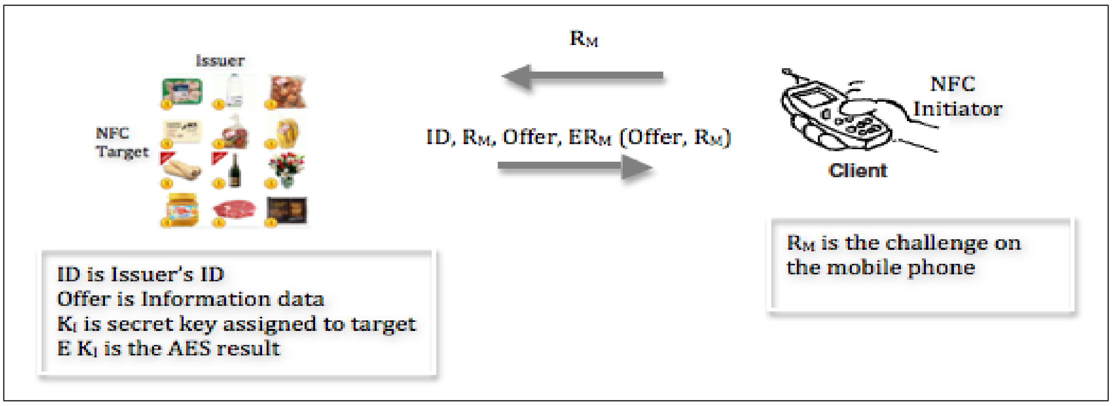

Issuer
NFC Target
RM
ID, RM, Offer, ERM (Offer, RM)
NFC Initiator
Client
ID is Issuer's ID
Offer is Information data
KI is secret key assigned to target
E KI is the AES result
RM is the challenge on the mobile phone

FIGURE 4.11 **Issuing VM**
This figure depicts a customer armed with an NFC-enabled mobile phone that acts as the Initiator performing service discovery on an RFID-tag list of groceries. This list is the NFC Target.

The customer conducts a service discovery on the issuer with his/her mobile handset which will generate a challenge R_M and pass this to the issuer. The information data is a combination of the following details: the type, issuing time, and validity range of the VM, so that the issuer attaches the offer to the challenge and encrypts the challenge along with additional data using the secret key K_I. It then sends a valid VM to the customer's mobile phone. At this point, the VM comprises the issuer's ID, the challenge, additional information data and an encryption result, say EK_1, known as the response (see Figure 4.11). To be able to cash in the VM, the customer has to 'touch' the merchant's reader device with a mobile phone. In turn, the mobile device sends the VM to the merchant over the NFC interface. Since the merchant's ID is already attached in the VM, the merchant, in this case the NFC target or reader device, searches through the key database for the secret key K_I of the issuer.

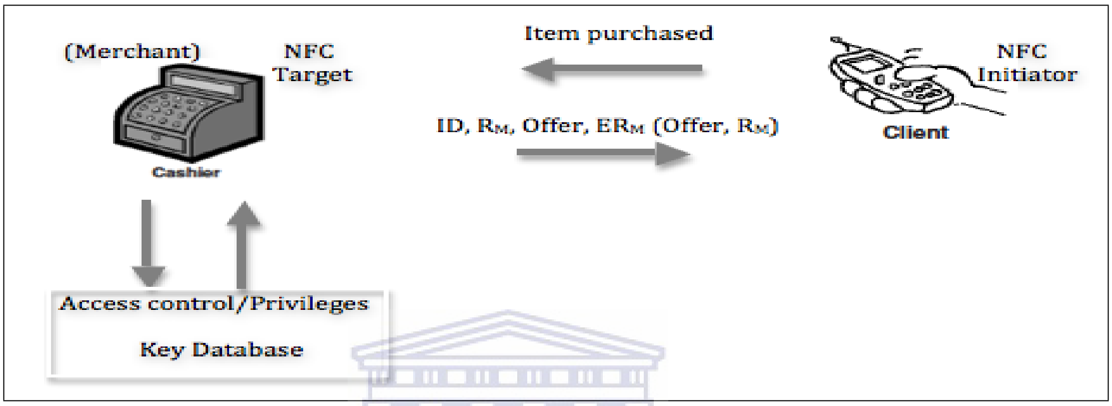
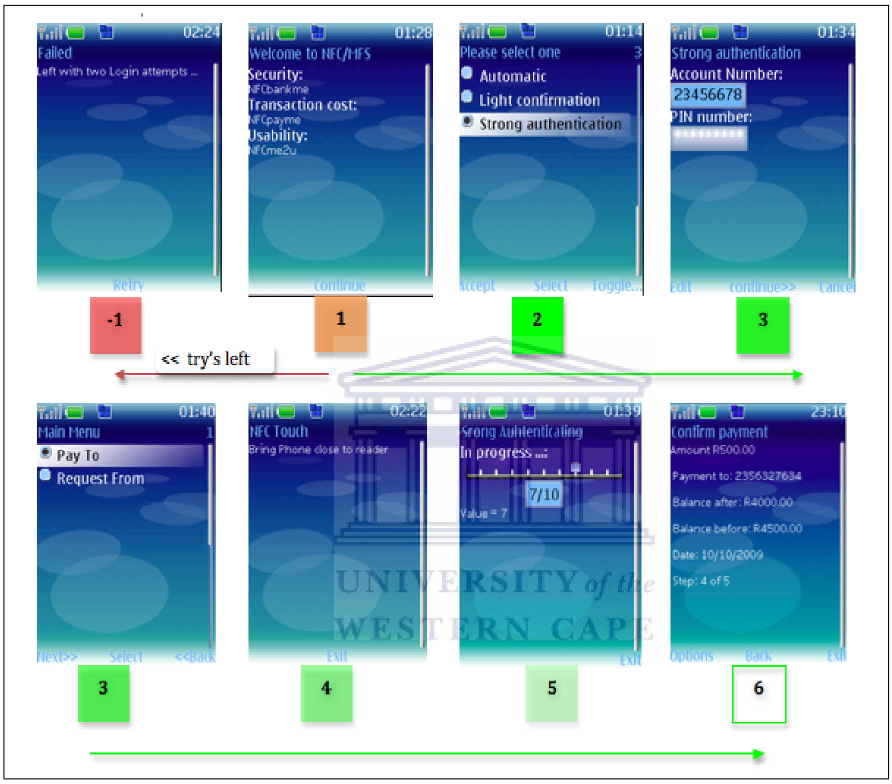


Figure 4.12 **Cashing in VM**
The cashing in VM for the protocol. This figure depicts a customer armed with an NFC-enabled mobile phone that acts as the Initiator making a purchase at the Merchant's contactless reader that acts as the NFC Target.

Once this key is found, the merchant can now use it along with the challenge R_M on the mobile phone and the offer to verify the encryption result from the issuer EK_I (refer to Figure 4.12). Since only the merchant has access to the keys in the database, the unauthorised manipulation and generation of VM is not possible. The merchant may decide to have multiple or more than one cashing in of the VM in which case the merchant will have to store the VM in the main database and compare identical ones.

4.2.5 Implementation

NFCpayme has a check balance task that allows a user to perform a banking activity, i.e. balance confirmation. The sequence of operations requires that the user clicks the continue command button to obtain a second screen. This second screen can be one of three screens, as shown in Figure 4.14. Assume that the full authentication mode is selected, and the user inputs the account and PIN number.



Failed
Left with two Login attempts ...

Welcome to NFC/MFS
Security:
NFCbankme
Transaction cost:
NFCpayme
Usability:
NFCme2u

Please select one 3
○ Automatic
○ Light confirmation
● Strong authentication

Strong authentication
Account Number:
23456678
PIN number:
****

Main Menu 1
● Pay To
○ Request From

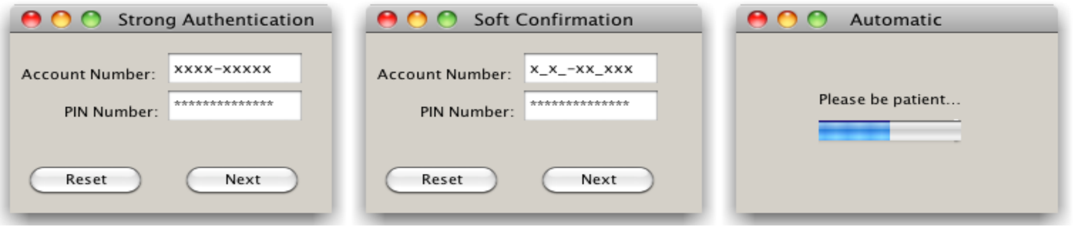
NFC Touch
Bring Phone close to reader

Srong Auhtenticating
In progress ...:
7/10
Value = 7

Confirm payment
Amount R500.00
Payment to: 2356327634
Balance after: R4000.00
Balance before: R4500.00
Date: 10/10/2009
Step: 4 of 5

FIGURE 4.13**NFCpayme steps in making a payment transaction**

The Main Menu screen is brought up as the fourth screen requesting that the phone be brought near the reader. This means the input is correct, otherwise a Failed screen appears decrementing the number of options left to re-enter details before exiting. Selecting a Pay To radio button and clicking Next prepares the phone for the NFC touch. The transaction details are displayed to solicit user confirmation. If granted by clicking Next, an authentication screen is shown. This is quick and once completed, the transaction is done (See Figures 4.13 and 4.14).



Account Number: xxxx-xxxxx
PIN Number: **************

Account Number: x_x_-xx_xxx
PIN Number: **************

Please be patient...

FIGURE 4.14**Three types of NFCpayme confirmation mode**

4.3 Mobile-to-mobile money transfer prototype

This section describes the NFCme2u, a mobile-to-mobile money transfer prototype. The prototype consists of a digital money system, an authentication system, and a GUI with secure communication protocol for performing p2p payments. Section 4.2.1 provides an overview of NFCme2u, Section 4.2.2 presents the requirements for NFCme2u, Section 4.2.3 provides the architecture of NFCme2u, Section 4.2.4 explains the protocol behind NFCme2u and Section 4.2.5 discusses the implementation the NFCme2u prototype.

4.3.1 Overview

Assume a situation where Bob takes a taxi home from the airport, but finds that he is low on cash. He will need to keep track of the receipt for the fare so that he can be reimbursed by his employer. To modify this scenario a little, assume that Bob's destination was away from home and he is not comfortable with the security of the environment he finds himself in and has no access to physical cash or some other payment method. The prototype system developed to deal with this scenario is shown in Figure 4.9.

This situation is very common to many travellers. If Bob has NFCme2u installed on his mobile device, all he needs to do is open up the NFCme2u MIDlet application and transfer the electronic equivalent of the physical cash he owes the driver, who should also have an NFC-enabled mobile device. NFCme2u can also provide for other types of payment scenarios. An analysis of the advantages and disadvantages of cash payments provides the basis for the analysis of NFCme2u. The aim is to achieve an NFCme2u system that is more favourable than physical cash payment without any major drawbacks.

4.3.2 Requirements

The requirements are categorised in terms of security and usability. NFCme2u is designed to investigate the trade-offs between security and usability. Users should not require correction and/or double checking for accuracy when transferring VM. The performance of the payment system should be independent of various situations that a user might encounter. The payment amount should not affect the time taken to make the payment. A system should be easy to learn and use, and transactions should not take an unacceptable amount of time.

The security concerns involves cryptographically storing VM on the phone to prevent theft. Counterfeiting the monetary representation should be next to impossible, thereby restricting certain unguarded actions such as backing up and reusing spent money. The system must protect VM from any form of alteration, and if by chance it occurs, the altered VM should be easily detectable and should be rendered unusable. Privacy infringement resulting from being able to trace who engaged in the payment should be impossible to accomplish, except if an external monitoring tool is put in place. Transactions must be resistant to attacks such that any form of interruption should cancel or roll-back the entire transaction.

4.3.3 Architecture

When two NFC-enabled mobile phones are used to send and receive electronic money (money transfer), each device is equipped with keypairs with regard to signature and the corresponding certificates: the issuer, the VM applet in the SE and the payment application in the payment terminal. The VM applet installed in SE has an RSA keypair that is used to obtain a signed certificate from the issuer. This allows the applet in the SE to use both the private keypair and corresponding certificate to secure and authenticate communication with a payment terminal or another applet in an SE. In this prototype, PKI is used for both signing and encryption.

The payment application has a keypair and a certificate, which is obtained from the issuer. This is needed as a communication channel for VM clearance. This is important for an initialisation phase to take place. The issuer holds two RSA keypairs: one for encryption and the other for signature. To sign and generate certificates for SEs and payment terminals, the signature keypair is used. For applets to register their keypairs during the initialisation phase, a secured communication is required. This is accomplished using the encryption keypair. To update these keypairs, a new applet is deployed via the TSM.

4.3.4 Protocol

The protocol allows VM transfer from one phone to another. Three entities are required to accomplish the transfer: a MIDlet application, a smart card (JavaCard), and a smart card terminal. The MIDlet running on the sender's phone facilitates the terminal mode and turns the SE into an active device. The MIDlet acts as the payment gateway responsible for the data movement between the SE, and back and forth between the sender and the receiver. In the client-to-client protocol, the SE is the target (receiving device, passive device or smart card), while the initiator (sender device, active device or smart card terminal) is in terminal mode. The MIDlet starts the SE in the initiator (see Figure 4.9 in Section 4.2.1).

1. The sender selects a MIDlet to transfer VM and the specific amount on interacting with the applet in the SE.The MIDlet in turn selects the transfer applet protected by a PIN that is stored by the MIDlet.

2. If (1) is successful, the MIDlet tells the transfer applet to transfer the specific amount via NFC. Otherwise, a transfer PIN agreed upon by both clients is set in their respective SEs.

3. Instructing the applet in the SE of the money transfer task to start causes an interaction with the SE on the receiving device by selecting the transfer applet.

4. After the applet is selected, the SE on the receiving device (recSE) generates a random challenge C and sends it to the SE of the sending device (sendSE) along with the key's PKI certificate associated with the applet and its recipient. Both the ID and the public key of the recipient are included in the PKI certificate.

5. The sendSE takes the following actions once it receives the C and the certificate;

   (a) It checks the certificate's information and extracts the recipient's ID and the recSE's public key.

   (b) It generates a random symmetric triple data encryption standard (3DES) session key (let this be K1).

   (c) R1 is formed from RSA using the public key of recSE to encrypt K1.

   (d) A session ID is generated.

(e) RSA-signs (C, session ID, recipient ID, K1) with the private RSA key of the sendSE, together with the session ID and the certificate information of the sendSE, and the result is presented in R2.

(f) send R1 and R2 are sent to the recSE.

6. The recSE receives the R1 and R2 and does the following:

   (a) K1 is obtained from RSA using the private key of recSE to decrypt R1.

   (b) The session ID is stored.

   (c) The certificate of the sendSE is verified.

   (d) The signature of the sendSE over C, the session ID, the recipient ID and the key K1 are verified.

   (e) The message authentication code (MAC) key K2 is computed from SHA-1(K1).

   (f) A 3DES MAC is computed over the session ID and the C with key K2 to get message R3. The transfer PIN is optionally transferred to the MAC.

   (g) R3 is sent to the sendSE.

7. Once sendSE receives R3 and checks the MAC, it marks the specific VM as used. 3DES then encrypts it under key K1 to form M1 and then sends it back to recSE.

8. The recSE then decrypts M1 and stores and verifies the included VM. It now uses the 3DES MAC to compute M2 over the received VM under K2, and sends it to the sendSE.

9. The sendSE receives M2 and checks the MAC. If successful, it deletes this specific amount of VM.

10. The recSE informs the user of the VM.

The recSE shows that it has the private key K1 connected to its certificate by correctly recovering key KI, and this further shows that after response R3, both the sendSE and recSE are communicating with each other. Furthermore, the symmetric key K1 is definitely generated from within the SE, since it is signed with a certificate keypair. On the other hand, the sendSE is able to show that it possesses the private key by correctly signing C, session ID, phone ID and K1, establishing that C was received correctly, that the session ID is genuine, that

K1 is original and the message is actually meant for the recSE. Because of the signature, the recSE considers K1 as fresh.

