Cellphone banking at the bottom of the pyramid

A THESIS PRESENTED IN PARTIAL FULFILMENT

OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

AT THE UNIVERSITY OF STELLENBOSCH

By

P.J.H. Kruger

December 2011

Supervised by: Prof. Willem Visser

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

March 2012

Summary

This thesis investigate the different available GSM bearer channels that can be used to launch a cellphone banking application. Specific attention is given to launch such a cellphone banking application to the so called "bottom of the pyramid". In South Africa, there are an estimate 11 to 13 million people with no bank accounts. The cellphone create an ideal opportunity to be used as a tool to reach this untapped market segment that today mainly uses cash to pay for day to day living expenses.

The thesis provide more information on the cellphone banking arena in South Africa as well as certain projects in other parts of the world. The thesis also highlight new developments on cellphone technology that include Android and IPhone delivery channels.

Focus is placed on how the cellphone banking presentation layer must be delivered through the USSD GSM bearer channel. USSD is at the current moment the ultimate channel to consider due to its extensive reach and ability to work on any GSM cellphone handset.

In conclusion, although cellphone banking can be used by any person, the benefit to bring financial services to the bottom end of the pyramid must be considered to achieve financial inclusion. The cellphone due to its reach is the ideal medium to access this lower end market.

Afrikaans summary

Hierdie tesis ondersoek beskikbare GSM selfoon kanale wat gebruik kan word om 'n selfoon bankdienste toepassing te initieer. Spesifieke aandag word gegee om so 'n selfoon bankdienste toepassing uit te rol na die sogenaamde onderste gedeelte van die bevolkings piramiede.

Die tesis verskaf meer informasie oor die selfoon bankdienste arena in Suid Africa maar dit brei ook ooit oor sekere soortgelyke projekte in ander dele van die wereld. Die tesis lig ook nuwe ontwikkelings uit in selfoon tegnologie wat Android en IPhone mediums insluit.

Fokus word geplaas op die selfoon bankdienste vertoning deur die USSD GSM kanaal. USSD is huidiglik die beste kanaal om te oorweeg as gevolg van die wydverspreide beskikbaarheid omdat die tegnologie op enige selfoon handstuk werk.

Die uiteindelike gevolgtrekking uit die werkstuk is dat selfoon bankdienste deur enige persoon gebruik kan word, maar selfoon bankdienste is 'n goeie idee om te oorweeg om mense in te sluit uit die onderste gedeelte van die bevolkings piramiede. Die selfoon kan dus as 'n ideale medium gebruik word om hierdie mense te betrek by finansiele dienste.

Acknowledgements

I would like to thank...

- my heavenly Father,
- my supervisor Prof. Willem Visser for his assistance and support to produce this work,
- my wife who supported me during this process,
- my parents for their support,
- my employer WIZZIT, that provided me the opportunity to gain experience in the field of cellphone banking technology.

Contents

1 Introduction **5**

2 Cellphone banking considerations **13**

2.1 Security 14

2.1.1 Application security in cellphone banking product 14

2.1.2 Security Zones in a cellphone banking solution 16

2.2 Usability of the cellphone banking application 19

2.3 Cellphone banking application support and maintenance 21

2.4 Channel customer reach 22

3 Available GSM channels for cellphone banking **24**

3.1 Introduction 24

3.2 Voice channel 26

3.3 Short Message Service channel 28

3.4 SIM Toolkit Application channel 33

3.5 Wireless Application Protocol channel 36

3.6 J2ME application channel 41
3.7 USSD channel 45
3.8 Android Apps 52
3.9 Apple iPhone and iPad Apps 54
3.10 BlackBerry Apps 55
3.11 Comparison of the GSM channels for cellphone banking 56

4 Presentation layer used in WIZZIT 65

4.1 Background 65
4.2 The USSD customer interface 66
4.3 WIZZIT USSD Short codes 68
4.4 Enhancement of security through cellphone banking PIN 69
4.5 Different language support through the cellphone banking frontend . . . 70
4.6 Introduction of new bearer channels like WAP and JAVA 71
4.7 Conclusion of the WIZZIT approach 72

5 Different types of cellphone banking approaches 73

5.1 Introduction 73
5.2 Bank led model 75
5.3 Mobile Network Operator led model 75
5.4 Combination of a bank and mobile network operator led model 76
5.5 Summary 76

6 Cellphone banking arena **79**

6.1 History of cellphone banking in South Africa 79

6.2 A new era for cellphone banking in South Africa 82

6.2.1 WIZZIT banking the unbanked 82

6.2.2 FNB Cellphone Banking 83

6.2.3 MTN Mobile Money 84

6.2.4 Nedbank 85

6.2.5 Standard Bank 85

6.2.6 ABSA 85

6.3 Cellphone banking offerings in other parts of the World 86

6.3.1 Philippines G-Cash and SmartMoney 86

6.3.2 M-PESA 87

6.3.3 ZANACO XAPIT solution Zambia 88

6.3.4 NMB Mobile Tanzania 89

6.3.5 Google Wallet 90

6.3.6 Summary 91

7 Conclusion **92**

Bibliography **96**

List of Figures

1.1 The economic pyramid of the world according to Prahalad [58] 6

1.2 Cellphone subscribers in South Africa 2009 [12] 9

2.1 Security zones of cellphone banking application 16

3.1 SIM Toolkit Application interaction with a cellular handset [30] 33

3.2 The WAP Programming model [29] 37

3.3 USSD Menu for a mobile network operator customer support 49

3.4 Example of a USSD airtime credit instruction from a prepaid subscriber phone 50

3.5 Comparison of available GSM channels 58

4.1 The WIZZIT USSD cellphone banking menu 67

4.2 Defining a WIZZIT short code as a phone book entry 69

4.3 Support for different languages on WIZZIT Menu 71

Acronyms

1G First Generation [81]. 38

2G Second Generation [105]. 33, 38

3G Third Generation [115]. 21, 38

3GPP 3rd Generation Partnership Project [114]. 33

4G Fourth Generation [82]. 38

API Application Programming Interface [73]. 17, 43

ATM Automatic Teller Machine [13]. 65, 66, 79, 83, 86, 89, 90, 94

BES BlackBerry Enterprise Server [74]. 55

BIS BlackBerry Internet Service [74]. 55, 56, 63

CDC Connected Device Configuration [78]. 41, 42

CLDC Connected Limited Device Configuration [79]. 41, 42

CPU Central Processing Unit [77]. 36

GPRS General Packet Radio Service [83]. 25, 43, 54, 71, 81, 82

GPS Global Positioning System [84]. 92

GSM Global System for Mobile Communications [35]. 10, 11, 13, 14, 17–23, 25–29, 31, 33, 45–48, 52, 54, 56–61, 71–73, 78, 80, 81, 83, 88, 89, 91–93

HLR Home Location Register [62]. 17, 18, 45

HTML HyperText Markup Language [85]. 36, 41, 79

IDE Integrated Development Environment [87]. 42

IN Intelligent Network [88]. 46, 50

IVR Interactive Voice Response [89]. 26–28, 60

J2ME Java Mobile Edition [94]. 22, 25, 41–45, 61, 64, 71, 74, 89

LTE Long Term Evolution [97]. 38

MIDP Mobile Information Device Profile [98]. 41, 42

MO Mobile Originating. 29

MSC Mobile Services Switching Center [131]. 18

MSISDN Mobile Station Integrated Services Digital Network or cellphone number [99]. 15, 16, 37, 40, 41, 44, 46

MT Mobile Terminating. 29, 31

NFC Near Field Communications [100]. 77, 90, 91

OTA Over the Air [102]. 34, 36, 81

PIN Personal Identification Number [103]. 14, 15, 27, 30, 32, 36, 40, 49, 60, 68–70

RIM Research In Motion [60]. 55, 56, 63

SATSA Security and Trust Services API [52]. 43

SIM Subscriber Identification Module [110]. 8–10, 14, 16–18, 21, 22, 25, 26, 33–36, 40, 44, 50, 57–59, 74, 81, 84, 87

SMPP Short Message Peer to Peer Protocol [107]. 29

SMS Short Message Service [108]. 9, 15, 22, 25, 28–32, 34–36, 39, 42, 43, 45, 51, 57, 59, 60, 63, 73, 74, 81–86

SMSC Short Message Service Center [109]. 30

SS7 Signalling System 7 [67]. 17, 47, 48

SSL Secure Socket Layer [106]. 17, 39, 59, 93

STK SIM Tool Kit [111]. 21, 25, 33–36, 45, 57–59, 63, 74, 81, 86, 87, 92

TCP/IP Transmission Control Protocol and Internet Protocol [113]. 17

URL Universal Resource Locator [117]. 42, 79

USAT USIM Application Toolkit [119]. 33

USSD Unstructured Supplementary Services Data [118]. 11, 12, 21–23, 28, 35, 43, 45–52, 57, 58, 61, 63, 65–69, 71, 72, 74, 82, 83, 85, 86, 88–91, 93

VPN Virtual Private Network [121]. 17, 48

WAE Wireless Application Environment [124]. 37

WAP Wireless Application Protocol [124]. 21–25, 36–41, 45, 59, 71, 74, 81, 85, 86, 89, 92

WASP Wireless Application Service Provider [125]. 50

WIG Wireless Internet Gateway [132]. 24, 87

WML Wireless Markup Language [126]. 36, 37, 41

XHTML MP Hypertextual computer language standard designed specifically for mobile phones [129]. 36, 37

Chapter 1

Introduction

The current world population is estimated at around 7 billion people, of which approximately 4 billion survive on a daily income of less than US$2. According to Prahalad these 4 billion people represent the "Bottom of the Pyramid" [58]. The economic pyramid of the world is shown in figure 1.1 and the "Bottom of the Pyramid" is indicated as Tier 5.

Contrary to the popular view, that people are not technologically connected at the Bottom of the Pyramid, mobile network operator statistics indicate huge numbers of subscribers in this customer segment as these bottom end users communicate regularly through their cellphones. The extensive reach of the cellphone to these communities make it an ideal channel to deliver financial services to this market in the form of cellphone banking. According to Richardson from WIZZIT [127] in South Africa, cellphone banking provides an opportunity to take banking to the people, instead of bringing the people to the bank [31].

South Africa has a population of approximately 50 million people, with an estimated 60 percent older than 16 years making use of conventional banks as a financial medium [2]. A total of 10 percent of the population older than 16 years of age is banked informally and 26 percent of this population is not related to any financial institution [27]. Due

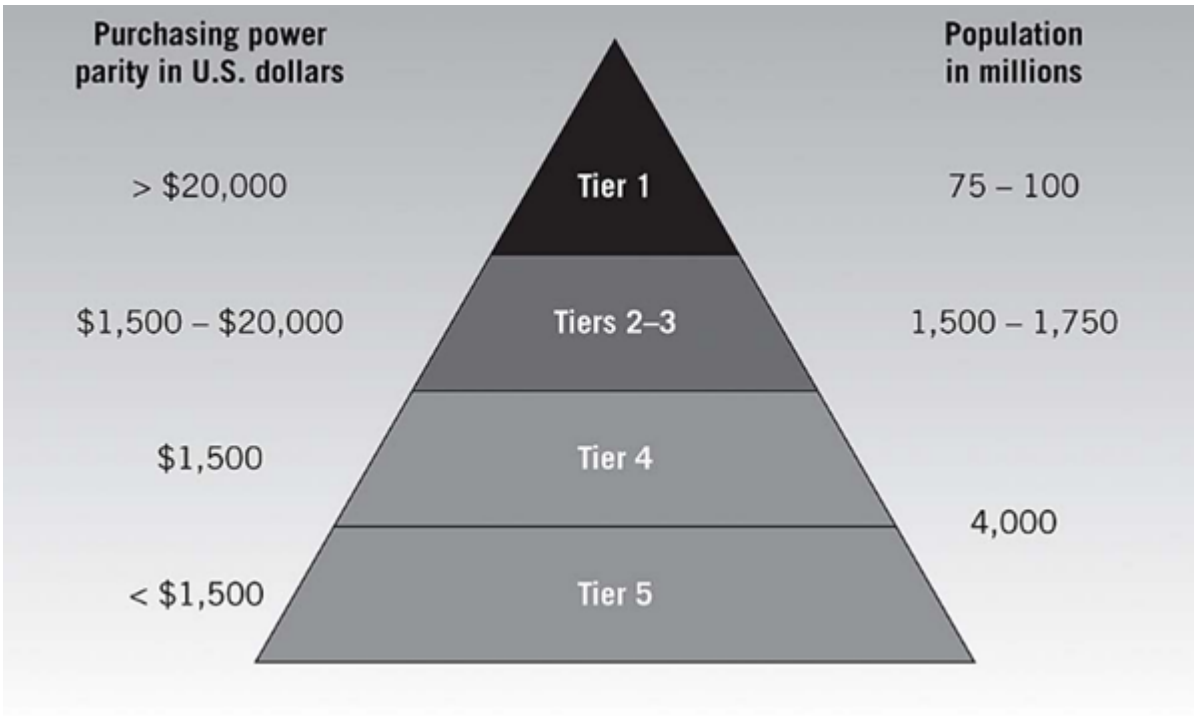

Figure 1.1: The economic pyramid of the world according to Prahalad [58]

to South Africa's history as a country of divides the traditional banks only targeted the middle and higher income classes of society in their attempts to lure clients. According to Pravesh Mahadeo, general manager of ABSA's self-service channel, an estimated 17.5 million people in South Africa is still classified as unbanked or under banked citizens, meaning that banks are not reaping the full market content of this segment [39].

To understand the context of being unbanked and under banked to its full extend it is important to define the context of each. A person is classified as unbanked when they do not have a bank account at all and rather save all available money in a safe place at home, usually under the proverbial mattress [6]. An under banked person is classified as a lower salaried person that receives a salary income into a bank account monthly and immediately withdraw all money to procure or sustain his living expenses such as food, transport or rent. In the example of the under banked individual, a bank account just acts as a more convenient way for the employer to pay salaries or wages without having

the risk of transporting large sums of cash, but actually holds no benefit to the under banked individual.

In a real life situation, during 2002, a student from a higher income household in South Africa enrolled for studies at one of the metro pole universities away from home, and experienced a cumbersome and lengthy process to open a bank account in order to receive his monthly allowance. This very difficult process was highlighted to his parents and at a later stage resulted in discussions between associates, Rowlinson and Ramaphosa. Their conclusion was that the complex process to open a bank account in South Africa is a barrier for entry into the formal banking sector for the so called unbanked and under banked South African population and that an alternative method must be considered to bring financial services closer to this segment of the South African population. Ramaphosa made an important statement during this discussion: "Provide a person with a bank account and you make that person an economic citizen of society".

The three founders of WIZZIT in South Africa, Rowlinson, Ramaphosa and Richardson debated in 2002 existing criteria and conditions for opening a bank account at length and decided to investigate the sustainability and feasibility for creating a banking product that would provide an opportunity to bank the unbanked and under banked population of South Africa. Such a product required an easy to use user interface and had to be understandable to the target market. The unbanked market is only used to live with cash as it is the predominant acceptance medium to pay for goods and services in the informal market. In this market segment, cash is also perceived as free from any cost as the target market does not recognise the cost and risk associated with the distribution and acceptance of cash at informal traders. This newly planned banking product had to support these requirements from the target market in order to support the need and relevance for such a product.

Original investigations by WIZZIT explored a smart card wallet solution that could facilitate cheap transactions for the end customer. However the acquiring costs of the physical smart cards as well as the capital layout for smart card acceptance devices were

too substantial at the time to warrant the drafting of a feasible business plan.

A common dominating connection amongst the target group of unbanked people was not revealed until further investigations and market research indicated that the majority of the target market had one common user reliance device in the form of their cellphones. They all knew how to make use of the various functions on the cellphone and used it extensively, irrespective of their disposable income bracket. As a recognised communication medium and a technological advanced device of the 20th century, cellphones are ever advancing and could be adapted to suite certain special market needs. The extensive reach on cellphones in the target market of unbanked people in South Africa was driven by innovative projects by the South African Mobile Network Operators. For example, Vodacom in South Africa was the first mobile network in the world to offer pay-as-you-use phone access to customers that could not afford expensive cellphone contracts allowing deep access into the rural unbanked areas of South Africa [3].

WIZZIT seized the opportunity to utilise the cellphone as a delivery channel for banking services to reach to the unbanked market in South Africa. The advantage of this approach was the fact that most of the end users already had access to a cellphone device and was familiar with the usages of these devices. WIZZIT aimed to deliver a banking service on the physical cellphone handset that was easily accessible and affordable to the end customer. This new concept of reaching out to the unbanked to provide them with a banking product through cellphone technology was first introduced to the South African market by WIZZIT in November 2004 [21].