4.3.5 Implementation

The series of steps for the user(s) is actually linked to those for the application (s) as described in Section 4.3.4. The user logs in with a username and password. An incorrect entry requires a re-entry and only three unsuccessful attempts are allowed, after which the user is completely logged out and requires a second backup PIN. On successful login, a user might choose to pay someone. In that case, a Money Transfer screen is shown and the user is required to enter the amount and destination account.

Once the Pay button is clicked, the details of payment are displayed and the user is required to make the first NFC touch for payment. The next screen after the NFC touch is completed shows details for the payment. Clicking to allow this activates the NFC touch to be requested. Once this is done, a receipt is displayed, together with proof of payment on the Completed Transaction screen.

Assume the following steps in the NFCme2u's GUI for interaction (refer to Figure 4.15);

1. The user enters the right account and PIN number, and clicks on Next If the Frame login is successful, then a Main Menu screen (proceed to third step) is shown otherwise the Failed screen comes up (go to second step).

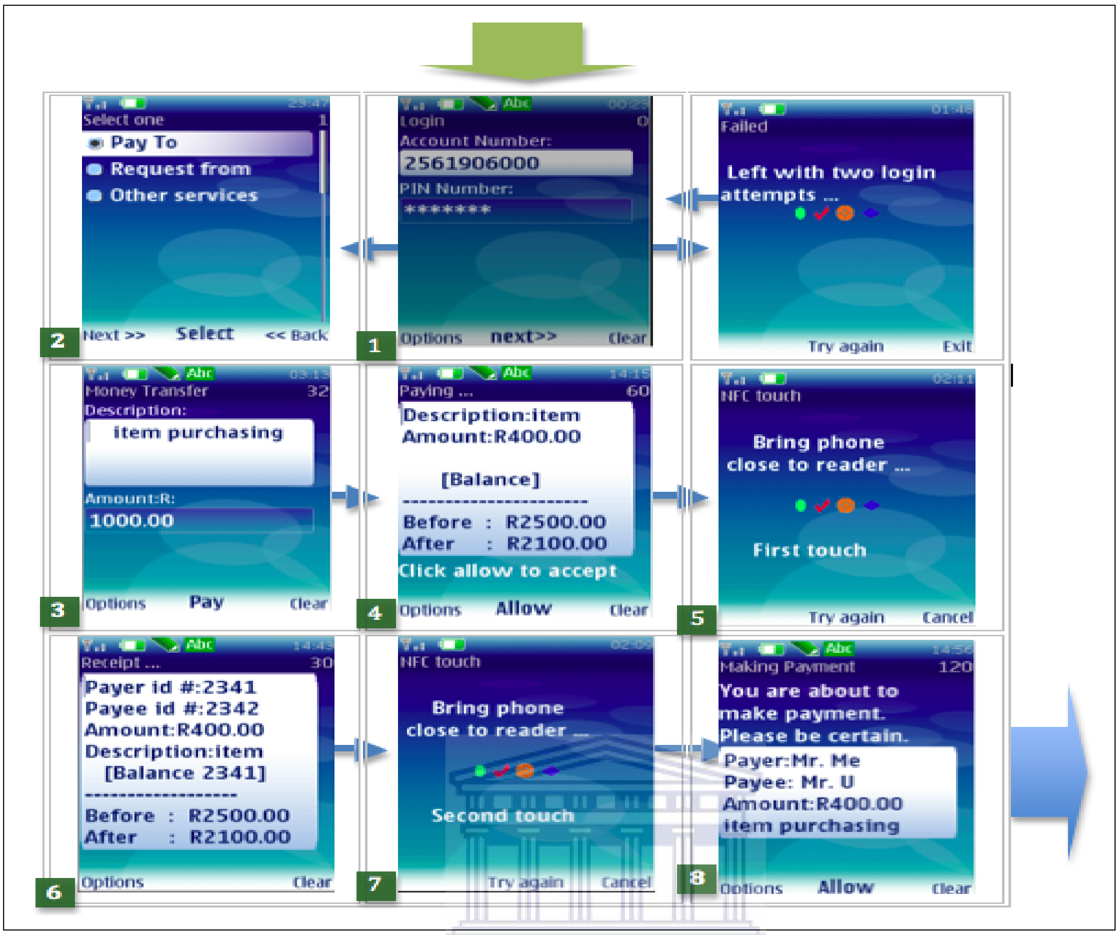
2. The Failed screen presents two more login attempts to the user after the first failed attempt, if Try Again is clicked.

3. In the Main Menu screen, a Pay To radio button might be selected, followed by click Select to bring up the Money Transfer screen.

4. The money transfer function requires the user to enter appropriate details in the Money Transfer screen and click Pay to bring up the Paying screen.

5. The Paying screen displays the transaction details of the payment and requires the user to accept by clicking the Allow or reject by clicking Options to go back. If the user accepts the payment details, then the NFC Touch screen is shown.

6. The NFC Touch screen displace the NFC interface for the first time touch for the payer to bring his/her mobile device (in active mode) near the payee's



Login 0
Account Number:
2561906000
PIN Number:
****

Select one 1
Pay To
Request from
Other services

Failed
Left with two login attempts ...

Money Transfer 32
Description:
item purchasing
Amount:R:
1000.00

Paying ... 60
Description:item
Amount:R400.00
[Balance]

Before : R2500.00
After : R2100.00
Click allow to accept

NFC touch
Bring phone close to reader ...
First touch

Receipt ... 30
Payer id #:2341
Payee id #:2342
Amount:R400.00
Description:item
[Balance 2341]

Before : R2500.00
After : R2100.00

NFC touch
Bring phone close to reader ...
Second touch

Making Payment 120
You are about to make payment.
Please be certain.
Payer:Mr. Me
Payee: Mr. U
Amount:R400.00
item purchasing

FIGURE 4.15 **Sequence of steps in NFCme2u payment mode**
At the top-centre is the Form Login, and if incorrect details are entered, the top-right corner of the Failed screen is shown. Otherwise the Main Menu at the top-left corner is shown.

NFC-enabled device (in active or passive mode). This will automatically continue to the next screen, Completed Transaction, unless Try Again were clicked.

7. The Completed Transaction screen displays the full details of the transaction to include the allowed identification details of the user. The user is again expected to do nothing, as the screen automatically proceeds to the next screen – NFC Touch – unless the Options were clicked within this short time frame to undo this part of the transaction. If nothing is done, the NFC Touch screen is displayed for the second time (i.e. two-touch protocol).

8. The second NFC Touch screen is automatically replaced by the Making Payment screen unless Try Again is clicked. If Try Again is not clicked, indicating the user's intention to proceed in the transaction, then the Making Payment screen is shown.

9. The last screen in the transaction is the Making Payment screen. This screen only requires that the user either rejects the final payment transaction details and returns back to the Main Menu screen, or a click on Allow implies an agreement and that the actual payment be made immediately. The proof of payment displayed can be printed out or sent via e-mail and printed.

4.4 Summary

Three prototypes were designed and implemented: NFCbankme for mbanking, NFCpayme for mpayment and NFCme2u for M2M money transfer. The discussion of NFCbankme looked at how an SMS with VM is sent to a mobile phone, and how to receive the SMS and save it to the SE. The former procedure used symmetric authentication while the latter used asymmetric authentication. The architecture consisted of mobile and contactless domains and it interfaced the GSM environment with an NFC phone/reader. SMS messages were routed within the GSM operating environment. Check balance and money transfer tasks were presented to show how requirements are met. NFCpayme was an extension of the check balance task in NFCbankme. NFCpayme employed asymmetric authentication. The requirement was to prevent security breaches. The architecture involved three parties: client, merchant and issuer. Keypairs were generated using RSA. P2p and client-merchant protocols were used. The prototype considered three modes of authentication. NFCbankme money transfer task was rebuilt into NFCme2u and used symmetric authentication. The architecture involved the use of a VM applet in the SE and the RSA keypair. The system had a MIDlet as the payment gateway, a JavaCard and a smart

Chapter 5

Results and analysis

This chapter analyses the results of the work on three NFC-based MFS prototypes: NFCbankme, NFCpayme and NFCme2u. The design and implementation of these three prototypes were discussed in the previous chapter. The focus of this chapter centres around the research question for this study, ***"How can Near Field Communication be used to support mobile financial services?"***. The research question has three questions addressing the following: security, usability and transaction cost. Section 5.1 presents the results and analysis for the background study, Sections 5.2, 5.3, 5.4 present the results and analysis of the studies on security, usability and transaction cost, respectively, Section 5.5 discusses the challenges faced and Section 5.6 concludes the chapter with a summary.

5.1 Background study

This section examines the background study that was carried out and presents an analysis of the results. The background study consisted of three activities: a small focus group, a demographic survey, and a preliminary survey. The results from this study influenced the subsequent user studies that were conducted.

5.1.1 Focus group

This was the very first activity that was carried out to ascertain what direction this study was to be headed. The average age of the seven respondents was 25, with four of them being each of 23 years of age. Four participants were undergraduate students, one was a postgraduate student and the others were non-academic staff members. Only the undergraduates were single, while the others were married with an average of two dependents in rural households.

Two of the undergraduates were employed part-time while the others, except for the non-academic staff, indicated 'None' for employment status. One undergraduate and the postgraduate come from the Eastern Cape, and spoke isiXhosa as their home language. One undergraduate and one non-academic staff member chose Afrikaans as their home language. The other two undergraduates selected isiZulu as their home language, while the other non-academic staff member chose seSotho as home language. Only the non-academic staff members lived off campus. One lived in the Gugulethu area and the other in Stellenbosch.

When asked about their original/permanent place of residence where their household members lived, one undergraduate came from the Eastern Cape, one non--academic staff member came from the Free State, one undergraduate came from the West Coast of the Western Cape, and one undergraduate came from KwaZulu-Natal, while the last participant (a non-academic staff member) was a male from the Northern Cape. One of the non-academic staff members was a female aged 25, and two undergraduates and the postgraduate were also females. The two non-academic staff members, the postgraduate and one undergraduate each had a house in the rural area where their household members resided. Others chose Informal settlement as their place of residence.

The average traveling distance to the nearest bank or ATM was three km, with the minimum being one km and the maximum six km. The undergraduates traveled home every six months during the university vacations for a month at least, while the rest only went home once a year, usually during the December holiday for Christmas and New Year. This study was conducted in February 2009. Only one person had no phone at that time, since she was mugged and her phone was stolen a week before the study. One undergraduate female had three different makes of phone and the others had one each.

On average, the undergraduate students received R850 per month from home as stipends, while the non-academic staff and the postgraduate sent money home. Two of the participants transferred money via people, one undergraduate used retail shops, and the rest each said they used a bank. Everyone used his/her mobile phone to communicate with household members back home. One person had recently installed internet service at home. No one used a fixed landline. Some said they had to travel a great distance to send/withdraw money. Electricity for three of the participants was not a problem, while they rest said that transaction cost was a concern.

When asked to share their thoughts about issues that currently affected them and their household members, each of the seven participants had something to say, and we present their words:

> *"There were a lot of charges when I withdraw money from another bank's ATM, e.g. ABSA, and not First National Bank (FNB), which I use. It charges R50 on my next withdrawal. The ATM sometimes has problem, e.g. it is out of service and does not get fixed in two days."*

> *"There is only one problem with this. When she i.e. his wife residing in a rural area goes to collect the money from the bank, she has to take a taxi cab and those taxi cabs are expensive. The last time I checked, it was something like R15 for a single trip to town. You can imagine how much she can spend just for transport."*

> *"We have only one bank on campus, FNB, which operates during office hours. The others are Standard Bank and ABSA, which are only accessible via ATM. Coming from a disadvantaged place, it would be more convenient if there could be a system that minimises traveling to a distant/remote bank. Also, the fact that we have only one bank branch means that the long waiting queues at ATMs also put us at risk of robbery. Therefore a system that would be secure and yet effective would be more helpful in rural communities. Despite being rapid and efficient, it must also be user-friendly and given the fact that people in rural communities are not well educated, it must be simple to use."*

> *"My mother is paraplegic, therefore having to travel long distances to deposit money for me is a big inconvenience. And sometimes she cannot make it at all and I am left with a dilemma."*

> *"The issue of having banks only in the towns/cities is one of major problems, and the absence of electricity in rural areas is also contributing to the absence of banks. Also, in terms of transport in the rural areas, there are gravel roads, which makes it difficult for public transport to come and pick up people. So people end up walking or riding bicycle to towns."*

> *"I think a software/technology will be more convenient because at banks' ATMs one has to wait in queues. You get mugged on your way there or at the ATM. Plus the huge bank charges."*

> *"Problems encountered include, inconvenience of sending and receiving money due to lack of outlets like shopping malls – Shoprite and commercial banks. One may need to travel a long distance to process a transaction. There are times when you don't get assistance (in making deposits/payments) as a result of time constraints and the slowness of the transport system. There are times where demand is higher than supply (especially at the end of the month). In these periods, it becomes almost impossible to send/receive money since you have to queue up for a long time to receive service."*

Responses from the participants indicated that they were particularly aware of bank charges, so cost was a factor, as they complained about charges associated with banking and cost associated with transportation. Inconvenience associated with the distance that needed to be traveled to make a payment/transfer was a major issue, given that four out of seven participants complained about it. Also, there was the issue of inconvenience as a result of the long queues because of the few banks that were available to these particular participants and their short office hours. Security was another major concern either as a result of the insecurity of transportation or the unnecessary delays in queues, leading to the risk of been robbed. Also poor service delivery was an issue as a result of not getting enough support. These issues affected all rural household members. They also affected people who needed to do banking, especially those without private transport and low-income earners. Overall, security, inconvenience and cost were the biggest issues.

5.1.2 Demographic study

The demographic study helped us to understand the groups we would be targeting and how to apply our study to their demographics. The relevant demographics were collected and participants were given the opportunity to interact with a PC emulator of an mpayment prototype to support the preliminary payment part of the survey questionnaire (see Section 5.1.3). Sixty-five per cent of respondents were below the age of 30 and 45% were female participants (See Figure 5.1), while 50% were rural students and the rest were migrant workers. In addition, 47.5% were married, 42.5% were single, and 10% were currently divorced and had not remarried. Also, 35% had no children, while 25% had four or more dependents. These demographics also suggested that there was a reasonable spread of South African provinces among the participants in each group. In terms of the highest

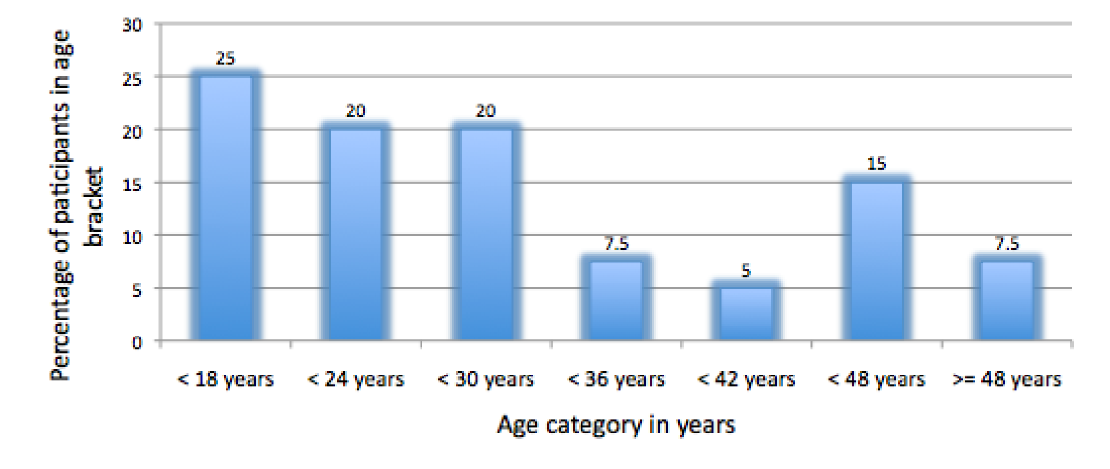


FIGURE 5.1 **Age of participants in the study**
This graph depict the age demographics for participants in the User Study.