One needs to take cognisance of the fact that cellphone banking was not a new concept to the South African market at the time. In fact some of the major banks in South Africa already launched cellphone banking services in the late 1990's and early 2000's to the more sophisticated banked customers, but not to the unbanked market. These services were offered in partnership with the local mobile network operators in South Africa, with a small banking application that had to be loaded on the Subscriber Identification Module [110] (SIM) card of the customer cellphone to provide access to this service. The

SIM based cellphone banking application communicated with the bank through secured Short Message Service [108] (SMS) messages. The commercial banks had very limited success in the cellphone banking uptake by the more educated portion of the population that already held a bank account. This limited response in uptake of cellphone banking by the educated population led the banks to rather focus on user friendly computer based internet banking applications that allowed these customers to have access to their bank accounts from the convenience of their workplace or home through the World Wide Web.

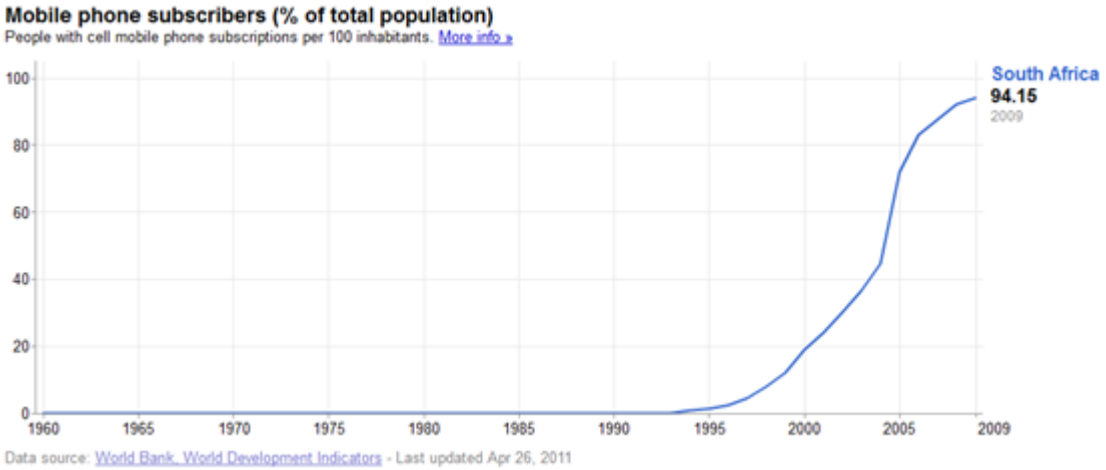

Figure 1.2: Cellphone subscribers in South Africa 2009 [12]

The World Bank estimated that South Africa had a 94% cellphone penetration rate in 2009 (see Figure 1.2) [12]. Today South Africa has a 100% penetration level in cellphone reach [45]. Cellphone penetration and usage is very high amongst the poorer levels of the population due to the availability of prepaid cellphone services. The high level of extensive cellphone usage by the unbanked and under banked segments of the market made it the ideal medium to be used as a channel to deliver banking services to this target group.

The focus area of this thesis will be on the technical approach and aspects that were followed by WIZZIT bank in South Africa to rollout a cellphone banking product that successfully reached the unbanked population of this country. Although the social aspect of WIZZIT has a great story to tell about changing lives, the thesis will not focus on any

of the sociological aspects.

The architect of the technical solution had to design and implement technology that would deliver a cellphone banking product to the unbanked. The task was to find a cellphone banking solution that would integrate with any cellphone device operated through any mobile network operator in South Africa, with limited or no interaction required from WIZZIT or the mobile network operators to upload the cellphone banking application on the customer cellphone. The installation and delivery of the cellphone banking application to the customer cellphone had to take place over the relevant Global System for Mobile Communications [35] (GSM) network channels. To find the ideal solution, consideration was given to the various GSM delivery channels that were available at that point in time to launch a successful cellphone banking application. The following GSM cellphone bearer channels existed in South Africa in 2004 and it formed part of the evaluation for the WIZZIT solution:

1. IVR — Interactive Voice Response [89]
2. SMS – Short Message Service [108]
3. STK – SIM Toolkit Application [111]
4. WAP – Wireless Application Protocol [124]
5. J2ME – Java mobile phone solutions [94]
6. USSD – Unstructured Supplementary Services Data [118]

The challenge was to select a cellphone delivery channel from the available bearer channels listed above that could reach a large section of the target market.

Four main points were taken into consideration to evaluate each GSM delivery channel:

1. The channel must be secure enough to deliver financial transactions.

2. The channel had to be easy to use from a customer perspective to contribute to the usability of the solution.

3. The deployment and maintenance effort that will be involved to support the cellphone banking application needs to be considered.

4. The cellphone banking application had to be able to work on any generation of cellphone models available in South Africa to assist with the customer reach of the solution.

Investigation and research activities conducted with user groups at WIZZIT exposed a generally available GSM channel called the Unstructured Supplementary Services Data [118] (USSD) bearer channel. The USSD bearer channel is a session based, text menu driven channel that is accessible on all GSM enabled cellphones [68]. WIZZIT's research at the time in 2004 indicated that USSD was the best bearer channel to deliver the cellphone banking service successfully to the targeted and unbanked market in South Africa. WIZZIT launched their pilot USSD cellphone banking channel in November 2004. This event was history in the making as it was the first time ever that the USSD bearer was used as a cellphone banking channel to reach the unbanked population in a country. In chapter 3 of the thesis, more information will be provided on the characteristics of USSD.

After the launch of the WIZZIT USSD cellphone banking application, various other banks in South Africa followed with the launch of similar USSD cellphone banking applications and today the main banks all have a USSD cellphone banking channel available. The utilisation of the USSD delivery channel as a cellphone banking delivery channel has also extend beyond the borders of South Africa and has become a relevant channel to consider when a cellphone banking application is introduced. In chapter 6 different cellphone banking initiatives are discussed elaborating on the technology utilised and the results in the various markets.

Cellphone banking and cellphone payments have become a very important area in bringing financial services to the poor. According to Mr Mohsen Khalil, Director, Global ICT The World Bank Group, there are more than 3 billion cellular phones in the world and this is most probably the largest distribution network and platform to most effectively provide social and economic services to the poor [31]. There were various pilots on cellphone banking and cellphone payments around the world of which Smart Money and G-Cash in the Philippines, WIZZIT in South Africa, M-Pesa in Kenya and WING in Cambodia are probably best known. Cellphone banking and cellphone payments make a lot of sense in countries where card acquiring infrastructure is not present. Africa as a continent is an ideal place for innovation around cellphone banking and cellphone payments due to wide spread geographic concentrations of people and this initiative can leap frog card payments. This is also applicable to countries in South America and Asia. According to Mr. John Staley, Director mobile banking and payments of Equity Bank Kenya, banking simply implies payments for customers and it is important that this is done in the most convenient way. It must be just as easy as using cash for payments [24].

The author is of the opinion that cellphone banking is still in early stages of development and as it matures, the focus will change more to cellphone payments also known as mobile commerce. There are a number of mobile commerce initiatives around the world that is based on Near Field Communication (NFC) integrated chips that are mounted on cellphones. The approach with NFC is that sophisticated card acquiring infrastructure must be in place to accept these types of cellphone payments. The African continent lack proper card acquiring infrastructure and alternative ways of accepting cellphone payments must be considered. A great success story around cellphone payments and acceptance is M-Pesa [37] in Kenya that has a participating merchant network of more than 30 000 merchants that all will accept cellphone payments.

In the next sections of the thesis, the author will provide more background on the approach that was followed to select and implement the USSD cellphone banking solution to the unbanked market in South Africa.

Chapter 2

Cellphone banking considerations

This chapter of the thesis will provide more detail on options that needs consideration when launching a cellphone banking application. Four areas will be covered as considerations:

- Security of the solution.
- Usability of the cellphone banking application.
- Maintenance effort that will be involved after the application has been launched.
- Channel customer reach.

In Chapter 3, a comparison is made between the different GSM channels that are available from a security, usability, maintenance and customer reach perspective together with the approach that was followed by WIZZIT in South Africa.

2.1 Security

2.1.1 Application security in cellphone banking product

The main purpose of a cellphone banking application is to provide customers with access to their bank accounts through their cellular phones. In order to comply with acceptable industry standards for access into a bank account, the first item to consider is the successful authentication of the customer. Once authentication is done, the information that is transported between the bank and the customer's cellular phone needs to be encrypted to eliminate interception by non-authenticated parties.

The security approach in a cellphone banking application is crucial, because the customer will use the cellphone to access his bank account remotely by utilising the network reach of his GSM mobile network operator. The cellphone banking application will allow the customer to view balances in accounts and to transfer money from his account to any other bank account, it is of the utmost importance that the cellphone banking application enforce that each transaction can only be executed by the owner of the bank account.

Application security in a cellphone banking application must assure non-repudiation [101] of transactions. This implies that there must always be proof that the originator of the transaction was uniquely authenticated before the transaction was processed on the bank account. To assist with proper authentication it is recommended that the approved technology always use a Two-factor authentication mechanism [116] of "something you have" (your cellphone) and "something you know" (your cellphone banking Personal Identification Number [103] (PIN)) [28]. To comply with the first factor of authentication which is "something you have", it is recommended that the application is designed to ensure that the mobile handset or unique SIM card is always linked to the customer profile during the registration process in the cellphone banking platform. This approach will limit the customer to only access the cellphone banking application from his own handset and it will eliminate fraudulent spoofing attempts from any available handset

making it more difficult for fraudsters to compromise the security of the application.

The second portion of the two factor authentication mechanism is a unique PIN that is selected by the customer during the registration process. PIN selection is important to assure that the customer's identity is not comprised. It is recommended that customers select unique cellphone banking PIN codes, while the application must be designed to not allow weak PIN combinations that follow patterns like "1111", "1234", "9876".

According to security audit best practices regarding a PIN code, the customer must be forced to change his cellphone banking PIN on a regular basis. This is embraced from a security perspective but experience has shown that people tend to have one PIN for multiple applications. For example customers select the same PIN for their bank card as well as for the cellphone banking PIN. Our experience in different countries proved that if you continuously force customers to select a new PIN after a certain period of time has elapsed, customers will become resistant and negative about the product and could even stop using both the card and cellphone banking product.

To assure security even further, it is recommended that all transactions with financial impact is notified to the customer through an alert service. The advantage of a cellphone banking application is the fact that the bank will always have the Mobile Station Integrated Services Digital Network or cellphone number [99] (MSISDN) of the customer and it allows the sending of transaction notifications immediately to the customers at the time of the transaction through an SMS alert service.

To support the security of a cellphone banking solution, it is good practice to introduce associated daily limits for the transaction types that will be delivered by the solution. The introduction of daily limits combined with transaction notifications that will notify the customer of fraudulent activity will make cellphone banking less vulnerable for attacks and mitigate the potential fraud risk. It is in the discretion of the bank to determine the value of these limits but the rule of thumb is that it needs to be small enough amounts that discourage fraudsters in attempting to bridge the security of the solution.

As part of the security of a cellphone banking solution, a bank will have to evaluate the ease of use of end to end encrypted channels compared to more easily accessible channels with less security in place. The author is of the opinion that the target market for the cellphone banking application will determine the security measures of the solution and further chapters will illustrate this opinion.

2.1.2 Security Zones in a cellphone banking solution

To have a better understanding of the different operations of the various cellular delivery channels, it will be a good approach to divide the flow and delivery of each cellphone banking message in 3 different zones as indicated by Figure 2.1 below. The 3 zones as illustrated in Figure 2.1 will be used to transport the message content of a cellphone banking transaction between the customer handset and the cellphone banking application server at the bank.

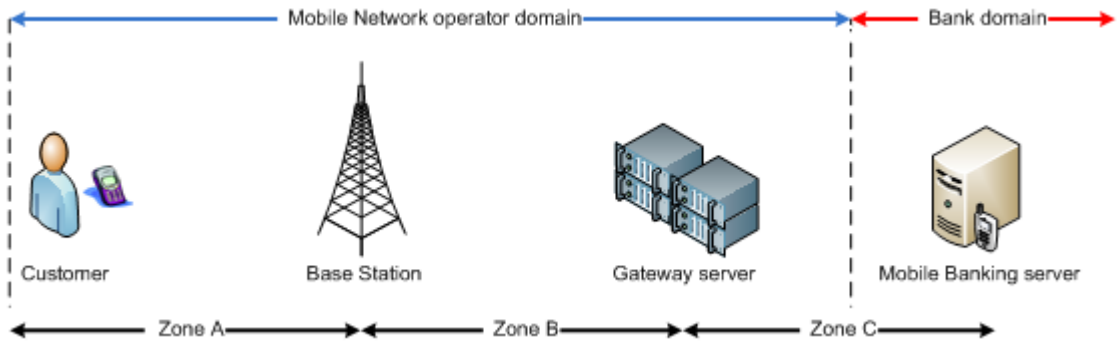

Figure 2.1: Security zones of cellphone banking application

Zone A displays the interaction between the customer handset and the base station in its proximity. In Zone A, the customer handset has a unique Subscriber Identity Module or SIM card that stores the MSISDN or cellphone number of the subscriber as well as the International Mobile Subscriber Identity shortly called the IMSI [90] that provision the customer in the Mobile Network.

Zone B indicates the transportation of the messages from the mobile network operator

base station to the appropriate gateway server inside the mobile network. Zone A and Zone B is implemented on the GSM Signalling System 7 [67] (SS7) protocol that supports encryption of the message content from the mobile hand set to the gateway server.

Zone C (Figure 2.1) is the network layer between the mobile network operator and the bank that delivers a cellphone banking solution. The implementation of this layer might vary between installations depending on the infrastructure that is available. The cellphone banking message content transported over the GSM network SS7 protocol will be converted at the mobile network operator in the gateway server to a Transmission Control Protocol and Internet Protocol [113] (TCP/IP) format that is more a generalised protocol to be used between application servers. Connectivity between the mobile network operator gateway server and the bank's applications server is implemented through relevant Application Programming Interface [73] (API) like JAVA servlets [95] or Web services [123]. The mobile network operator will supply to the bank the relevant API documents so that the bank can build the interface into the gateway servers at the mobile network. To secure communication over Zone C, it is recommended that a dedicated digital link is installed between the mobile network operator and the participating bank that supports Virtual Private Network [121] (VPN) technology. The implementation of a Secure Socket Layer [106] (SSL) connection that enforces at least 128 bit encryption between the gateway server at the mobile network operator and the cellphone banking server at the bank is recommended.

GSM cellular networks implement encryption for three reasons [34]:

- Authentication: The authentication algorithm implemented in GSM networks is known as the A3 algorithm [133]. The task of the algorithm is to generate the 32-bit signed response (SRES) utilizing the 128-bit random challenge (RAND) generated by the home Home Location Register [62] (HLR) and the 128-bit individual subscriber authentication key (Ki) from the customer SIM or the HLR. The A3 algorithm is implemented inside the SIM card of the customer.

- Encryption: The encryption algorithm used in GSM networks is a stream cipher known as the A5 Algorithm [134]. The stream cipher is initialised with the Session Key (Kc) and the number of each frame. The same Session Key is used throughout a specific call or service, but the 22-bit frame number changes during the call, generating a unique key stream for every frame. The same Session Key (Kc) may be used on more than one occasion until the Mobile Services Switching Center [131] (MSC) does a new authentication. The A5 algorithm is implemented inside the subscriber mobile handset.

- Key generation: The key generation algorithm implemented in GSM networks is known as the A8 Algorithm [135]. The A8 algorithm's task is to generate the 64-bit Session Key (Kc), from the 128-bit random challenge (RAND) received from the MSC and from the 128-bit individual Subscriber Authentication Key (Ki) received from the SIM or the HLR. The A8 Algorithm is implemented in the SIM card.

Although known attempts exist for attacks on the above GSM encryption standard, the general assumption is made that the mobile operators will implement the described algorithms as explained above, with the strongest key pairs possible to eliminate attacks to the GSM network.

In summary, figure 2.1 indicates the relevant security zones to consider when launching a cellphone banking application and it is clear from the previous paragraphs that communication can be secured from the customer handset to the server at the bank. Depending on the type of GSM delivery channel that will be used the security in the three zones can be increased or decreased. Unfortunately with increased security, the user experience and ease of use of the cellphone banking application is compromised. Each available GSM delivery channel will be evaluated according to capability in the next chapter, including a security perspective.

With the function of the different security zones in delivering a cellphone banking transaction now described, further investigations surrounding additional requirements to launch

a cellphone banking application can be discussed.

2.2 Usability of the cellphone banking application

Usability encompasses the focus on the ease of use of the cellphone banking application from the end users perspective. According to the website www.useit.com, there are mainly 4 challenges to address with cellphone applications namely [48]:

1. Small screens – small screens means fewer visible options at any given time,
2. Awkward input of information, especially for typing,
3. Download delays – getting the next screen takes forever,
4. Badly designed sites – Websites are typically optimised for desktop usability and don't follow guidelines available for usable mobile access.

Each available GSM network channel available for cellphone banking will be evaluated and compared with the above four points. From this comparison it will be demonstrated why the original launches of cellphone banking applications failed as a result that banks mainly just downscaled their internet banking onto a cellphone banking application. Usability of cellphone banking applications depends on the make and model of handheld phones used. Smartphone devices [112] for example support a much more sophisticated user experience, but because of the limited spread of these devices it only supports a limited reach for a cellphone banking application.