Province of original place of residence	Workers	Students
Gauteng	1	0
Eastern Cape	3	5
Northern Cape	3	1
North-West	2	3
Limpopo	0	1
Mpumalanga	1	1
Western Cape	3	1
Kwa-Zulu-Natal	5	4
Free State	2	3

TABLE 5.1: Participants' province of original place of residence

level of education attained, 25% of participants had reached undergraduate level at university, 22.5% had completed high school and 17.5% had no formal education (Refer to Figure 5.2). The majority of respondents were evenly spread across the country (See Table 5.1). When it came to the issue of where they currently resided, it was not as widely spread, because students from the same university were participants and so they had to live close to the campus. The 20 migrant workers resided in various places in the Cape Town area.

5.1.3 Preliminary survey

This survey tested an emulated prototype by giving participants the opportunity to interact with a prototype and provide their responses. The feedback from users directed this research. When asked what they saw as the main benefit, 20% felt it provided greater security,15% said it would reduce cost, while 45% said that

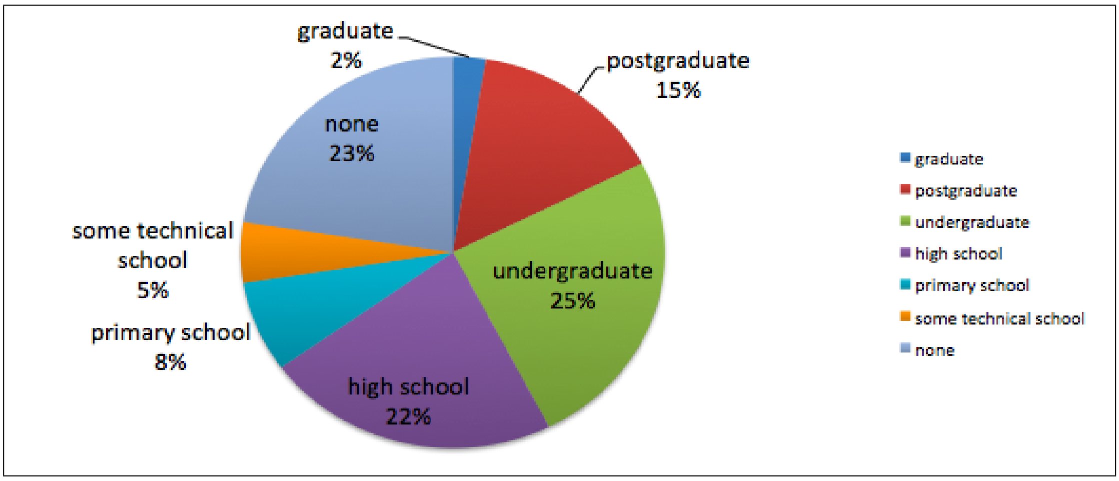


FIGURE 5.2 **Highest level of education attained by participants (%)** This pie chart illustrates how participants faired in terms of highest formal education attained.

convenience was key. Also, 80% indicated that they spent an average amount of between R250 and R3,000 per transaction, and 52.5% indicated that these transactions took place monthly. This pattern of spending can be explained by the fact that it coincides with end-of-the-month salary payments in South Africa (see Table 5.2). When asked how much they were willing to spend to obtain an NFC-enabled device, 70% agreed they would spend less the R250. When asked who they thought this type of service would benefit the most, 70% indicated migrant workers and students. Additionally, 27.5% currently were out of work, 17.5% had their own business, 25% worked part-time, and 15% either had a casual or a full-time job..

Interval between transactions		
Interval	**Frequency**	**%**
Weekly	3	7.5
Bi-month	6	15
Monthly	21	52.5
Quaterly	5	12.5
Every 4 months	3	7.5
Yearly	2	5

TABLE 5.2: Interval between transactions

Exactly 75% of the participants took an average of less than 12 seconds to complete each task (refer to Figure 5.3). These tasks included making a payment, depositing, making a withdrawal, and sending and receiving money. The respondents were also asked which area they felt most needed improving after working with the

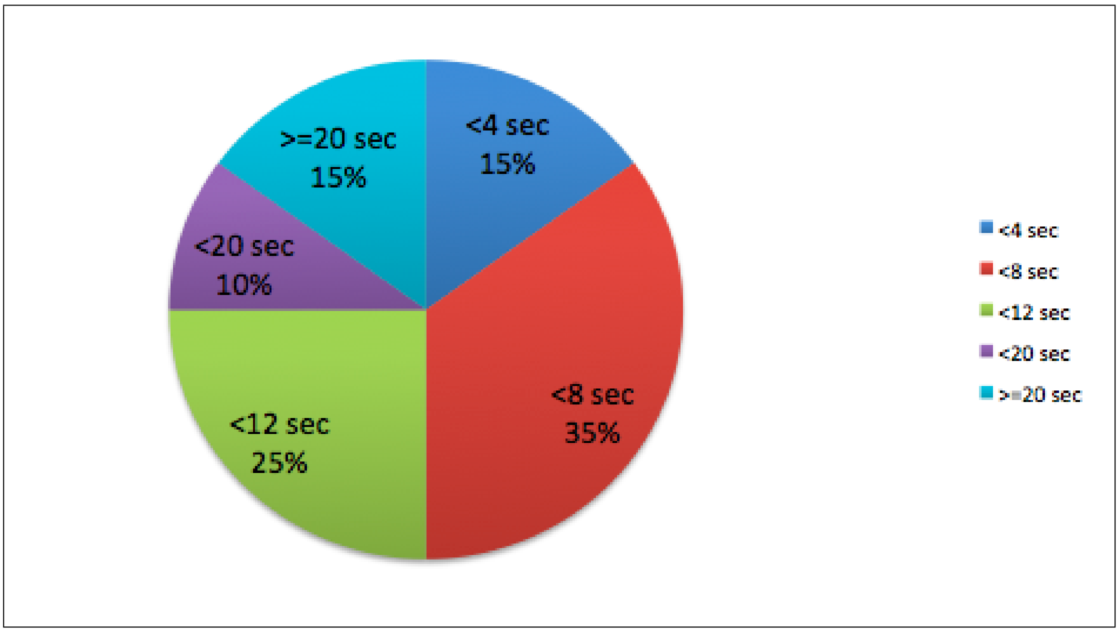


Figure 5.3 **Time take to complete task 'purchase a ticket' (%)**
This pie chart illustrates how average time in seconds taken to complete task

prototypes, and 60% indicated that security required more work, 10% said it was the speed, 15% referred to the interface and 15% indicated functionality.

In the preliminary payment survey using the PC emulator application, two-thirds of the participants indicated that they were willing to purchase an NFC-enabled device as long as it cost no more than R250. More than this percentage even felt stronger about paying for MFSs using NFC, as they indicated that they were willing to transact a maximum of R3,000. Also, more than half of the respondents perform monthly transactions of an MFS nature. The majority of participants felt that aside from rural students, migrant workers would most benefit from such a service. More than half the total sample felt strongly that security required more work, and to a lesser extent performance, GUI and functionality. The key was convenience, as about 45% admit it was a concern. The system also appeared to be very usable: more than two-thirds of the participants found it usable, as the learning curve was not steep. Thus, security and usability/convenience had surfaced as the main problems. Also, transaction cost was still an issue from the previous activity that required ways of limiting the total cost, while users had a limiting cap on spending on MFSs.

5.2 Analysis of security attack results

This section considers the question "How can NFC be used to provide secure mobile financial services?" The mbanking prototype, NFCbankme, laid the foundation for subsequent prototypes: NFCpayme and NFCme2u. In Section 3.4.2 we provided information on how the security studies were conducted using NFCbankme. Similarly, Sections 4.1 and 4.3 addressed security by describing the security features that were built into the NFCbankme and NFCme2u prototypes.

In this section, we start by describing the context in which security attacks were performed using NFCbankme. We present results of the following: securing SMS configured on a Kannel gateway system, performing various security tests and attacks using NFCbankme, and employing NFC to improve security in the existing SMS setup. We consider the security aspects of NFCme2u explored with users during the user studies, the goal of which was to acquire information that could be used to improve security in NFCme2u. We present the results in a radar plot from testing with users.

In general, security systems try to attain a certain level of security. Based on our system as laid out in Section 3.4.2 and the challenges as described in Section 3.1, we sought to achieve this by testing how our NFCbankme system dealt with security attacks. The NFCbankme server needed to authenticate the identity of the requesting NFCbankme client through the process of authentication. Given that at least two parties are involved in any one transaction (the bank and its client), they should be able to ensure that they are talking and/or listening to each other and not some malicious hacker through the process of mutual authentication. We also needed to ensure that even if a hacker were to retrieve messages travelling via the GSM network, they would be unreadable, thus providing message confidentiality. Furthermore, if a hacker were to change the message in transit, a receiving party should be able to detect these changes, thereby validating the integrity of an incoming message.

To be able to carry out these tests using NFCbankme, we explain the series of steps taken to perform the tests. We simulated a SMS centre (SMSC) using a simple protocol to test out a Kannel SMS gateway, which is an open source WAP gateway that also works as an SMS gateway for GSM networks. It was not a real SMS centre and could not be used to send or receive SMS messages from real phones. Thus, it was used for testing purposes alone. The following configuration applies to these tests.

```
group = smsc
```

```
smsc = fake
port = 10000
connect-allow-ip = 127.0.0.1
```

The first test was done on the OTP: we generated a duplicate password that already existed in the MySQL database. When we attempted to authenticate the NFCbankme system with it, the system threw the nonUniquepassword exception to indicate that the password existed in the database. All the MySQL relational database queries that were performed on the database were successful, and correct values were verified and returned. For the MySQL connection group variables, where max-connections were used for the database pool, we used the following configuration to test:

```
A sample ‘mysql-connection group:
group = mysql-connection
id = dlr-db
host = localhost
username = NFCbankme2
password =  2emkanbCFN
database = dlr
max-connections = 1
```

The next test was to ascertain whether the bank server was talking or listening to the correct port; here, Kannel was used. The SMS gateway with the Kannel configuration file was edited to contain the following lines:

```
group = smsc
smsc = at
modemtype = premicell
device = /dev/ttyS1
```

In addition, for the default handling of the delivery reports (DLRs) we used the internal DLR storage, which required no special configuration. In order to configure bearerbox to use the internal DLR storage, we used dlr storage = internal in the core group. To store DLR information into MySQL database, we used the dlr storage = mysql configuration directive in the core group. A dlr-db group was defined that specified the table field names that were used to the DLR attributes and a mysql-connection group that defined the connection to the MySQL server itself.

```
group = mysql-connection
id = mydlr
host = localhost
username = NFCbankme2
password = 2emkanbCFN
database = dlr
max-connections = 1

group = dlr-db
id = mydlr
table = dlr
field-smsc = smsc
field-timestamp = ts
field-destination = destination
field-source = source
field-service = service
field-url = url
field-mask = mask
field-status = status
```

Also, the machine that ran the SMSC used it owns hostname. We set the IP-list to 127.0.0.1, which mapped to localhost and allowed only connections from these IP addresses to be accepted. The IP-list allowed one to maintain and search a list of IP addresses where each address was mapped to an arbitrary string for representation. We used a base64 format for message bytes such that testing for received messages had first to be decoded using base64 before entering the secure SMS protocol.

The returned messages were checked for the following and, if one was missing, the appropriate exception was thrown: correct message version bytes, sequence numbers mismatch, decrypting the received messages, whether message content had been compromised, and whether login in PIN was valid. In addition, they were checked to see if, when a transaction was successful, the server sent an encrypted notification back to the sender, and the existence of the account was confirmed in the database.

The results showed that testing whether an NFCbankme client could send and receive SMSs to/from the NFCbankme server proved successful. To test whether the specified port was the correct or listening port, we performed the following: a wrong port was used on both the NFCbankme client and server and the results on each occasion caused a wrong port exception to be thrown. The same thing happened when a non-specified port was used. However, a specified port caused a mobile phone to receive the message. Thus, the test was successful.

In order to use NFC to improve security in the SMS protocol, the encryption used was based on a GSM security algorithm, i.e. symmetric key encryption and AES with a 128-bit key length. The results recorded a speed of 183 milliseconds faster on average in a Nokia 6131 than in a Nokia 6212 Classic mobile phone. Another source of delay, this time in both NFC-enabled phones, was that an external NFC connection for a constantly polling target that is listening had first to be closed before opening an internal connection. We later observed this effect to be more pronounced in the Nokia 6212 Classic. A possibly explanation may be its slowness, as it does not immediately respond when brought into close range, which can be traced to the fact that it has less focus on a specific point than the Nokia 6131.

When decrypting messages, the mobile device was instrumented to record the time taken to accomplish tasks. The results showed that the maximum size of an SMS message input was $< 2^{64}$ and outputs 160 characters. Decrypting a message with an invalid key proved unsuccessful, as it threw an invalid key exception message.

The SHA-I algorithm was used to compute the message digest. In timing the execution speed of SHA-1, the results indicated that it took an average of 146 milliseconds. When different alteration forms were performed on the message digest bytes to see if a slight change, e.g. changing a single character, would produce a correct message or a different message digest, a different message digest was in fact produced.

More attack tests were conducted to include deliberately altering a portion of the content during transmission to cause a digest mismatch at the receiving end, since a new digest was created. This test proved sufficient against compromising the integrity of the message. The strength of the integrity checks was founded on how strong the algorithm that generated the digest value was and the strength of the encryption algorithm that hid the sensitive data.

On testing the replay attack in a situation where a third party was in possession of the transmitted messages, we stored every received message in the server and performed security checks on the sequence number for a specific account identifier. So the same message was transmitted multiple times. The result was that the server simply discarded identical messages after the first was received.

Another test was to attack the system armed with the knowledge of the PIN and an invalid OTP. This also proved futile, as the attacker needed a correct OTP that correctly encrypted the banking details. At the receiving end, the server was unable to decrypt the message using the database password. The system proved quite difficult for attackers to deceive.

Rebuilding NFCbankme into NFCme2u provided the latter with similar security features to those implemented in the former. Thus, the security aspects of NFCme2u were explored by giving users tasks to perform during the user studies. One of the tasks was to carry out a money transfer transaction a number of times with various changes in the steps involved (See Figure 4.15). The first set of changes required users to perform two sets of tasks, the first with a one-touch protocol and the second with two-touch protocol. Exactly 35% percent of the participants said they preferred the one-touch protocol, compared to the 65% who selected two-touch.

The second set of changes required three different types of authentication to be done: one-time authentication, authentication at every step and timed authentication. The one-time authentication implied that users only had to be authenticated once while interacting with the system, which took place at the beginning of the interaction (In frame/step I of Figure 4.15). Authentication at every stage meant that the user had to re-authenticate himself/herself at steps I, III, IV, VI and in the last step after the final window to end (See Figure 4.15). The fixed-timer method meant that users had three minutes to perform the one-time authentication.

The users used NFCme2u twice. On the first use, participants were given NFCme2u to use without any information about its security features. The second time, they were first informed of its many security features and then given NFCme2u to use. The results showed that participants did not think re-authentication was more secure than the fixed-timer method before making an informed decision, but preferred it slightly more after making an informed decision (See Figure 5.4). Also, participants stated that they felt that their payment was very secure using NFCme2u in the lower sinusoidal-like plot. At the end of the experiment, 42.5% of participants supported the use of one-time authentication and 57.5% preferred re-authentication at every stage.