As with any product in the current market, the more user friendly a product is presented the more likely it is to succeed in the modern high speed and simplistic driven economy. Usability of the cellphone banking solution is mainly defined by the GSM presentation layer that will be used on the customer handset. The author is of the opinion that the presentation layer was the main reason for cellphone banking implementations not originally being successful in different market segments.

The following important aspects of the presentation layer were not considered or neglect in earlier cellphone banking implementations:

1. Banks approached cellphone banking as an extension of their existing internet banking offering that was launched to the market during the nineties. It was difficult to complete a transaction on the cellphone because of the limited resources available on the cellphone handset compared to a computer.

2. The size of the cellphone screen display and small numeric key pad made it extremely difficult to use.

3. Internet connectivity on cellphones was very slow.

4. Different cellphone handsets on the market delivered different views and experiences and caused confusion to the end user, making customer support via a customer support center difficult.

In conclusion, the solutions available at the time were not optimized enough for the end device (cellphone handset) that was used to process a cellphone banking transaction.

The recommended approach to a bank would be to launch a cellphone banking product with a bearer channel that will provide a similar experience on handsets available in the target market. To penetrate the selected market segment, it is important to utilize a GSM phone channel that is known to the target market of the bank. If a bank provides a customer with a familiar experience in the cellphone banking application, it will create trust and familiarity around the product.

To conclude, usability of a cellphone banking application is the ease of use with which customers can access the application and similarity in experience independent of the type of cellphone handset that will be used.

2.3 Cellphone banking application support and maintenance

A cellphone banking transaction will be executed from the cellphone handset of a customer. The SIM card inside the cellphone determines the mobile network operator to whom the cellphone subscriber belong too. Since the bank does not own the mobile handset of the customer, they need to work closely with participating mobile network operators to launch the cellphone banking application on their network. Maintenance of the cellphone banking application is the effort that will be required to install a cellphone banking application onto the end user phone, but includes the later effort required to update and enhance the application on the user phone if new versions of the cellphone banking application becomes available.

Some of the delivery channels in GSM networks allow a server residing application where each screen is rendered from an application server hosted at the bank. Good examples of such GSM delivery channels are Wireless Application Protocol [124] (WAP) and USSD. For any maintenance to the application, the changes are applied to the application server at the bank and it becomes immediately available to the customers. The maintenance effort to deploy the application and to make changes later on is a fairly easy process, provided that the correct bearer channels are used. In the case of a server residing solution, introduction of new versions of the application can be introduced easily by upgrading the application on the server and deploying the new version to all clients accessing the server. The down side to this approach is that it requires more data bandwidth from the mobile networks that is currently still limited to high end phones that support Third Generation [115] (3G) data services.

Other delivery channels in the GSM network require that the application is first downloaded and then stored onto the cellphone handset or stored inside the SIM card of the phone. Recognised examples of these types of delivery channels are Java Midlets [93] or SIM Tool Kit [111] (STK) applications. The effort required to download the applications

to the phone is the first consideration and add to the total maintenance effort. Updating the applications in future on the handset or SIM card require also tremendous effort and usually requires changes on the phone itself to be made. The challenge with the client side approach is that it will require the redistribution of new versions of the application to the cellphones if functionality changes in the application or if new features need to be introduced. This implies that application version control needs to be addressed and maintained to ensure that all customers operate on the latest version.

Client– and server–side approaches have advantages and disadvantages to consider in maintaining the cellphone banking application and some banks use both approaches. This dual approach creates a burden for the support center as they have to first determine which channel the customer is accessing and then apply the resolution of the relevant server or client residing application to resolve a problem. In most cases the customer does not know what channel he was using and it can make the support of the application a difficult and lengthy process.

2.4 Channel customer reach

In evaluating the different GSM channels, it is important to consider the reach of such a channel. In other words, how many of the cellphone handsets available in the current market will be able to access the cellphone banking application through the specific GSM channel. Channels like Voice, SMS and USSD are able to function on the oldest and lowest technology enabled cellphone devices in any market. WAP and Java Mobile Edition [94] (J2ME) will only be supported on newer type of cellphones. Android and iPhone applications will only function on either Android or iPhone devices that only arrived recently on the scene.

A cellphone banking application will be successful if it is launched on a GSM channel that is supported by most phones in the target market. In developing countries where mainly older cellphones are available USSD, SMS and Voice has the best potential to

reach most people in a country. In developed markets the tendency is that people will have higher end cellphones and this provide the opportunity for WAP, Android and Apple applications to be successful although technologies like USSD has proven to be also successful because it works on the oldest as well as newest of cellphone devices. Cellphone banking applications has great potential to bring banking closer to people but the correct delivery GSM channels needs to be considered to reach the target market.

The aforementioned paragraphs indicate the major considerations to take into account when launching a cellphone banking application. In the next chapter, the different GSM channels will be analysed based on security, usability, ease of maintenance and customer reach perspective.

Chapter 3

Available GSM channels for cellphone banking

3.1 Introduction

In an effort to find a suitable banking solution for the unbanked population, extensive research into needs and practicality towards the target market were conducted in this unknown field. Original considerations pointed at the issue of a chip based smart card that could be used for payments, but this route was soon eliminated by the high costs of chip based cards. In research conducted with potential user groups at the time, the finding was made that people would consider using their cellphones to do payments and conduct other banking transactions if it was a secure medium. Although this was an interesting outcome to the research, a concern was that all four major banks in South Africa at the time had already launched cellphone banking applications delivered either through Wireless Internet Gateway [132] (WIG) or WAP applications, but the penetration into the more sophisticated market was small and in many cases seen as a failure.

Research indicated that possible causes inhibiting the uptake and acceptance of cellphone

banking products at that time were:

(A) The available memory space on the GSM cellphone SIM cards was only 8 kilobytes at the time and this restricted the functionality of the applications.

(B) The General Packet Radio Service [83] (GPRS) data services were not yet available in all parts of South Africa and it limited the use of the application.

(C) The available GPRS speed fluctuated between 9 to 56 kilobits per second, making the user experience on channels like WAP and J2ME undesirable due to the slow data speeds available on the GSM network.

(D) STK applications utilized a number of SMS messages to communicate with the cellphone banking application server and the cost of these SMS messages made it very expensive for the end user to access the cellphone banking application.

(E) The successful delivery of SMS messages in a STK application is of critical importance, unfortunately these SMS messages did not always arrive successfully at either the application server or customer handset, resulting in negative user experiences with the application.

At the time in 2004 cellphones were the common element used between both the banked and unbanked population, and provided an excellent medium to create a financial banking product that could possibly reach the unbanked. As previously mentioned, the challenge was to find the correct GSM delivery channel that required minimum effort to deliver the application to the customer handset. South Africa had already high cellphone penetration rates with a very high uptake in the unbanked population segment. Cellphone uptake in the unbanked market was mainly driven by the available prepaid airtime services that allowed people to own a phone and receive calls but only pay for outgoing calls as and when needed.

It was evident that a solution had to be found that could utilise the use of the cellphone to reach the estimated 11 to 13 million unbanked people of South Africa. The main

obstacle was to uncover a cellphone banking channel that could work on any cellphone device available in the South African market and that did not require the replacing of SIM cards on the cellphone of the end user. The ultimate channel had to enable stable data delivery and ensure a guaranteed positive user experience to the customer in order to deliver a successful cellphone banking application.

According to the website GSM World, more than 3 billion people are using GSM telephone devices, covering approximately 80 percent of the world's population with mobile networks. With these statistics, GSM is fast becoming the most popular way to deliver information, communication and entertainment services to people worldwide [35].

The next paragraphs describe each available GSM channel and evaluate its characteristics to launch a cellphone banking application.

3.2 Voice channel

The voice channel that is provided over GSM networks are used daily in making phone calls via the cellular networks with cellular phones. The voice channel was the main driving force in creating cellphone technology that did not restrict voice communications to physical land line connections. The GSM voice channel can also be used for self-service assistance, this technology is called Interactive Voice Response [89] (IVR). According to the website PCMAG.com the definition of IVR is an automated telephone information system that speaks to the caller with a combination of fixed voice menus and data extracted from the database in real time. The caller is prompted to respond by pressing digits on the telephone, speaking words or short phrases. Typical applications implemented through an IVR channel include bank-by-phone, flight-scheduling information and automated order entry and tracking [53].

Customer support in a bank call center is another example of the usage of the voice channel. In using IVR technology, a pre-defined voice menu is setup on an application

server with relevant voice tags associated for each menu option. A customer will dial a service number and will hear a voice announcing the menu options. The customer will select the relevant option and the IVR voice will continue to request the relevant information from the customer to complete an associated request. The ability of IVR to request information from a person and route the information correctly makes it a very good channel to use when implementing a cellphone banking application.

A great benefit of IVR is that it works on all cellular handsets that are available in the market. Similar phone banking services were already launched in the early nineties on normal telephone land line phones. If IVR is used to deliver a cellphone banking application, it will work on any cellphone without any changes on the cellular device. The application will only use the voice channel that is available on the cellular phone to connect to the mobile network operator that will route the request to the cellphone banking application server.

Security on the voice channel in a GSM environment is again implemented through the A3 and A5 algorithms that secure the voice communication through the network as indicated in Figure 2.1 of chapter 2. As part of the authentication of the application, a customer will have to select a cellphone banking PIN as part of the registration process for authentication purposes during any interaction with the application. This PIN will have to be captured every time during the IVR interaction session to determine the identity of the customer. To secure the implementation of a cellphone banking application over IVR, it is recommended that the cellphone banking application server only allow requests from registered cellphone handsets and a customer can only use the combination of his registered phone ("something you have") and selected cellphone banking PIN ("something you know") to access the service. With this approach, a two-factor authentication for access to the application will be enforced.

The benefit of IVR from a usability perspective is that the menu can be offered in different languages and it allows customers to interact with the service in their preferred language.

An inhibiting factor of an IVR voice cellphone banking application is the cost that the end user customer will incur to execute a transaction over this channel. A cellphone banking application can have a complex menu structure that forces the IVR Voice to announce all options before the customer can make a selection of the preferred transaction that needs to be executed. The entire duration of the call is billable to the customer at normal voice channel rates and the extensive cost to the end user made it too expensive to consider as an adequate bearer channel to reach the unbanked in South Africa.

As part of WIZZIT's research before the launch of the cellphone banking service in 2004, the voice channel was considered as a delivery channel. The fact that the service could work on any cellular phone in the market if a voice IVR solution was used, made this option extremely relevant to reach the unbanked population. Another positive consideration was the fact that through the IVR, the service could be implemented in all the different languages spoken in South Africa. It was also a fairly simple procedure to implement the IVR voice channel because all the networks at the time supported IVR Services. It is important to note that although the reach of the voice channel made it a very good channel to consider, WIZZIT were not overwhelmed to launch an IVR Voice service as it stood in resemblance of the land line phone banking solutions that were already in the market.

WIZZIT launched in 2004 their cellphone banking service through USSD and IVR channels but the uptake through the IVR channel was extremely low. Further investigation revealed that the cost of conducting a transaction on this channel was too expensive for the target market and today WIZZIT has eliminated the IVR channel from their cellphone banking service offering.

3.3 Short Message Service channel

The SMS GSM channel allows the user to prepare a text message of 160 alphanumeric characters and to send it to any other cellphone user. The First SMS messages was send in

December 1992 and today it has become a standard and cheap way to communicate over distance through your cellular phone [63]. SMS was originally only used for short text message communication between individuals but today it is used in multiple customer relationship management software as a means of communication with customers.

In the early days of SMS messaging, companies used GSM modems that were connected to application servers to distribute SMS notifications. Mobile networks realised the revenue opportunity and subsequently introduced the Short Message Peer to Peer Protocol [107] (SMPP) to third parties to submit batches of SMS messages directly to the mobile network for distribution to customer cellphones. SMPP is an open, industry-standard protocol for sending text message (SMS) data over the Internet. It is used primarily for connecting third-party services with SMS centres, enabling various types of automated SMS services. It is also used to link SMS centre gateways, enabling inter-carrier messaging [57].

This led to the classification of SMS messages into two groups namely Mobile Originating (MO) and Mobile Terminating (MT). MO SMS is defined as when an end user sends a SMS message from a cellphone to a destination that could be another phone or SMS service center [55]. MT SMS is defined as big volumes of SMS messages being processed through the Mobile Network SMPP interface to be sent to end user handsets [56]. MT SMS allow the receiver to reply with a response message that could be used by the originating application server to gather customer feedback.

To enhance the features of SMS in Mobile networks, the operators introduced a concept of SMS Short Codes to make it easier for customers to submit SMS messages to a specific destination. A SMS Short Code is a numeric code that is assigned to a commercial organization for text messaging (SMS). The user sends a message to a SMS short code rather than to a telephone number, in order to receive a quick answer or to subscribe to a service that sends them periodic alerts. SMS Short Codes are three to eight digits in length depending on the country, and, like telephones, numbers often spell out brand names for easy memorisation [54]. Examples of SMS Short Code usage are marketing

campaigns, voting exercises and purchasing of cellphone wall papers and ring tones.

SMS is also referred to as stored-and-forward technology due to the way of how messages are transmitted to and from cellphones. The message (text only) from the sending cellphone is stored in a central Short Message Service Center [109] (SMSC) which then forward it to the destination cellphone. This means that in the event that the recipient is not available, the short message is stored and can be sent at a later time [36].

A security risk around SMS technology is that the context of a SMS is stored unencrypted in the send items box of the originating cellphone handset, making this technology extremely vulnerable and easy to infiltrate if used in a cellphone banking application.

The banking industry launched limited cellphone banking applications through the SMS channel, but these applications could only serve transactions like balance enquiries, mini-statement requests and cheque book ordering. Transactions with financial impact introduced a security risk because the cellphone banking PIN had to be captured as part of the originating message. The unencrypted storage of the message in the originating sent items box, exposed the cellphone banking PIN of the customer in the clear to any other person that might have access to the cellphone handset.

From a usability perspective, SMS provide an easy method to capture originating requests offline, but the challenge is to educate the end user to capture the correct message format for a cellphone banking instruction SMS that can be interpreted correctly by the cellphone banking application server. The following can act as format for a balance enquiry message:

[Balance] [account number] [Cellphone banking PIN]

Or

“Balance 400000000023 1234”.

If SMS technology is considered for a cellphone banking application, it is important to take cognisance of the fact that the SMS channel cannot be interactive to execute

a number of transactions in a single request. A customer can only execute one SMS instruction that correlate to one cellphone banking transaction at a time. The cellphone banking application server will require a new SMS message request from the customer to execute further instructions.

A great advantage of SMS is that the channel is supported by any GSM cellphone handset, making it a great ubiquitous channel to implement a cellphone banking application. This implies that a user can immediately start using the cellphone banking service once registration for the service took place.

From a maintenance perspective a SMS channel can be easily managed as new transactions can be introduced on the cellphone banking application server, and the message format must be shared with the end users to request the transactions successfully.

The SMS bearer has become an excellent notification medium. Banks started to introduce bank account alerts that were distributed to their customers through MT SMS messages. Today, this is almost standard practice to receive a SMS alert notification from your bank in the case of financial transactions such as cash withdrawals, point of sale or internet purchases from your bank account.

When cellphones were launched into the market, voice communication was the main purpose of the utilisation of the device. Afterwards SMS messaging followed as a method of communication by sending text messages between people. As the cellphone technology evolved, various different applications were introduced and one of the possibilities was to launch a basic cellphone banking application through the SMS bearer channel. A bank customer would send in a SMS messages to a dedicated SMS Short Code that was serviced by a cellphone banking application server at the bank and after a few seconds the result of the enquiry would be send back to the customer in the form of a SMS text message.

The following transactions were considerations in a SMS cellphone banking approach as must have abilities:

(a) **Balance Enquiry:**

The customer would send an SMS string in the format "Balance 40000000023 PIN 1234" to a central number "55555" and the bank server would reply with "Account 4000000003 Current Balance: R1000 Available Balance: R870.00".

(b) **Inter account transfer:**

The customer would send an SMS string in the predefined format "Transfer from acct to acct Amount Reference PIN 1234" to a central number "55555" and the bank server would reply with "Your transfer was successful. Thank you for using the service. Your reference number is CE243EDGC."

(c) **Transfer to another person:**

The customer would send an SMS string in the predefined format "Transfer receiving cell number Amount Reference PIN 1234" to a central number "55555" and the bank server would reply with "Your transfer was successful to number 0834503438. Thank you for using the service. Your reference number is AUE3D342."

Although this SMS approach would work on all phones in South Africa at the time, it proved to be complex to train the customers to execute these pre-defined SMS strings. A further disadvantage was that the cellphone banking PIN number had to be included unencrypted inside the SMS message. A serious security risk is the factor that most cellphones keep a history of sent SMS messages. This would mean that an unattended cellphone could be scrutinised by a third party for the last few SMS messages that were send, obtaining the clear cellphone banking PIN number of the customer for fraudulent use.