In addition to the security features inherited from NFCbankme, NFCme2u was implemented to include encryption techniques, protocols and key exchange to improve security in the transaction (see Section 3.1 and Section 4.3.2). In the first touch, both parties had knowledge of one another, since identifying details were exchanged using certificates (see Figure 4.15). This identifying information is the

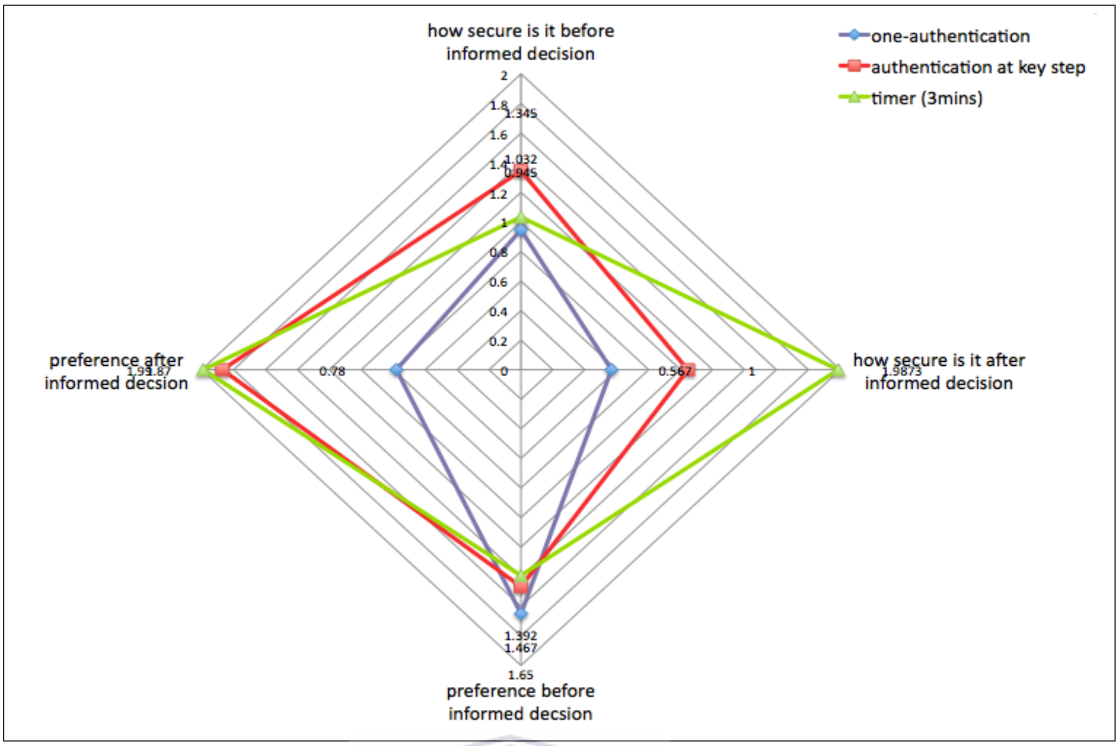


FIGURE 5.4 **Task speed in different authentication modes**
The radar graph plots task speed in different authentication modes and user perceptions of these authentication modes. Also, this Figure illustrates the preference for one-time authentication, which increased after an informed decision was made, as was expected. Preference for the fixed-timer method, which had three minutes to elapse, and how users felt about NFCme2u security improved after an informed decision was made.

payment message that the receiver must verify and top up as VM on his/her mobile phone during frame V. This triggers a receipt to be sent to the sender as proof of the transaction in frame VI.

These outcomes of either the receipt and/or payment message were either all or nothing. Furthermore, NFCme2u prevented users from making copies of the VM for reuse. When users attempted to tamper with the results of the payment, NFCme2u reacted by turning off the MIDlet and making it disappear. It only reappeared when a new session was started. The use of cryptography to store VM from a transaction made on the phone made unauthorised use impossible, even when the mobile phone was given to a participant to attempt to use another user's identity.

5.3 Analysis of usability

This section considers the question "How can NFC be used to improve usability of secure mobile financial services?" The user studies used NFCme2u and NFCpayme to answer this question. This section reports on the results and analysis in terms of the balance between security and usability.

For the first phase of the NFCme2u prototype, we had a complete GUI that offered information transfer and exchange using NFC. One objective was to determine key design decisions that improved user interaction with the NFCme2u prototype. The results were collected from users' feedback after they had carried out a set of tasks and certain parameters were measured.

When users were asked about various features of NFCme2u, the following results were obtained: 97.5% said they used the easy recovery tool, 90% said that telling them how much still needed to be done and where they were in the transaction was useful, and 95% said they understood details of the financial implications as a result of the helpful information given by the NFCme2u prototype. All participants agreed that the following features of the prototype were useful: displaying the user's current balance, requiring explicit confirmation of the full details of the payment, displaying a transaction summary screen after a transaction showing the expected post-transaction cash balance, and displaying a transaction summary screen after the transaction to show the current transaction cash balance.

In addition, the results provided information on how well NFCme2u compared in terms of other types of payment. With physical cash acting as the baseline, the measured parameters included: how easy it was to use, how fast it was to use, how steep the learning curve was, whether different situations/circumstances affected the performance of the system and whether calculations of the amount required no corrections or double checking.

The tasks involving the use of cash and NFCme2u required no introduction, and no learning effects was seen when going from using cash to using NFCme2u. Users were asked to make a payment to or receive a payment from the experimenter. For each participant, a coin toss randomly decided which to do first. The cash payment was done first and then the one using NFCme2u. Participants started the application by clicking on the MIDlet to start and finished only when the task was completed on the final screen. In each of the tasks, we measured the following variations: using simple cash with and without change, using NFCme2u with and without change, and using NFCme2u to request VM.

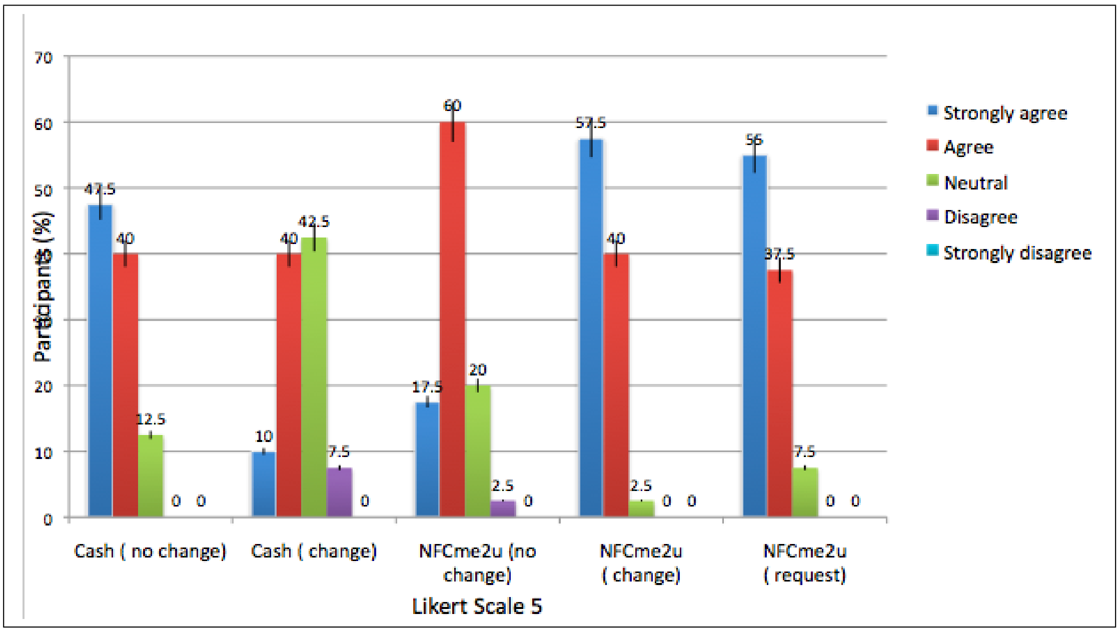


FIGURE 5.5 **NFCme2u: how fast to use?**
The figure is a column graph to illustrates how fast to use NFCme2u is. The potential for error in this figure is 5%.

In terms of how fast NFCme2u compared with the cash transactions, using NFCme2u without change was completed quickest (refer to Figure 5.5). This was closely followed by using NFCme2u to request VM, and next was using cash without change. Using cash without change was slower probably due to participants having to count their money before paying. The test using NFCme2u with change was slower than the one using cash with change. This is probably because participants were more careful about checking the amount of change they received.

The leaning curve (see Figure 5.6) for NFCme2u when compared to that of physical cash was reported as follows: 17.5% strongly agreed and 57% agreed that it was easy to learn to use NFCme2u without change; 50% strongly agreed and 47.5% agreed that it was easy to learn to use NFCme2u with change; and 30% strongly agreed and 47.5% agreed that it was easy to learn to use NFCme2u to request VM.

In Figure 5.7, 90% of participants strongly agreed to having more confidence in the accuracy of using NFCme2u with change, compared to 40% using physical cash with change. When no change was involved, 90% of participants strongly agreed that NFCme2u was more accurate, compared to 70% who strongly agreed that using physical cash was more accurate.

For the results on confidence in Figure 5.7, in both cases involving physical cash, participants were not told a priori that the cashier had no change. If the participant

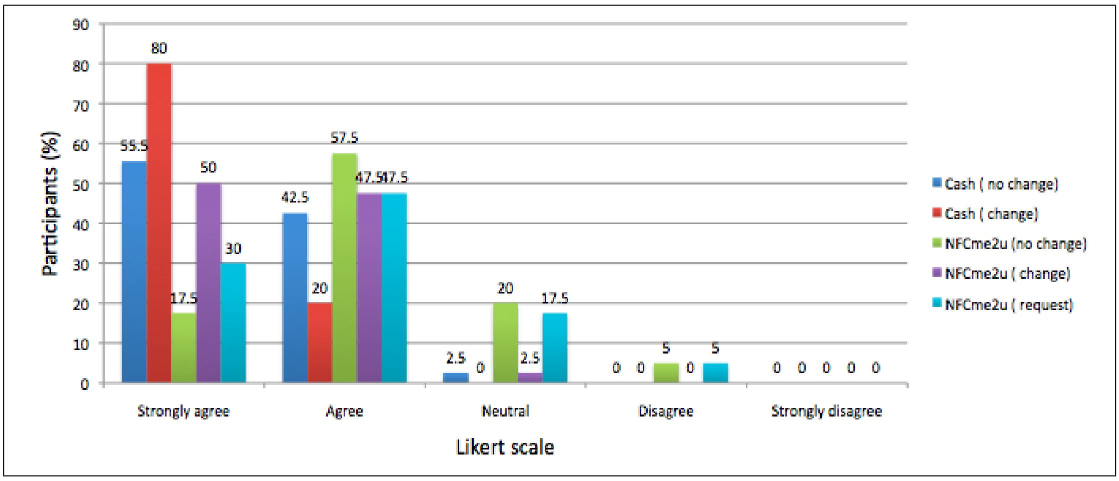


FIGURE 5.6 **Comparison of speed of use of NFCme2u and cash**
The figure is a column graph to illustrates how easy to learn NFCme2u. The potential for error in this figure is 5%.

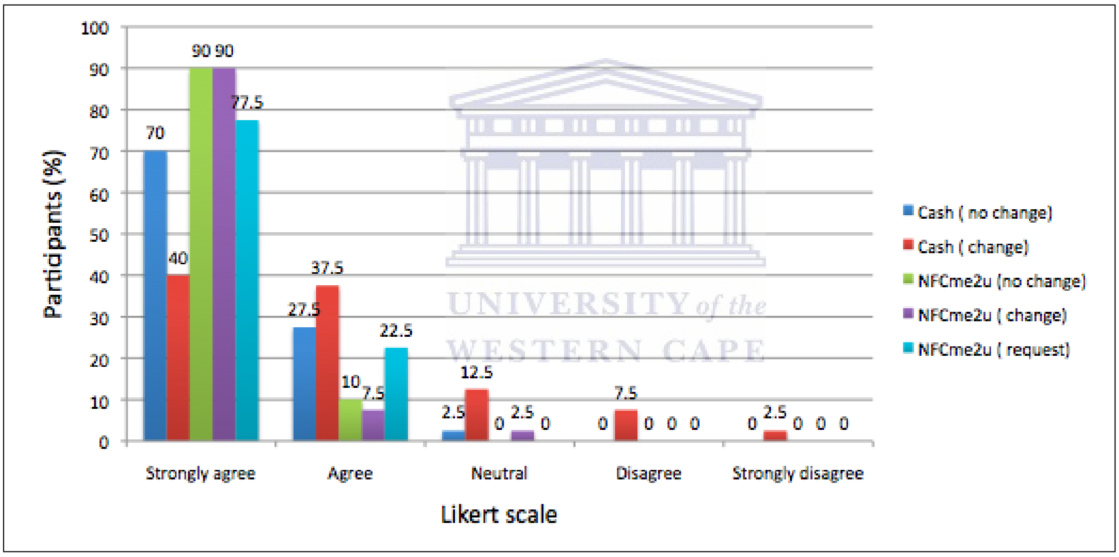


FIGURE 5.7 **Comparison of confidence in the accuracy of NFCme2u and cash transactions**
The potential for error in this figure is 5%.

provided a larger amount than the cost of the item, they were told to provide the exact change. We not only found that consumers were felt more confident using the NFCme2u prototype at this point, but they felt it was comparably faster than cash payments, and even more so with large cash transactions. Participants strongly agreed that using NFCme2u was more accurate and faster than using cash. As a result the felt more confident with using NFCme2u

Figure 5.7 shows perceived confidence in the accuracy of NFCme2u using a 5--point Likert scale, with lower scores indicating greater confidence. The majority of the participants made choices that fell within ‘strongly agree’ and ‘agree’ (i.e below unit 2) that NFCme2u was accurate. For the case of using physical cash with change required, the values were ‘disagree’ and ‘strongly disagree’. Using NFCme2u to request VM and using physical cash without change required fell within the domain of ‘agreed’ and ‘strongly agreed’.

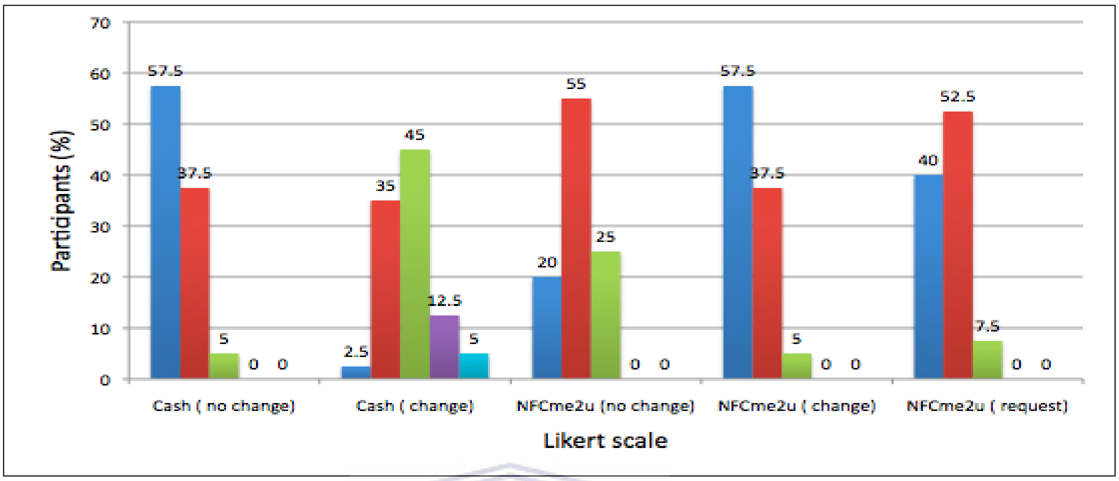


Figure 5.8 **Comparison of NFCme2u and cash transactions in terms of ease of learning how to use them**
This bar graph shows how easy it was to perform the experiment tasks with minimal training. The figure is a column graph also indicates error bars has the error amount at 5%

Figure 5.8 shows how participants rated NFCme2u’s ease of use with minimal training on a 5-point Likert scale. Ninety-five per cent of the participants either strongly agreed or simply agreed that NFCme2u with change was easy to use with minimal training, while 80% agreed or were neutral in terms of the ‘cash requiring change’ task, with minimal training.