A SMS cellphone banking approach would provide an ubiquitous solution but the problematic combination of complicated customer education and high security risk due to the storage of unencrypted PIN numbers on the cellphone device eliminated the SMS mobile network channel as a preferred option.

3.4 SIM Toolkit Application channel

In the original approach to launch a cellphone banking application the option of utilising the STK [111] application were explored. According to Gemalto, one of the largest cellular STK card manufacturers in the world, the STK application is a set of commands which define how the card should interact with the outside world, and extends the communication protocol between the card and the cellphone handset. With STK application, the card has a proactive role with the handset (this means that the SIM initiates commands independently of the handset and the network). In Second Generation [105] (2G) networks, STK was defined in the GSM 11.14 standard. From release 4 onwards, GSM 11.14 is replaced by 3rd Generation Partnership Project [114] (3GPP) 31.111 which also includes specifications of USIM Application Toolkit [119] (USAT) for 3G networks [30].

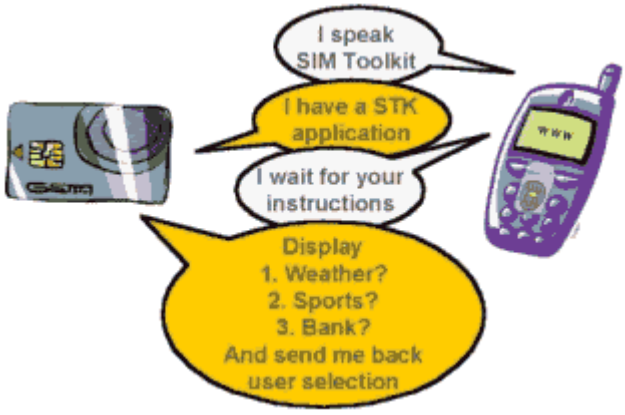

Figure 3.1: SIM Toolkit Application interaction with a cellular handset [30]

Typically, a cellphone banking application would be implemented by utilizing the STK builder that creates binary code that is stored on the SIM card. This application needs to be developed in conjunction with the mobile network operator to assure that the application will fit onto the available memory space of the SIM card. A specific security key pair is required from the mobile network operator to sign and load the binary application onto the memory available on the SIM cards.

History showed that the available application space on the mobile network operator SIM cards were originally the biggest obstacle for implementing a STK cellphone banking solution. Mobile network operators at the time could only deployed SIM cards into the market that supported 8 Kilobytes of memory space, as the technology used by SIM card manufacturers at the time could only supported 8 Kilobytes of memory space.

The bank and participating mobile network operators had to work closely together to ensure that the application would fit onto the available memory space of the SIM cards. The cellphone banking application had to share memory space with the other applications and information that were already loaded by the mobile network operators onto the SIM card. This space restriction led to cellphone banking applications with limited functionality and it only offered transactions like balance enquiries, mini statement enquiries and basic account transfer transactions. The memory space limitation on SIM cards has been rectified in recent years as SIM card technology advanced. SIM card manufacturers now has the ability to deploy bigger memory size SIM cards into the market, and today it is common to see SIM cards that have memory sizes in the region of 64kb, 128kb and 256kb in size.

The mobile network operators play a very important role in a STK approach because they have the ability to determine which banks are allowed to deploy a cellphone banking application on the SIM cards, as they are the owners of the SIM card. The mobile operator has to provide the security key pair that will allow the bank to develop and load the application on the SIM card.

In a STK approach, the bank has three options to deploy a cellphone banking application into the market:

- Load the application during the manufacturing process of the SIM card.
- Download the application later Over the Air [102] (OTA) utilizing a set of binary SMS messages. The biggest challenge experienced with this option is the fact that the SMS messages must arrive in the correct sequence on the mobile handset to

install the application correctly. It causes big frustration during the deployment process as most of these applications require more than 20 SMS messages to be received in sequence on the mobile handset to install correctly.

- Do a SIM swap for all bank customers that want to use cellphone banking. All customers need to visit their bank or mobile operator to swap out their existing SIM card with a new SIM card that has the cellphone banking application installed. There are huge costs involved in the SIM swap exercise and the cost recoupment is passed onto the customer, creating a barrier to customer entry.

In light of the above problems regarding SIM memory space availability coupled with the problematic deployment of the application to the mobile handset, made it difficult to create new features to the application and resulted in the application becoming inappropriate and out dated over time.

A STK solution delivers an excellent user experience due to the fact that the application executes directly from the SIM card located in the customer handset. The result is that the customer experiences fast interactive browsing of the menu's implemented through the SIM based application.

STK programs are implemented through a client-server technology approach where the application on the SIM card acts as the client. Interaction with the bank's cellphone banking server can be implemented by utilizing SMS messages or USSD messages. The utilisation of SMS or USSD as the communication medium to interact with the cellphone banking server can contribute extra costs to the customer because the mobile network operator will invoice the mobile subscriber who is the bank's customer directly for the message traffic generated by the cellphone banking application.

The security measures implemented through a STK solution is secure, due to a session key being used to encrypt the cellphone banking transactions from the customer handset through all three zones as indicated in figure 2.1 in chapter 2. This implies that the message travels fully encrypted with the session key from the mobile handset to the

bank's cellphone banking application server.

In summary, although various STK cellphone banking solutions are available, customer uptake is not very high due to the limited features of the application as a result of the limited space available on the SIM cards. The OTA download creates big frustration both from an end user perspective and a bank support perspective. Lastly, the cost of SMS messages to deliver instructions to the bank's application server resulted in criticism regarding this approach to deliver a cellphone banking application.

3.5 Wireless Application Protocol channel

According to the WAP Forum Wireless Application Protocol white paper published in June 2000, "WAP is the de-facto world standard for the presentation and delivery of wireless information and telephony services on mobile phones and other wireless terminals at the time' [29]. Cellular phones have limited Central Processing Unit [77] (CPU) power, memory capacity and battery life compared to standard computers. Cellular phones are companion products that allow the ability to deliver information, process transactions and enquiries when the user moves around. According to the WAP Forum white paper, "WAP services provide PIN point information access and delivery when the full screen environment is either not available or not necessary" [29]. WAP solutions leverage tremendously on existing server infrastructure and programming knowledge that allows software developers to develop sophisticated applications with existing development tools.

The WAP protocol is similar to current internet technology available on personal computers, but pages will be rendered by the internet browser of the customer mobile handset. Instead of utilizing HyperText Markup Language [85] (HTML), WAP 1.X applications are implemented through Wireless Markup Language [126] (WML) pages. A re-engineered version of the WAP protocol was released in 2002 and was called WAP 2.0. WAP 2.0 uses a scaled down version of Hypertextual computer language standard

designed specifically for mobile phones [129] (XHTML MP) with end-to-end HTTP eliminating a gateway server and custom protocol. A WAP Gateway can be used with WAP 2.0 but it serves only as a standard proxy server. In the case of WAP 2.0 the function of the WAP gateway changes from translation to a function where the Mobile Network Operator can configure additional data to be submitted with each request to the Application server. This additional information include things like the MSISDN, location, billing information or even handset information of the requester. For WAP 1.X, the primary language of the Wireless Application Environment [124] (WAE) is WML where in WAP 2.0 the primary language is XHTML MP.

Most mobile handsets available in the market today will support an Internet browser that will support WAP 2.0.

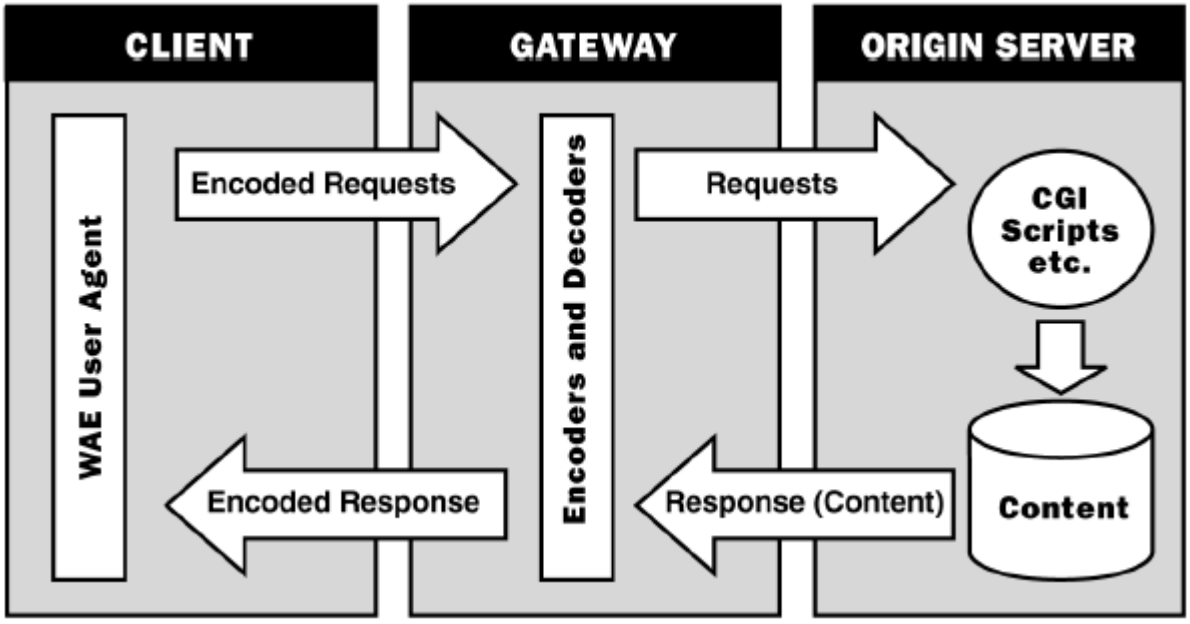

Figure 3.2: The WAP Programming model [29]