Protocol using NFCme2u				
Parameters	**One-touch**		**Two-touch**	
Minimum	0.70	0.66	2.50	2.11
Maximum	2.40	2.21	4.02	3.02
Average	1.288	1.186	3.054	2.583
Standard deviation	0.3766	0.3841	0.2898	0.2911

Table 5.3: Runtime performance using NFCme2u: one-touch vs two-touch protocol
This table compares the two protocols on NFCme2u with and without change.

We recorded the time taken to use NFCme2u during the experiments for both the one-touch vs two-touch protocol, and the results are given in Table 5.3. As would be expected, completing the second protocol took longer than the first. The results of the mean and standard deviations reflect a similar pattern. The results were generally moderate, suggesting that a better cryptographic protocol could be used. Nevertheless, participants were satisfied with the overall performance of the NFCme2u system because it demonstrated faster performance than cash and had lower cognitive load.

The user preference in terms of receipt mode indicated that 60% of participants preferred their receipts to be provided in the text area, while 25% and 15% preferred to have their receipt in the drop-down list and combo box (see the questions in Table E.5). Predictable performance was obtained by computing the absolute difference between the cash with and without change, and also between NFCme2u with and without change. Most users were more favourable to accepting payment request options by doing the confirmation first (see the questions in Table E.5). NFCme2u provided all three modes, but the confirm first mode remained the default. The NFCme2u prototype gave users three ways of annotating receipts with a reason for the transaction (see the questions in Table E.5). When user preferences for information display (receipts, etc.) were examined among text area, drop-down list and combo box, text area was the most preferred.

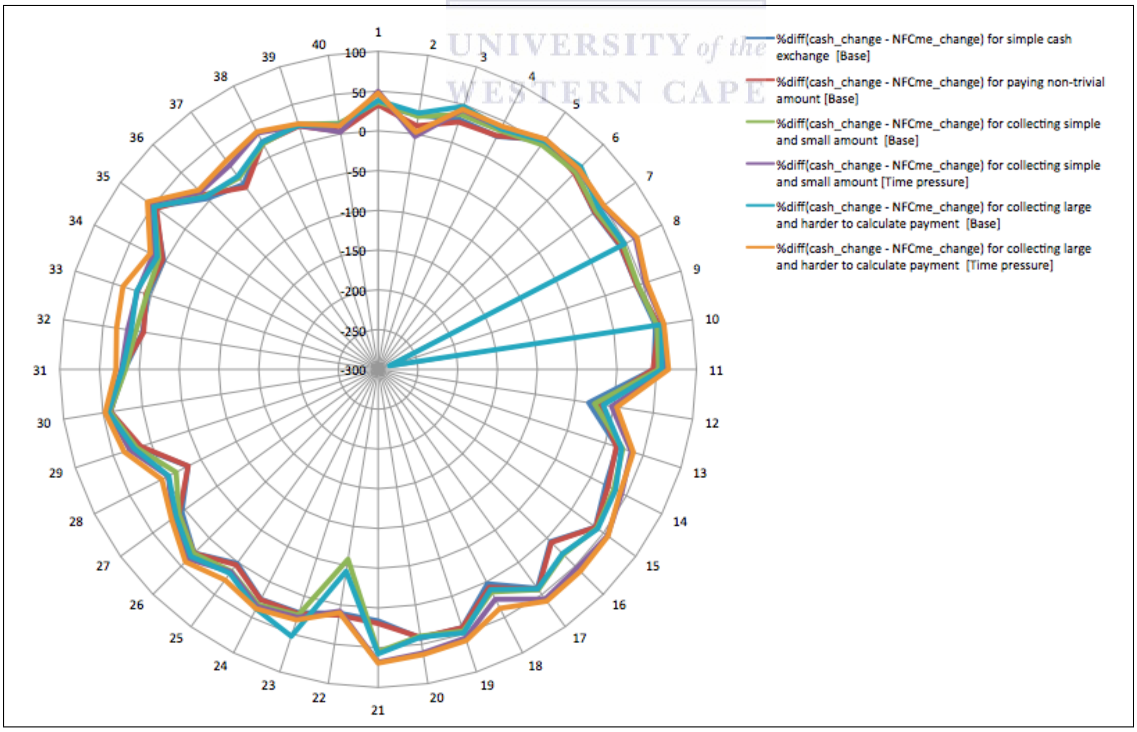


FIGURE 5.9 **NFCme2u: low cognitive load**
This diagram illustrates the cognitive load of NFCme2u and compares the load ratings with those of cash-based payment to demonstrate that NFCme2u has low cognitive load (refer to Appendix E: Table E.6).

Table E.7 provides cognitive load scores for four tasks: simple cash exchange, paying a non-trivial amount, collecting a simple-to-calculate and small amount, and collecting a large and harder-to-calculate amount. These tasks were first conducted with NFCme2u and then with cash. These scenarios measured the actual cognitive load: frustration, effort, temporary demand, physical demand, performance and mental demand using NASA TLX (see Table E.6).

In user study II, users were asked to provide ratings in six dimensions of load and rank those ratings using user-provided importance rankings. Based on Figure 5.9 and the associated tables, the values in the tables, the '% Diff.' column represents the difference between cash and NFCme2u for that scenario

$$\%diff = ((cash - NFCme2u)/cash) * 100. \tag{5.1}$$

Positive values imply that NFCme2u has lower cognitive scores than cash. This means NFCme2u. Furthermore, Figure E.1 indicates the IQR, while Table E.7 explains the values of q_numbers.

All participants felt that the following usability features were useful (see Table E.4): how much is needed to be done on each screen when doing a task, showing current balance during the transaction on the screen, showing the expected post-transaction cash balance, showing information details to fully understand the financial implications of the transaction, and explicitly confirming the full details of a payment (payee and amount). Only one person felt that she found the recovery tools difficult to use. According to her, it needed a help file or more instructions.

In terms of usability, more that 90% of participants felt that NFCme2u was more usable because of the many informative features and that it had excellent predictability and learnability features. Similarly, the prototypes were understandable and had useful features with regard to how participants would like to perform MFSs using such a system. The predictable performance of the prototype showed the prototype to be reasonably fast when compared to physical cash. Participants were confident when using the system and the results also showed that the system was accurate in explaining to users the responses that were required from them when they made payments or requested change.

Another perception was that the prototype was easy to use, given the minimal training provided. When the results on usability were presented, users perception of security was moderate, as they felt more security features might be needed. In terms of performance, participants were satisfied. A similar result was also obtained with lowering cognitive load. Users preferred the confirmation first mode and the simple text area for annotating the receipt. Furthermore, responses from participants indicated that the NFC-based prototype required few steps to accomplish a task, did what they asked it to do, and had a very informative and appealing GUI, while the majority of participants said they understood the information communicated.

User study II, discussed in Section 3.4.3, described the usability test that was conducted using NFCpayme. Three different authentication modes for the mpayment scheme were implemented such that their levels corresponded with the least to the most effort required of a customer to perform task, i.e. automatic, light and strong authentication. The level of difficulty or ease of use referred to the degree of risk, amount of money involved and security confirmation that was necessary. Users were asked to perform payment transaction tasks using NFCpayme in three different modes (refer to Table 5.4 for results, 3.1 for the task and Appendix E, Table E.1 for questions).

	Completion time mode			Maximum acceptable amount (ZAR)			
Mode	Automatic	Light	Full authentication	Mode	Automatic	Light	Full authentication
Seconds	%	%	%	Amount (ZAR)	%	%	%
< 5	40	12.5	5	< 100	27.5	25	15
< 10	32.5	32.5	12.5	< 250	37.5	55	32.5
< 20	17.5	30	25	<500	22.5	12.5	32.5
< 30	5	12.5	32.5	< 1000	10	7.5	20
< 45	2.5	7.5	15	< 5000	2.5	0	0
< 60	2.5	5	2.5				
>= 60	0	0	7.5				

TABLE 5.4: Completion time mode and maximum acceptable amount (ZAR)

The results in Table 5.4 show that 72.5% of the participants completed the tasks in under 10 seconds in automatic mode; 62.5% took between 10 and 20 seconds to do the same task in light confirmation mode; and 57% spent between 20 and 30 seconds to do the same task in full authentication mode. Furthermore, the results shows that 65% of the participants were willing to transact less than R250 while using the system in automatic mode, 80% were willing to transact less than R250 while using the system in light confirmation mode and 65% of the participants were willing to transact between R250 and R500 while using the system in full authentication mode. From these results, one can infer that, despite their low--income brackets, users were willing to transact a reasonable amount and their trend of transacting strongly supported the more strongly authenticated approach. Thus, security appeared to be of the utmost importance to them.

5.4 Analysis of transaction cost

During the user trials, this section considers the question “How can the trade--offs between usability and security be balanced to minimise transaction costs in NFC-based MFS systems?” The prototype considered was the NFCpayme.

To carry out the study on transaction cost, we used all 40 participants. Participants were given the tasks of carrying out payments using NFCpayme in a customer-merchant scenario. They were given an NFC-enabled mobile phone to make payment for a tagged item by swiping a CSC reader using a contactless ‘touch’ (Refer to Figure 4.13 and for the GUI and Figure 3.4 forth system set up). Each user performed the task in three different authentication modes: automatic, light confirmation and strong authentication.

The parameters measured were completion time, perceived convenience, anxiety over security, anxiety over reliability, anxiety over privacy and the maximum acceptable amount for the user to transact in a transaction. The results were not normally distributed and we needed to compare the distribution of two modes at a time for all three modes in terms of the parameters measured. Thus, we considered the non-parametric version of the paired sample t-test, two-related-samples, in which the Wilcoxon signed-rank test was used. The Wilcoxon signed-rank test considered information about both the sign of the differences and the magnitude of the differences between pairs. Because the Wilcoxon signed-rank test incorporates more information about the data, it is more powerful than the sign test. The data are ordinal and not nominal, which rules out the McNemar test and the extension known as the marginal homogeneity test.

Completion time in seconds for each of the authentication modes showed that the median of 40 participants in automatic mode was more than in light confirmation, but less in strong authentication. This result implied the medians of strong authentication and that of light confirmation are significantly different ($Z = -4.028$, $\rho < 0.05$, N = 40). This means the ‘Wilcoxon’ signed-rank statistic, converted to a z-score, is equal to -4.028 with a significance (ρ-value) equal to less than 0.05. Thus, it takes a significantly longer time to complete a task using in strong authentication than using light confirmation. Even more pronounced is the significant difference in using strong authentication and light confirmation ($Z = -5.480$,

$\rho < 0.05$, N = 40). A similar result was obtained with light confirmation and automatic mode, as there was a significant difference ($Z = -4.622$, $\rho < 0.05$, N = 40).

When perceived convenience for each authentication mode was considered, the results indicated that light confirmation and automatic mode had $Z = -5.517$ and $\rho < 0.05$; strong authentication and automatic mode had $Z = -5.49$ and $\rho < 0.05$; and strong authentication and light confirmation $Z = -2.54$ and $\rho = 0.011 < 0.05$. Furthermore, the results on anxiety over security was taken and showed that for light confirmation and automatic mode had $Z = -2.4$ and $\rho = 0.016 < 0.05$. However, for strong authentication and automatic mode, $Z = -1.83$ and $\rho = 0.067 > 0.05$, and strong authentication and light confirmation $Z = -0.347$ and $\rho = 0.729 > 0.05$ the results showed a greater significance value than the chosen ρ value. Nevertheless, the z-score is the value of interest to our study.

When we considered anxiety over reliability, light confirmation and automatic mode had $Z = -0.2$ and $\rho = 0.984 > 0.05$; strong authentication and automatic mode $Z = -0.815$ and $\rho = 0.415 > 0.05$; and strong authentication and light confirmation $Z = -0.892$ and $\rho = 0.372 > 0.05$. Also, when we looked at anxiety over privacy, light confirmation and automatic mode had $Z = -4.474$ and $\rho = 0.00 < 0.05$; strong authentication and automatic $Z = -4.857$ and $\rho = 0.00 < 0.05$; and strong authentication and light confirmation $Z = -0.324$ and $\rho = 0.001 < 0.05$.

We also considered whether there was any significant difference in the maximum acceptable amount users were willing to transact while using NFCpayme. The results showed that light confirmation and automatic mode were $Z = -4.348$ and $\rho < 0.05$; strong authentication and automatic $Z = -4.965$ and $\rho < 0.05$; and strong authentication and light confirmation $Z = -0.3458$ and $\rho = 0.01 < 0.05$.

The results showed that the majority of participants found the automatic mode the most convenient when compared with the other modes. Most rural students perceived more risk to be associated with light confirmation and strong authentication, whereas the migrant workers perceived higher anxiety to be associated with automatic mode, which may be as a result of their concern over the security of their money. Also, most migrant workers were reluctant to transact in the light confirmation or the automatic mode, while rural students were willing to transact large amounts using the light confirmation or automatic mode. On the question of how participants perceived convenience, 80% strongly agree when it came to automatic mode, 30% were neutral and 37.5% disagreed when it came to light confirmation mode, and in strong authentication mode 67.5% disagreed or strongly disagreed (See Table 5.5).

Perceived convenience mode				**Anxiety over security mode**			
	Automatic	**Light confirmation**	**Strong authentication**		**Automatic**	**Light confirmation**	**Strong authentication**
	%	%	%		%	%	%
Strongly agree	80	2.5	2.5	Very high	35	27.5	45
Agree	17.5	22.5	12.5	High	35	20	7.5
Neutral	2.5	30	17.5	Normal	17.5	10	0
Disagree	0	37.5	35	Low	2.5	20	7.5
Strongly disagree	0	7.5	32.5	Very low	10	22.5	40
Anxiety over reliability mode				**Anxiety over privacy mode**			
	Automatic	**Light confirmation**	**Strong authentication**		**Automatic**	**Light confirmation**	**Strong authentication**
	%	%	%		%	%	%
Very high	42.5	22.5	37.5	Very high	12.5	5	2.5
High	17.5	47.5	22.5	High	32.5	42.5	15
Normal	25	20	15	Normal	37.5	35	37.5
Low	12.5	10	7.5	Low	10	17.5	45
Very low	2.5	0	17.5	Very low	7.5	0	0

Table 5.5: Perceived convenience and anxiety
Perceived convenience and anxiety over security, reliability and privacy

In terms of transaction cost, based on the results of this study, the more security features were employed in the system, the less favourable the perception of usability from the participants. Furthermore, the more effort and time expended to perform each task, the higher the transaction cost for the participants. However, participants were willing to spend a higher maximum amount on the more secure authentication system than they were on the system they perceived to be the more usable one. However, while the migrant workers showed more fear of spending on any other authentication mode than on the strongly authenticated security system, rural students were more accepting or trusting of other modes with their maximum transaction amount.

5.5 Challenges

Various challenges constrained the extent of this study. Regarding the security attacks, a major drawback was that when NFCbankme was implemented, testing was done in a laboratory and a limited number of resources informed this process. The NFCbankme solution made use of a mobile phone and testing using the Kannel SMS gateway that used a backend MySQL database. The TCP/IP socket connection and Nokia 6131 emulator and phone were used. The successful client-server communication and retrieval of the desired results indicated that the desired outcome was obtained. We could not find a real banking environment that would allow our system to be tested. On the advice of our supervisors, we redesigned the NFCbankme into two new prototypes: NFCpayme and NFCme2u, in order to extend the range of the study.

Concerning transaction cost and usability, the main weakness with this experiment lay in the way in which risks were assessed. Risks are often difficult to evaluate, even in a well-administered laboratory-based study. NFCpayme's risks included to security, reliability and privacy. An accurate assessment of these risks remained a challenge and it is possible that they were underestimated.

5.6 Summary

This chapter presented results and analysis of a background study, and analysis in terms of security, usability and transaction cost. It also presented the challenges encountered during the study. The background study involved the use of a focus group, and demographic and preliminary studies. The focus group study identified the challenges facing MFSs and provided the necessary argument and results for subsequent activities and studies. The demographic survey showed that besides the variation in income, education and current place of residence, participants had a similar pattern of transactions. The results of the preliminary survey indicated that a subsequent study was needed on NFC-based MFSs and that a migrant workers target group should be added to the rural students group. This study also indicated the need to build an NFCbankme application to support MFSs. From the background study, it was clear that security, usability and transaction cost posed the biggest issues that needed to be addressed in further studies.

The results of the various security attacks were presented and they showed that it is possible to effectively secure an SMS and NFC-based MFS service for GSM networks. Successful results were obtained on the encrypting and decrypting of transmitted messages and the carrying out of digest mismatch tests using SHA-I on a number of messages. The results showed that reasonable MIDlet sizes and speed on mobile devices during use were obtainable. The test on replay attacks showed that NFC-based MFS applications can be effectively protected against replay attacks using cryptography.

On the question of usability, the conclusion may be drawn that NFCme2u is comparably faster than cash payment, and even more so with large common cash payments. The amount of money transferred using NFCme2u was accurate. It was observed that despite some participants using NFCme2u for the first time, the results were very encouraging. Most users were more favourable to accepting payment request options by first effecting confirmation. When user preferences for the display of information (receipts, etc.) were examined among text area, drop-down list, and combo box, text area was the most accepted. That the preference for one-time authentication increased after participants made an informed decision was to be expected. In addition, preference for the fixed timer, which had three minutes to elapse, improved after an informed decision was made in terms of user preference and how users felt about NFCme2u security. On transaction cost, the results showed that an increase in lighter interaction mode raised the users' anxiety, but also lowered the cost by enhancing usability and/or convenience. With light confirmation and automatic modes, users could afford the risk as long as the transaction size was sufficiently small. Thus, the benefits – security, reliability and privacy – appeared to outweigh the perceived risks. The inability to extend the support for user testing on NFCbankme into a real-world situation was a drawback.

Chapter 6

Conclusions

6.1 Conclusions

This study presents the results from work to develop three prototypes – NFCbankme, NFCpayme and NFCme2u – that use NFC technology to provide secure contactless MFSs on mobile phones. It considers the implementation and design of combining SMS and NFC technology in offering mbanking in a secure way. The study evaluated the trade-off between security and usability, how it affects the cost of transaction in mpayments and how user interaction modes can be used to minimise cost. The study covered design considerations and evaluated M2M money transfer system in two phases of user study, comparing VM usage with a physical cash-based system.

On the subject of security, the NFCbankme prototype was evaluated. Duplicating passwords were prevented, and encryption and decryption of encoded sent/received messages in a secure SMS protocol using base64 algorithm within a laboratory environment proved successful. Other tests were run on authentication, message integrity, strong anonymity and non-repudiation. The results showed that SMS-based MFSs can be secured and improved using NFC. Furthermore, security attacks were conducted on NFCbankme such as replay attacks and altering the message digest, and NFC-based MFSs proved to be secured. When the NFCme2u prototype was evaluated, it was relatively faster than using physical cash, especially with large amounts of money. Despite the fact that some participants were using NFCme2u for the first time, the results were very encouraging.

In all cases, the amount of money transferred using NFCme2u was accurate. Most users preferred accepting payment request options by effecting confirmation first. NFCme2u provided all three modes, but the confirm first mode remained the default. When user preferences for the display information (receipts, etc.) were examined among text area, drop-down list and combo box, the text area was the most preferred, while one-time authentication was also preferred. In addition, the fixed timer, which had three minutes to elapse, was preferred to provide security.

Transaction cost increased with lighter interaction mode by raising users' anxiety, but it also lowered this cost by enhancing usability and/or convenience. With light confirmation and automatic mode, users felt they could afford the risk as long as the transaction size was sufficiently small. Ultimately, the benefits of improved security, reliability and privacy appeared to outweigh the perceived risks.

A section of the thesis considered the various SMS-based MFS systems and then presented results to show that NFC can secure such systems. The results from carrying out security attacks and tests proved NFC-based MFS prototypes to be secure and participants were very satisfied. Regarding the usability of MFSs, the provision of a secured NFC-based MFS system that was simple, intuitive, easy to use, easy to learn, and that had a user-friendly interface improved unbanked participants' willingness to use MFSs. Furthermore, with regard to the issue of transaction cost of MFSs, the results showed that security and usability can each affect the transaction cost, which can impact on users' willingness to use MFSs.

This thesis assumed that various forecast made on the availability of NFC-enabled devices would prove to be true in the near future. Although NFC-enabled devices are already available and it is predicted that several hundred million NFC-equipped mobile phones will be in use by 2013, it is uncertain when the developing world will fully embrace their use. Market research estimates that 30% of all sold mobile phones in 2011 will be NFC-enabled. At the time of writing this thesis NFC-enabled devices were not yet available on the African continent and the funds to remedy this still needed to be made available.

6.2 Recommendation

MFS providers could add value for unbanked consumers by negotiating the full or partial deposit of various forms of government payments to users' mobile accounts, perhaps to an integrated, interest-bearing savings product. Also, because MFS technology involves strong network effects, providers seeking to reach the unbanked will benefit from marketing strategies that leverage existing social networks. In addition, for MFS technologies to gain traction in the marketplace, providers will have to guarantee all users a level of security and convenience comparable with, if not superior to, competing financial services.

For the success of NFC-based MFSs, a number of stakeholder dynamics must be taken into account. Cooperation from a host of stakeholders is needed for the successful use of NFC-based devices to make VM transactions: banks need to back VM; mobile device manufacturers and telecom SPs need to provide NFC-based handsets and promote NFC-based projects; and retail and regulatory bodies and policy-makers need to facilitate the legalising of p2p payments for consumers, particular for the unbanked. Furthermore, meeting the business and strategic goals of stakeholders requires the involvement of both government and regulatory bodies. The issues of policy strategies and regulatory changes are, however, beyond the scope of this thesis.

6.3 Future work

The success of SMS banking in developing economies, especially among the unbanked population, will depend on the general adoption of SMS banking, which we envisage will be informed by the issues of security and usability, and the convenience and accessibility of personal accounts. Data packets that transport mediums without overlaying protocols such as WAP/SMS have shown to be vulnerable, an example being the GSM. Although with overlaying protocol security is better enforced, this has not totally eliminated the possibility of security risks that could have a costly impact on mbanking.

In this thesis, a secure SMS mobile banking approach is presented with a special focus on its protocol and implementation. Furthermore, to provide alternative authentication for its mobile application, an NFC-based approach using asymmetric protocol analysis is suggested to eliminate the problem of phishing. However, this involves a lot of hand/finger movements, which proves not to be cost-effective, but was employed because security had greater priority in this study. In our design we assumed that mbanking applications would be pre-installed on the client's mobile device. However, this is likely not cost-effective at present and mobile phone manufacturers would have to deliver in this area.

Defining NFC-based services and applications requires not just solving the related technological problems, but also designing the appropriate business models and processes. These will involve card companies and MNOs, who are important in harmonising interoperable solutions in order to gain market acceptance, or the technology itself will cease to grow.

It is important for the viability of NFC-based projects to secure mass-market appeal by leveraging scale economies and the network externality effect where NFC-based projects for MFSs may influence social networks. Providing a highly usable, secure and generally effective alternative to all cash-based transactions may potentially increase mass-market appeal. Since these benefits appear to be feasible, the focus was on these aspects. A gradual introduction into the market is one way of considering NFC-based MFSs as a substitute for existing MFS solutions such as topping up scratch cards, buying coupons, purchasing items at vending machines or using phone cards in phone booths. Increasing support for NFC-based MFSs will motivate the unbanked to use MFSs and ensure the success of those who offer them.

Bibliography

[1] Aday, L. & Cornelius, L. (2006). *Designing and conducting health surveys: A comprehensive guide*. San Francisco: Jossey-Bass Inc Pub.

[2] Aigner, M., Dominikus, S., & Feldhofer, M. (2007). A system of secure virtual coupons using NFC technology. *IEEE International Conference on Pervasive Computing and Communications Workshops*, (pp. 362–366). Piscataway, NJ: IEEE Press.

[3] Al-Tawil, K. & Akrami, A. (1999). A new authentication protocol for roaming users in gsm networks. *International Symposium on Computers and Communications*, (p. 93). Washington, DC: IEEE Computer Society.

[4] Alliance, S. (2007). In *Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure*, Princeton Junction, NJ: Smart Card Alliance.

[5] Anyasi, F. & Otubu, P. (2009). Mobile phone technology in banking system: Its economic effect. *Research Journal of Information Technology*, 1(1), 1–5.

[6] Balan, R. K. & Ramasubbu, N. (2009). The digital wallet: Opportunities and prototypes. *Computer*, *42*(4), 100 –102.

[7] Balan, R. K., Ramasubbu, N., Prakobphol, K., Christin, N., & Hong, J. (2009). mFerio: The design and evaluation of a peer-to-peer mobile payment system. *MobiSys '09: Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services*, (pp. 291–304). New York, NY: ACM.

[8] Barkan, E., Biham, E., & Keller, N. (2008). Instant ciphertext-only cryptanalysis of GSM encrypted communication. *Journal of Cryptology*, 21, 392–429.

[9] Ben-Asher, N., Meyer, J., Moller, S., & Englert, R. (2009). An Experimental System for Studying the Tradeoff between Usability and Security. *International Conference on Availability, Reliability and Security*, (pp. 882–887). Los Alamitos, CA: IEEE Computer Society.

[10] Benyó, B., Sodor, B., Fordos, G., Kovacs, L., & Vilmos, A. (2010). A generalized approach for NFC application development. *International Workshop on Near Field Communication*, (pp. 45–50). Los Alamitos, CA: IEEE Computer Society.

[11] Benyó, B., Vilmos, A., Fördös, G., Sódor, B., & Kovács, L. (2009). The StoLpaN view of the NFC ecosystem. In *WTS'09: Proceedings of the 2009 Conference on Wireless Telecommunications Symposium*, (pp. 233–237). Piscataway, NJ: IEEE Press.

[12] Brief, A. E. (2004). AfDB. *Director*, *216*, 7110.

[13] Broll, G., Keck, S., Holleis, P., & Butz, A. (2009). Improving the accessibility of NFC/RFID-based mobile interaction through learnability and guidance. In *MobileHCI '09: Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*, (pp. 1–10). New York, NY: ACM.

[14] Chen, J. J. & Adams, C. (2004). Short-range wireless technologies with mobile payments systems. In *ICEC '04: Proceedings of the 6th international conference on Electronic commerce*, (pp. 649–656). New York, NY: ACM.

[15] Chen, L.-d. (2008). A model of consumer acceptance of mobile payment. *International Journal of Mobile Communication*, *6*(1), 32–52.

[16] Chen, W., Hancke, G., Mayes, K., Lien, Y., & Chiu, J. (2010). NFC mobile transactions and authentication based on GSM network. In *2nd International Workshop on Near Field Communication*, (pp. 83–89). Los Alamitos, CA: IEEE Computer Society.

[17] Chen, Z. (2000). *Java Card technology for smart cards: Architecture and programmer's guide.* Boston, MA: Addison-Wesley Longman Publishing.

[18] Cheng, H.-C., Chen, J.-W., Chi, T.-Y., & Chen, P.-H. (2009). A generic model for NFC-based mobile commerce. In *ICACT'09: Proceedings of the 11th International conference on Advanced Communication Technology.* (pp. 2009–2014). Piscataway, NJ: IEEE Press.

[19] Chikomo, K., Chong, M. K., Arnab, A., & Hutchison, A. (2006). *Security of mobile banking*, University of Cape Town, South Africa, Technical Report, 1 Nov.

[20] Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches.* Thousand Oaks, CA: Sage Publications, Inc.

[21] Davison, R. M. (2002). Ethics and research methods. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, (pp. 3439–3445).

[22] Dominikus, S. & Aigner, M. (2007). mCoupons: An application for Near Field Communication (NFC). In *AINAW '07: Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, (pp. 421–428). Washington, DC: IEEE Computer Society.

[23] Donner, J. (2008). Research approaches to mobile use in the developing world: A review of the literature. *The Information Society*, *24*(3), 140–159.

[24] Donner, J. (2009). Blurring livelihoods and lives: The social uses of mobile phones and socioeconomic development. *Innovations: Technology, Governance, Globalization*, *4*(1), 91–101.

[25] Donner, J. & Tellezb, C. (2008). Mobile banking and economic development: Linking adoption, impact, and use. *Asian Journal of Communication*, *18*(4), 318–332.

[26] Dörflinger, J., Friedland, C., Merz, C., & de Louw, R. (2009). Requirements of a mobile procurement framework for rural South Africa. In *Proceedings of the 6th International Conference on Mobile Technology, Application and Systems.* (pp. 1–4). Nice, France: ACM.

[27] Duncombe, R. & Boateng, R. (2009). Mobile phones and financial services in developing countries: A review of concepts, methods, issues, evidence and future research directions. *Third World Quarterly*, *30*(7), 1237–1258.

[28] Emmanuel, A. & Jacobs, B. (2007). Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services, (pp. 23–33). Radboud University Nijmegen, Netherlands: Citeseer.

[29] Finkenzeller, K. (2003). *RFID handbook: Fundamentals and applications in contactless smart cards and identification.* New York, NY: John Wiley and Sons.

[30] Fowler, F. (2009). *Survey research methods.* Newbury Park, CA: Sage Publications, Inc.

[31] Fuchs, C. & Horak, E. (2008). Africa and the digital divide. *Telematics and Informatics*, *25*(2), 99–116.

[32] Ghìron, S. L., Sposato, S., Medaglia, C. M., & Moroni, A. (2009). NFC Ticketing: A prototype and usability test of an NFC-based virtual ticketing application. *NFC '09: Proceedings of the 2009 First International Workshop on Near Field Communication*, (pp. 45–50). Washington, DC: IEEE Computer Society.

[33] Groves, R., Dillman, D., Eltinge, J., Little, R., Biemer, P., Groves, R., Lyberg, L., Mathiowetz, N., Sudman, S., Dillman, D., et al. (2005). Survey methodology. *Technometrics*, *47*(2), 246–246.

[34] Hardy, R., Rukzio, E., Wagner, M., & Paolucci, M. (2009). Exploring Expressive NFC-Based Mobile Phone Interaction with Large Dynamic Displays. *NFC '09: Proceedings of the 2009 First International Workshop on Near Field Communication*, (pp. 36–41). Washington, DC: IEEE Computer Society.

[35] Hayashi, E., Dhamija, R., Christin, N., & Perrig, A. (2008). Use your illusion: secure authentication usable anywhere. *Proceedings of the 4th Symposium on Usable Privacy and Security*, (pp. 35–45). Pittsburgh, PA: ACM.

[36] Herzberg, A. (2003). Payments and banking with mobile personal devices. *Communications of the ACM*, *46*(5), 53–58.

[37] Hu, X., Li, W., & Hu, Q. (2008). Are mobile payment and banking the killer apps for mobile commerce? *In Proceedings of the Hawaii International Conference on System Sciences*, (p. 84). Los Alamitos, CA: IEEE Computer Society.

[38] Hughes, N. & Lonie, S. (2007). M-pesa: Mobile money for the "unbanked"; turning cellphones into 24-hour tellers in kenya. *Innovations: Technology, Governance, Globalization*, *2*(1-2), 63–81.

[39] Ivatury, G. & Mas, I. (2008). The early experience with branchless banking. *CGAP Focus Note*, *46*.

[40] Jamil, S. & Mousumi, F. (2009). Short messaging service (SMS)-based m-banking system in context of Bangladesh. In *ICCIT 2008: 11th International Conference on Computer and Information Technology*, (pp. 599–604). Washington, DC: IEEE Computer Society.

[41] Jones, M. & Marsden, G. (2006). *Mobile interaction design*. Chichester, West Sussex UK: John Wiley & Sons Ltd.

[42] Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, *24*(2), 381–394.

[43] Kadambi, K. S., Li, J., & Karp, A. H. (2009). Near-field communication-based secure mobile payment service. *ICEC '09: Proceedings of the 11th International Conference on Electronic Commerce*, (pp. 142–151). New York, NY: ACM.

[44] Kasper, T., Carluccio, D., & Paar, C. (2007). An embedded system for practical security analysis of contactless smartcards. *WISTP'07: Proceedings of the 1st IFIP TC6 /WG8.8 /WG11.2 International Conference on Information Security Theory and Practices*, (pp. 150–160). Berlin, Heidelberg: Springer–Verlag.

[45] Kfir, Z. & Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard. *International Conference on Security and Privacy for Emerging Areas in Communications Networks*, (pp. 47–58). Los Alamitos, CA: IEEE Computer Society.

[46] Knudsen, J. (2003). *Wireless Java: Developing with J2ME*. New York, NY: Apress.

[47] Kreyer, N., Pousttchi, K., & Turowski, K. (2002). Standardized payment procedures as key enabling factor for mobile commerce. *E-Commerce and Web Technologies*, (pp. 383–390). Augsburg, Germany: Springer–Verlag.

[48] Kungpisdan, S., Srinivasan, B., & Le, P. D. (2005). A secure account-based mobile payment protocol. In *ITCC 2004: Proceedings of the International Conference on Information Technology: Coding and Computing*, volume 1. (pp. 35–39). Las Vegas, NV: IEEE Computer Society.

[49] Lacmanovic, I., Radulovic, B., & Lacmanovic, D. (2010). Contactless payment systems based on RFID technology. *MIPRO, 2010 Proceedings of the 33rd International Convention*, (pp. 1114–1119). Washington, DC: IEEE Computer Society.

[50] Larman, C. & Basili, V. (2003). Iterative and incremental developments: A brief history. *Computer*, *36*(6), 47–56.

[51] Leavitt, N. (2010). Payment applications make e-commerce mobile. *Computer*, *43*, 19–22.

[52] Lehdonvirta, V., Soma, H., Ito, H., Yamabe, T., Kimura, H., & Nakajima, T. (2009). UbiPay: Minimizing transaction costs with smart mobile payments. *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems*, (pp. 1–7). New York, NY: ACM.

[53] Lo, J. L., Bishop, J., & Eloff, J. H. (2008). SMSSec: An end-to-end protocol for secure SMS. *Computers & Security*, *27*(5-6), 154–167.

[54] Lord, S. (2003). Trouble at the telco: When GSM goes bad. *Network Security*, *2003*(1), 10–12.

[55] Madlmayr, G. (2008). A mobile trusted computing architecture for a Near Field Communication ecosystem. In *iiWAS '08: Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services*, (pp. 563–566). New York, NY: ACM.

[56] Madlmayr, G., Brandlberger, D., Langer, J., & Scharinger, J. (2008). Evaluation of smartcard webserver as an application platform from a user's perspective. In *MoMM '08: Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia*, (pp. 360–363). New York, NY: ACM.

[57] Madlmayr, G., Dillinger, O., Langer, J., & Schaffer, C. (2007). The benefit of using sim application toolkit in the context of Near Field Communication applications. *International Conference on Mobile Business*, (p. 5). Los Alamitos, CA: IEEE Computer Society.

[58] Madlmayr, G., Kleebauer, P., Langer, J., & Scharinger, J. (2008). Secure Communication between Web Browsers and NFC Targets by the Example of an e-Ticketing System. *In EC-Web '08: Proceedings of the 9th international conference on E-Commerce and Web Technologies*, (pp. 1–10). Berlin, Heidelberg: Springer–Verlag.

[59] Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). NFC devices: Security and privacy. *Proceedings of the 2008 Third International Conference on Availability, Reliability and Security*, (pp. 642–647). Washington, DC: IEEE Computer Society.

[60] Madlmayr, G., Langer, J., & Scharinger, J. (2008). Managing an NFC ecosystem. *7th International Conference on Mobile Business*, (pp. 95–101). Washington, DC: IEEE Computer Society.

[61] Mallat, N. (2007). Exploring consumer adoption of mobile payments - a qualitative study. *Journal of Strategic Information System*, *16*(4), 413–432.

[62] Mallat, N., Rossi, M., & Tuunainen, V. K. (2004). Mobile banking services. *Communications of the ACM*, *47*(5), 42–46.

[63] Massoth, M. & Bingel, T. (2009). Performance of different mobile payment service concepts compared with a NFC-based solution. *International Conference on Internet and Web Applications and Services*, (pp. 205–210). Los Alamitos, CA: IEEE Computer Society.

[64] Matsuoka, Y., Schaumont, P., Tiri, K., & Verbauwhede, I. (2004). Java cryptography on KVM and its performance and security optimization using HW/SW co-design techniques. *Proceedings of the 2004 International Conference on Compilers, Architecture, and Synthesis for Embedded Systems*, (P. 311). New York, NY: ACM.

[65] Mbogo, M. (2010). The impact of mobile payments on the success and growth of micro-business: The case of M-Pesa in kenya. *Journal of Language, Technology & Entrepreneurship in Africa*, *2*(1), 182.

[66] Michahelles, F., Thiesse, F., Schmidt, A., & Williams, J. R. (2007). Pervasive RFID and Near Field Communication technology. *IEEE Pervasive Computing*, *6*(3), 94–96.

[67] Min, Q., Li, S., & Zhong, Q. (2009). An empirical study of M-Commerce adoption from usability perspective. *International Conference on Mobile Business*, (pp. 215–220). Los Alamitos, CA: IEEE Computer Society.

[68] Mirabaud, N. (2009). Migrants' remittances and mobile transfer in emerging markets. *International Journal of Emerging Markets*, *4*(2), 108–118.

[69] Mitha, A. (2011). *The transformative role of Mobile Financial Services and the role of German Development Cooperation.* Eschborn, Germany: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

[70] Morawczynski, O. & Miscione, G. (2008). Examining trust in mobile banking transactions: The case of M-PESA in kenya. *Social Dimensions of Information and Communication Technology Policy*, (pp. 287–298). Boston: Springer.

[71] Morse, J. (1991). Approaches to qualitative-quantitative methodological triangulation. *Nursing Research*, *40*(2), 120.

[72] Mulliner, C. (2009). Vulnerability analysis and attacks on NFC-enabled mobile phones. *International Conference on Availability, Reliability and Security*, (pp. 695–700). Los Alamitos, CA: IEEE Computer Society.

[73] Nie, J. & Hu, X. (2008). Mobile banking information security and protection methods. *International Conference on Computer Science and Software Engineering, 3*, (pp. 587–590). Los Alamitos, CA: IEEE Computer Society.

[74] Ohkubo, M., Suzuki, K., & Kinoshita, S. (2005). RFID privacy issues and technical challenges. *Communications of the ACM*, *48*(9), 66–71.

[75] Ondrus, J. & Pigneur, Y. (2007). An assessment of NFC for future mobile payment systems. *International Conference on Mobile Business*, (p. 43). Los Alamitos, CA: IEEE Computer Society.

[76] Ortiz Jr., S. (2006). Is Near-Field Communication close to success? *Computer*, *39*(3), 18–20.

[77] Paik, M. (2010). Stragglers of the herd get eaten: Security concerns for gsm mobile banking applications. *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, (pp. 54–59). New York, NY: ACM.

[78] Panjwani, S. & Cutrell, E. (2010). Usably secure, low-cost authentication for mobile banking. *Proceedings of the Sixth Symposium on Usable Privacy and Security*, (PP. 1–12). New York, NY: ACM.

[79] Paret, D. (2005). *RFID and contactless smart card applications.* West Sussex, UK: John Wiley and Sons.

[80] Pering, T., Anokwa, Y., & Want, R. (2007). Gesture connect: Facilitating tangible interaction with a flick of the wrist. *TEI '07: Proceedings of the 1st International Conference on Tangible and Embedded Interaction*, (pp. 259–262). New York, NY: ACM.

[81] Porteous, D. (2006). The enabling environment for mobile banking in Africa. London, UK: DFID.

[82] Preneel, B. (2007). A survey of recent developments in cryptographic algorithms for smart cards. (1) advances in smart cards and (2) topics in wireless broadband systems. *Computer Networks*, *51*(9), 2223 – 2233.

[83] Rankl, W. & Effing, W. (2004). *Smart card handbook.* Chichester: John Wiley.

[84] Rashid, A. & Elder, L. (2009). Mobile phones and development: An analysis of IDRC-supported projects. *The Electronic Journal of Information Systems in Developing Countries*, *36*.

[85] Rea, L., Parker, R., & Allen, R. (1997). *Designing and conducting survey research: A comprehensive guide.* San Francisco, CA: Jossey-Bass.

[86] Reveilhac, M. & Pasquet, M. (2009). Promising secure element alternatives for nfc technology. *NFC '09: Proceedings of the 2009 First International Workshop on Near Field Communication*, (pp. 75–80). Washington, DC: IEEE Computer Society.

[87] Sale, J., Lohfeld, L., & Brazil, K. (2002). Revisiting the quantitative-qualitative debate: implications for mixed-methods research. *Quality and Quantity, 36*(1), 43–53.

[88] Sander, C. (2009). *Remittance money transfers, microfinance and financial integration: Of credo, cruxes, and convictions.* Berlin & Heidelberg: Springer.

[89] Sparks, D. (2008). Electronic Payments in sub-saharan Africa: Will mobile telephony accounts systems be the next leapfrog technology for development? *International Review of Business Research Papers*, *4*(1), 325–336.

[90] Taghiloo, M., Agheli, M., & Rezaeinezhad, M. (2010). Mobile-based secure digital wallet for peer to peer payment system. *Arxiv preprint arXiv:1011.0279.*

[91] Tiwari, R., Buse, S., & Herstatt, C. (2006). Customer on the move: Strategic implications of mobile banking for banks and financial enterprises. *IEEE International Conference on Enterprise Computing, E-Services and E-Commerce Technology.*

[92] Van Damme, G., Wouters, K. M., Karahan, H., & Preneel, B. (2009). Offline NFC payments with electronic vouchers. *MobiHeld '09: Proceedings of the 1st ACM Workshop on Networking, Systems, and Applications for Mobile Handhelds*, (pp. 25–30). New York, NY: ACM.

[93] Varshney, U. & Vetter, R. (2001). A framework for the emerging mobile commerce applications. *Proceedings of the Hawaii International Conference on System Sciences*, *9*, (p. 9014). Los Alamitos, CA: IEEE Computer Society.

[94] Want, R., Fishkin, K. P., Gujar, A., & Harrison, B. L. (1999). Bridging physical and virtual worlds with electronic tags. *Proceedings of the SIGCHI*

Conference on Human Factors in Computing Systems: The CHI is the Limit, (pp. 370–377). Pittsburgh, PA: CHI'99.

[95] Wiechert, T., Thiesse, F., Michahelles, F., Schmitt, P., & Fleisch, E. (2007). Connecting mobile phones to the internet of things: A discussion of compatibility issues between EPC and NFC. *Americas Conference on Information Systems, AMCIS*, Keystone. CO: AMCIS '07.

[96] Yeh, T.-C., Wang, Y.-J., Kuo, T.-C., & Wang, S.-S. (2010). Securing RFID systems conforming to EPC class 1 generation 2 standard. *Expert Systems with Applications*, *37*(12), 7678–7683.

Appendix A

Information sheet

What is this about? I am going to tell you about a software project based on a new technology called NFC that can be used for a number of things such as purchasing items, banking, and money transfer especially by people from and in rural communities. In addition, the project objective is to let you send money to and/or receive money from your relatives or friends in rural area.

Who is running the project? We are Computer Science researchers from the University of the Western Cape and the University of Cape Town. You might know Dr. Bill Tucker. He is the project leader. The student responsible for this particular project is Poroye Adeola (Seyi).

What do we want to do? We want to improve communications for banking of the unbanked (provide financial service to those from rural areas). There are many mobile phone financial service providers systems available on mobile phone. These systems (For instance, mobile phone financial service providers systems) make use of the Internet but they are not designed to help cater for rural areas. The different mobile phone financial service providers is that most of the systems do not use NFC at the moment.

What will we do? Our research group will provide the computer equipment and other relevant resources for this project. We will design and build the software for mobile phone financial service solution. The main criticism of our approach is that both the simulation of the real thing and the actual implementation have not been fully and rigorously tested beyond the laboratory experimentation.

What do we expect of you? We want students and temporary internal migrant workers from rural area to help us design the system . We do not expect this participants to build a software because that is what we do. But we do not know how the rural community have been transacting cash and how they will respond to the NFC-based solutions. Participants from rural area understand how cash transactions are done in rural areas very well and they understand the needs better than we do.

That is why we want to work together. We can help participants from rural area learn about technology. Participants will give us very good ideas about how technology can affect the lives of folks in rural communities. We want to use those ideas to build better software for the person(s) living from and in rural areas.

If you agree to join this project, we will ask you to sign a consent form. You may leave the project at any time without any penalty to you at all. Participation is your free choice. You will be asked to use the system and allow yourself to be interviewed about the system.

Appendix B

Consent form

I, ——————, fully understand the NFC-based project and I agree to participate. I understand that all information that I provide will be kept confidential, and that my identity will not be revealed in any publication resulting from the research unless I choose to give permission. Furthermore, all recorded interview media and transcripts will be destroyed after they have been analysed. I am also free to withdraw from the project at any time.

I understand that NFC-based solutions is aimed at providing NFC research support for banking the unbanked and/or underbanked from and/or in rural areas of South Africa. In addition, the interviewer is bound by a code of ethics that does not allow him/her to repeat any information that is given during the discussions. This means that my identity will remain confidential. For further information, please do not hesitate to contact:

Poroye Adeola Oluwaseyi,
Dept of Computer Science, University of the Western Cape
Private Bag X17, Bellville 7535
Email: xxxxxxx@uwc.ac.za (The complete information was provided)
Phone: 021 959 xxxx (The complete information was provided)

Cell/Phone: ——————
Name: ——————
Signature: ——————
Date: ——————

Appendix C

Background study

C.1 First activity: focus group study

We provide questions used during the focus group session for seven participants. Information (Please tick ($\surd$) in front of your selection)

About you

In this focus group meeting we will like to ask you some questions about what you think of a software that can be used on a mobile phone to carry out banking anywhere and anytime.

- **Your Date of Birth** DD_____ MM_____ YYYY __________
- **Your Gender** □ F □ M
- **Your Academic Program** □ Undergraduate □ Postgraduate □ Other (if other specify) ____
- **Have you worked before?** □ Yes □ No
- **Are you currently working?** □ Yes □ No

About the Conversation

We now ask questions about your home in rural community.

- **Amount you get from home per month (ZAR)?** □ None □ < 250 □ < 500 □ < 1000 □ >= 1000

- **Amount you send home per month (ZAR)?** □ None □ < 250 □ < 500 □ < 1000 □ >= 1000

- **Means of transferring money to/fro home?** □ Banks □ People □ Other (if other specify) ________________

- **Means of communicating with people at home?** □ mobile phone □ internet □ Other (if other specify) ________________

- **Travelling distance from bank to home (km)?** □ < 1 □ < 2 □ < 5 □ < 10 □ >= 10

- **Which social amenities do you have at home?** □ Mobile network □ Internet □ Electricity □ Fixed Landline

- **Additional information that you might like to share with us?**

  ____

  ____

  ____

  ____

  (Thank you for your time and please have some tea and snacks before you go)

C.2 Second activity: demography study

This question pertain the demography questions posed and answered during the preliminary background survey for 20 rural students. Information (Please tick ($\surd$) in front of your selection)

- **Your Date of Birth?** □ < 20 □ $20-29$ □ $30-39$ □ $40-49$ □ >= 50

- **Highest level of Education?** □ None □ High School □ Undergraduate □ Graduate □ Postgraduate □ Other (if other specify) ________________

- **Marital status** □ Married □ Single □ Divorce ________________

- **Your Gender** □ F □ M

- **Employment status** □ Part-Time □ Full-Time □ None □ Self-employed □ Casual worker

- **Home language?** □ Afrikaans □ IsiXhosa □ Sesotho □ Setswana □ IsiZulu □ Other (if other specify) ________________

- **Current living place?** □ UWC campus □ Bellville □ Mowbray □ Stellenbosch □ Parow □ Other (if other specify) ________________

- **Original living province (with household)?** □ Eastern Cape □ Kwa--Zulu Natal □ North West □ North Central □ Western Cape □ Other (if other specify) ________________

- **Type of residence back home?** □ House □ Informal settlement □ Flat □ Other (if other specify) ________________

- **Purpose of moving here (Target group)?** □ Rural student □ Migrant workers □ Other (if other specify) ________________

- **Travelling distance from bank to home (km)?** □0 □1 □2 □3 □ > 3

- **How frequently do you travel home (per year)?** □1 □2 □3 □ > 3

- **Last time back home?** □ $<$ 1week □ $<$ 1month □ $<$ 6months □ $<$ 12 months □ $>=$ 1year

- **Number of mobile phone(S) you own?** □0 □1 □2 □3 □ > 3

C.3 Third activity: preliminary survey

This question pertain the participant's payment questions posed and answered during the preliminary background survey for 20 rural students.

Preliminary survey: Part I

We ask questions about the payment prototype and the concept you have just seen.We would like to ask you to take part in this survey.

- **What group of people will need it the most?**
  □ Rural students □ Migrant workers □ Entrepreneurs □ Other (if other specify) ________________

- **What mostly will it be used for?**
  □ Banking service □ payment at shop's POS □ Transportation □ Money remittance □ Other (if other specify) ____________

- **Amount you will be willing to spend on an NFC phone (ZAR)?**
  □ < 100 □ < 250 □ < 500 □ < 1000 □ >= 1000

- **What part of the prototype will you like to see improve?**□ Interface □ Functionality □Security □ Other (if other specify) ____________

- **Time taken to perform task(seconds)?** □ < 10 □ < 20 □ < 30 □ < 60 □ >= 60

- **How composed were you during the experiment?** □ Confident □ Excited □Calm □Unsure □ Other (if other specify) ____________

Preliminary survey: Part II

For this part (part II) of the preliminary payment survey questionnaire, please consult Likert scale in Table C.1 for the options in scale category. We ask question about the payment prototype and the concept you have just seen.We would like to ask you to take part in this survey.

- **Is there a need for NFC (scale category is E in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

- **Will you use the NFC based solution, if deployed (scale category is E in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

- **How easy is it to use (scale category is A in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

- **Will you tell others about it(scale category is E in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

- **How easy is it to learn(scale category is A in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

- **How safe did you feel when using it (scale category is A in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

Likert Scale Table

#	**A**	**B**	**C**	**D**	**E**	**F**	**G**
1	Strongly agree	Very important	Very good	Always	Definitely	Very fast	Very high
2	Agree	Important	Good	Frequently	Most probably	Fast	High
3	Neutral	Moderately important	Barely acceptable	Sometimes	Probably	Moderately fast	Normal
4	Disagree	Of little importance	Poor	Rarely	Possibly	Slow	Low
5	Strongly disagree	Not important	Very good	Never	Probably not	Very slow	Very low
6					Most probably not		

Table C.1: Likert scale for preliminary payment survey

- **How relevant is this work to your community (scale category is B in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

- **How will you rate the performance/speed (scale category is F in Table C.1) ?**
  □ 1 □ 2 □ 3 □ 4 □ 5 □ 6

This part of the questionnaire concerns the mode of money transfer. We consider home to mean your rural household.

- **Average amount (ZAR)?** □ < 100 □ < 250 □ < 500 □ < 1000 □ >= 1000

- **Medium of sending money home?** □ Bank □ People □ Post Office □ Retail Shops □ Wizzit □ MTN banking □ Other (if other specify) ________________

- **Medium of receiving from money home?** □ Bank □ People □ Post Office □ Retail Shops □ Wizzit □ MTN banking □ Other (if other specify) ________________

Thank you for taken some time to participate in this survey and for completing this questionnaire. It is greatly appreciated.

Appendix D

User study I

	Measured values	**Use Likert scale C.1**						
#		Category	1	2	3	4	5	6
1	**Perceived convenience in automatic mode**	A						
2	**Perceived convenience in light confirmation mode**	A						
3	**Perceived convenience in strong authentication mode**	A						
4	**Anxiety over security in automatic mode**	G						
5	**Anxiety over security in light confirmation mode**	G						
6	**Anxiety over security in strong authentication mode**	G						
7	**Anxiety over reliability in automatic mode**	G						
8	**Anxiety over reliability in light confirmation mode**	G						
9	**Anxiety over reliability in strong authentication mode**	G						
10	**Anxiety over privacy in automatic mode**	G						
11	**Anxiety over privacy in light confirmation mode**	G						
12	**Anxiety over privacy in strong authentication mode**	G						

TABLE D.1: NFCpayme survey I: perceived convenience, anxiety over security, anxiety over reliability and anxiety over privacy

Usability requirement predictable performance											
	Please make a tick $\|\|\surd\|\|$ in front of your choice										
cash and change		$<= 5sec$		$<= 10sec$		$<= 20sec$		$<= 30sec$		$> 30sec$	
cash and no change		$<= 5sec$		$<= 10sec$		$<= 20sec$		$<= 30sec$		$> 30sec$	
NFCme2u and change		$<= 5sec$		$<= 10sec$		$<= 20sec$		$<= 30sec$		$> 30sec$	
NFCme2u and change		$<= 5sec$		$<= 10sec$		$<= 20sec$		$<= 30sec$		$> 30sec$	
NFCme2u and request		$<= 5sec$		$<= 10sec$		$<= 20sec$		$<= 30sec$		$> 30sec$	

TABLE D.2: NFCme2u survey I: predictable performance

	Ease of use with minimal training										Fast to use (# of errors)					
Please make a tick $\Vert\surd\Vert$ in front of your choice, refer to scale category table C.1																
	Category	1	**2**	**3**	**4**	**5**					**Category**	1	**2**	**3**	**4**	**5**
cash and change	**A**										**A**					
cash and no change	**A**										**A**					
NFCme2u and change	**A**										**A**					
NFCme2u and no change	**A**										**A**					
NFCme2u and request	**A**										**A**					
Ease to learn											Perceived accuracy (Confidence)					
Please make a tick $\Vert\surd\Vert$ in front of your choice, refer to scale category table C.1																
	Category	1	**2**	**3**	**4**	**5**					**Category**	1	**2**	**3**	**4**	**5**
cash and change	**A**										**A**					
cash and no change	**A**										**A**					
NFCme2u and change	**A**										**A**					
NFCme2u and no change	**A**										**A**					
NFCme2u and request	**A**										**A**					

TABLE D.3: NFCme2u survey I: measure ease of use for minimal training, fastness of use, learnability, perceived accuracy (confidence).

			Cash		NFCme2u			
Sample Payment amount	**change received**	**Experiment Code**	**Change**	**No change**	**Change**	**No change**	**request**	**Objective**
R50	N/A	A						**simple cash exchange**
R540	N/A	B						**paying non-trivial amount**
R50	R34.00	C						**collecting simple and small amount**
R540	R217.65	D						**collecting large and harder to calculate payment**

Table D.4: This section of the questionnaire provide for comparison between cash-based and NFCme2u-based experiment for first user study I.

Appendix E

User study II

#	Measure quantity		Please make a tick ‖√‖ in front of your choice					
13	Maximum acceptable amount in automatic mode		<= 100	<= 250	<= 500	<= 1000	<= 5000	> 5000
14	Maximum acceptable amount in light confirmation mode		<= 100	<= 250	<= 500	<= 1000	<= 5000	> 5000
15	Maximum acceptable amount in strong authentication mode		<= 100	<= 250	<= 500	<= 1000	<= 5000	> 5000
16	Completion time in automatic mode		<= 10sec	<= 20sec	<= 30sec	<= 60sec	> 60sec	
17	Completion time in light confirmation mode		<= 10sec	<= 20sec	<= 30sec	<= 60sec	> 60sec	
18	Completion time in strong authentication mode		<= 10sec	<= 20sec	<= 30sec	<= 60sec	> 60sec	

Table E.1: NFCpayme survey I: maximum acceptable amount and completion time

		NFC mpayment			
	To what extent can NFCpayme reduce users' payment transaction costs?				
		Most			Least
		Please fill in your rank order: 1 for most convenient and 3 for least convenient			
1		Automatic	Light confirmation		Strong authentication
		Please fill in your rank order: 1 for most anxious and 3 for least anxious			
2		Automatic	Light confirmation		Strong authentication

Table E.2: NFCpayme: rank convenience and anxiety

	NFC mpayment			
	Can gains in transaction speed and convenience offset the associated increase in perceived risk?			
	Where perceived risk = Function(Amount of money involved)			
		Most		Least
		Please fill in your rank order : 1 for most amount willing to pay and 3 for least		
3		Automatic	Light confirmation	Strong authentication

Table E.3: NFCpayme: rank maximum transaction size

Evaluating choices	
Enter yes (y) if feature is available and no (n) if not	**y or n**
tells where you are in the transaction?	
how much need to be done?	
users current balance on the screen?	
requires explicitly confirm full details of payment (payee & amount)?	
displays transaction summary screen after transaction to show	
current transaction cash balance?	
expected post transaction cash balance?	
details of how much amount you have?	
details to fully understand financial implications?	
allows easy recovery from errors?	

Table E.4: Evaluating features for NFCme2u I

Evaluation: features and choices		
Touch protocol	1	Two-touch
	2	Single-touch
Type of authentication	1	re-authentication at each stage
	2	Single or one-time
Payment acceptance request options	1	Always
	2	Confirm first
	3	Never
Annotating receipts	1	Text area
	2	Drop down list
	3	Combo box

Table E.5: Evaluating choices for NFCme2u II

		Frustration	**Effort**	**Temporary demand**	**Physical demand**	**Performance**	**Mental demand**
Cash	**change**	**q51**	**q56**	**q59**	**q63**	**q67**	**q71**
	no change	**q52**	**q57**	**q60**	**q64**	**q68**	**q72**
NFCme2u	**change**	**q53**	**q58**	**q61**	**q65**	**q69**	**q73**
	no change	**q54**	**q59**	**q62**	**q66**	**q70**	**q74**

Table E.6: This section of the questionnaire provide for cognitive load test on NFCme2u.

			Base					Time pressure					
			cash		NFCme2u			cash		NFCme2u			
Payment amount	change received	Experiment Code	Change	No change	Change	No change	request	Change	No change	Change	No change	request	Objective
R50	**N/A**	**A**	q75	q76	q77	q78	q79	q80	q81	q82	q83	q84	**simple cash exchange**
R436.75	**N/A**	**B**	**q85**	q86	**q87**	q88	q89	q90	q91	q92	q93	q94	**paying non-trivial amount**
R50	**R34.00**	**C**	**q95**	q96	**q97**	q98	q99	q100	q101	q102	q103	q104	**collecting simple and small amount**
R575.60	**R217.65**	**D**	**q105**	q106	**q107**	q108	q109	q110	**q111**	q112	**q113**	q114	**collecting large and harder to calculate payment**

Table E.7: Experiment for cognitive test: cash vs NFCme2u
Four experiments are done for both cash and NFCme2u experiments: A,B,C, and D in user study II.

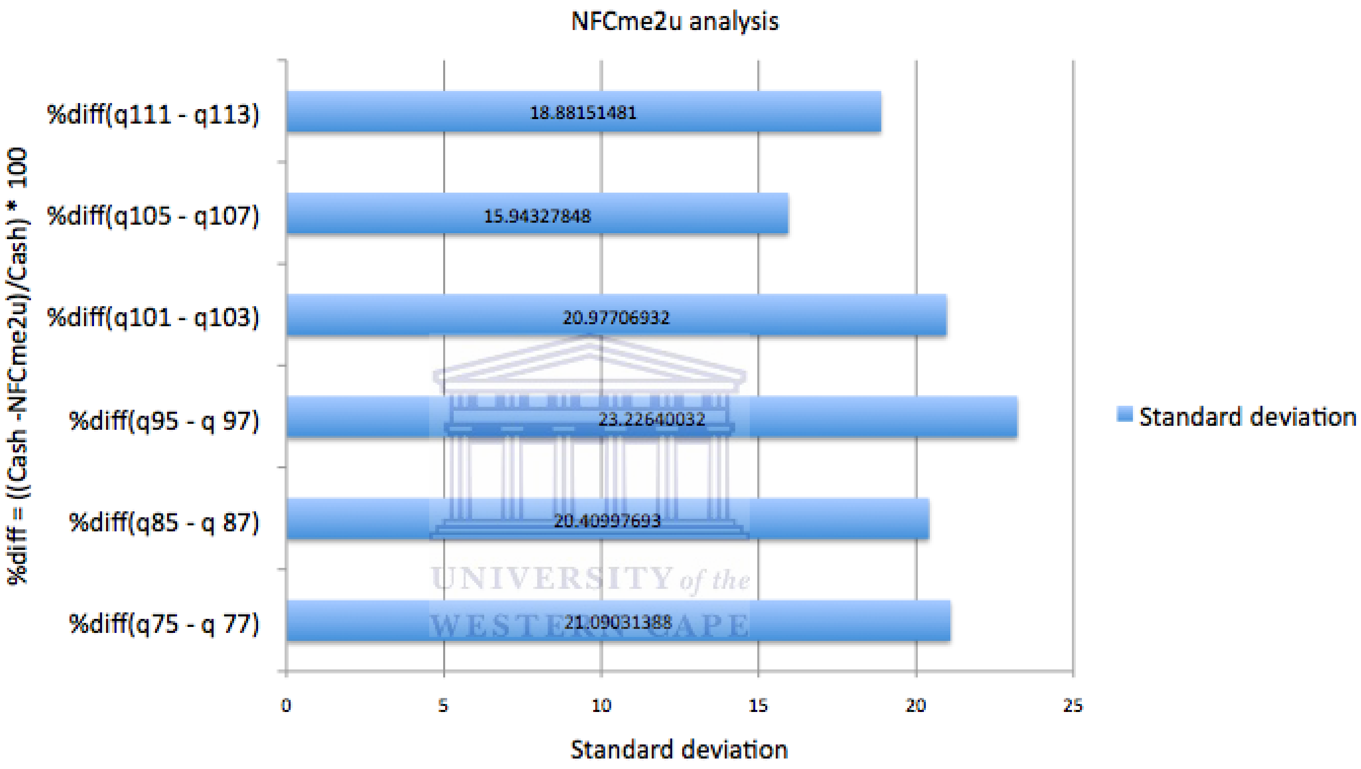


Figure E.1 **Standard deviation obtained from NFCme2u analysis**
This is possible by transforming the data via eliminating the outliers so that we obtain a normally distributed data and in turn, we can obtain the standard deviation. This diagram illustrates a bar graph that shows the
$\%diff = ((Cash - NFCme2u)/Cash) * 100$
for each of q75 to q77, q85 to q87, q95 to q97, q101 to q103, q105 to q107, and q111 to q113 to be known. Refer to Table E.7