Figure 3.2 provides a schematic presentation of the WAP Programming model. A customer will access an application through the web browser on his cellular phone and a request will be routed to the gateway server that is usually located inside the mobile network operators. The gateway server route the request to the relevant application

server at the bank to process the customer request. Once the request is processed and information is available, the response message is routed back to the gateway server and from there passed back to the browser on the customer handset.

WAP is proving to become a preferred bearer channel due to the continuous increase in speed and quality of data services provided through mobile network operators. The availability of cellular phone internet browsers that can render the content of mobile websites supports the growth of WAP.

Mobile networks evolved from First Generation [81] (1G) to Fourth Generation [82] (4G) during the past decade. During the 1G time period, mobile handsets were mainly used for wireless phone calls. In the 2G stage, networks started to introduce data services but at very low speed that made it cumbersome to launch data orientated services like cellphone banking. In the last few years, 3G supported handsets were introduced to the market and faster data services of up to 1 Megabits per second could be reached. With the latest launch of 4G networks that utilize Long Term Evolution [97] (LTE) technology wireless data transmission speeds of up to 50 Megabits per second can be achieved. Most mobile network operators are nearing saturation levels in mobile phone communication income streams, and wireless data services is regarded as the next growth opportunity. All this development in the speed of data on cellular networks led to the introduction of very advanced wireless data technology that can boost the utilization of WAP applications to deliver advanced browser based applications. It is noticeable that an increasing number of companies have recently launched specific mobile device web sites (www.makro.mobi, www.sterkinekor.mobi, www.fnb.mobi, etc.). These websites are registered as .mobi (dot mobi) domain websites [44] that are specifically optimised to be accessed from a cellular phone. With the increase off smart cellphones on the market and the increased data speeds available, internet browsing on mobile phones is becoming a much more user friendly experience.

The original approach from banks to implement WAP based cellphone banking solutions

were to scale down their existing internet banking to a smaller size page that was presented on a cellular phone handset web browser. The problem with this approach was that the mobile screen is very small and the customer only has a 9 character keypad to complete transactions. On Smartphone devices that has QWERTY keyboards [104] available, access to these web sites become easier. Availability of data services, the speed of data service, the small screen and numeric based keyboard at the time before Smartphone devices, caused a barrier to the acceptance of WAP based cellphone banking applications.

Securing the WAP channel on cellular phones can be implemented by utilizing SSL encryption with relevant trusted center certificates provided by companies like VeriSign or Thawte. The internet browser on the mobile handset will verify the authenticity of the SSL certificate against the provided entrusted centre and will encrypt all communication between the mobile handset web browser and the cellphone banking application server utilizing the SSL certificate.

A great advantage of WAP based cellphone banking application is that the solution is implemented on the application server residing at the bank and the user presentation is rendered through the web browser on the cellphone handset. This approach does not require the customer cellular handset to receive any downloads or upgrades to support a cellphone banking service. The cellphone banking service can be enhanced on the application server at the bank to include new features without any change needed on the customer cellular handset. This allows a more dynamic approach to cellphone banking that will ensure better customer retention due to continuous innovations and new features presented through the service.

WAP based cellphone banking solutions can be distributed to customers by providing them with a SMS Short Code. This will assist them to send a SMS message to the short number and in turn the cellphone banking application server respond with the relevant .mobi web site of the bank that delivers the WAP cellphone banking application. Alternatively, the bank can promote their WAP cellphone banking web site through

normal marketing and the customer can access the site directly from the browser on the mobile phone.

There are two solution approaches that can be followed to implement a WAP based cellphone banking solution:

- **Internet:**

  With this option, the bank will launch the service as a WAP site that is normally accessible through the internet. The customer only requires internet connectivity from his cellphone to be able to access the service through the specified web site address. The risk with this approach is that internet hackers all around the world can access the .mobi website from PC browsers or cellphone browser simulators and this creates a security risk with possible hacking attempts. This approach does not support the Two-factor Authentication method of "something you have" (cellular phone) and "something you know" (cellphone banking PIN) and because of the risk involved, it is not recommended to follow this approach.

- **WAP Gateway [122]:**

  In this approach, the bank will launch the service through the WAP gateway of the participating mobile network operators.

  - The first benefit of this approach is that only cellphone handsets with SIM cards of the participating mobile network will be able to browse the WAP cellphone banking site of the bank.
  - A second benefit of this approach is that the mobile network operator will provide with each browsing request the originating MSISDN (cellphone number) of the requester. This provides the opportunity to first authenticate if this cellphone number is registered for the cellphone banking service and provide the ability to implement a two factor authentication approach. This ensures that a customer of the bank will only be able to access the service from a registered cellphone handset and the bank can utilize this feature to authenticate

the identity of the customer.

The WAP Gateway based cellphone banking application is recommended for a secure and safe cellphone banking application that is delivered through the Wireless Application Protocol.

More and more cellphones are equiped today with Internet Browsers that support full HTML rendering and does not require WML markup any more. The purpose of this dissertation is to investigate cellphone banking at the bottom of the pyramid and in this market there are still a number of phones that only supports WAP 2.0 internet browsing. Mobile Network Operators offer Internet Connectivity through their WAP Gateway as a service and the important thing to note here for a cellphone banking application is that the WAP Gateway will transfer the MSISDN of the phone that is accessing the application. This feature assist with the two factor authentication approach for cellphone banking applications.

3.6 J2ME application channel

J2ME [66] is a version of Java [91] that is aimed at devices with limited resources like cellular phones, microwaves and microprocessors that are used in the industry. J2ME consists of a set of profiles that is defined for a particular device type and consists of a minimum set of Java class libraries required for that device as well as a specification of a Java virtual machine required to execute J2ME applications on the device. SUN Java has originally released a Mobile Information Device Profile [98] (MIDP) for cellular phones and today different handsets support either MIDP 1 or MIDP 2. The MIDP profile is just a specification but is implemented through specific configurations. There are currently two J2ME configurations available for MIDP J2ME applications namely Connected Device Configuration [78] (CDC) and Connected Limited Device Configuration [79] (CLDC) [66]:

- **CDC [78]:** An implementation of the Foundation Profile for next-generation consumer electronic and embedded devices.
- **CLDC [79]:** An implementation of MIDP for small, resource-constrained devices such as cellular phone devices.

The J2ME cellular applications are designed and then developed in JAVA supported by Integrated Development Environment [87] (IDE) like Eclipse or Netbeans. These development environments have different cellular front end simulators to test applications before they are deployed to the cellular handsets. J2ME applications are interpreted and executed through a JAVA virtual machine that is shipped with a number of cellular handsets available on the market today. The application developer must design and test the application in such a way that MIDP and CLDC functionality is incorporated and supported to ensure the application will work on most of the cellular handsets available on the market.

J2ME applications are compiled on the development environment IDE and can then be downloaded from the development computer on to a cellular handset through a connection cable. If the application development computer and the mobile handset both support Bluetooth [76] connection, the compiled J2ME application can be transmitted to the cellphone handset through Bluetooth. These two approaches are only acceptable during the development and testing period of a cellphone application because it does not support the download to multiple cellphones concurrently.

A more advanced deployment method for a J2ME cellphone banking application onto multiple phones is to incorporate a SMS short number that is communicated to all banking customers. The customer can SMS the word “register” for example to the number “31500” and a response SMS will be send back to the customer containing a specified internet Universal Resource Locator [117] (URL) that can be used to download the J2ME application. The only other requirement is that the customer cellphone must support internet browsing to download the application. The J2ME application will be

downloaded onto the phone and will usually install under the applications folder of the cellphone handset. The customer will have to launch the J2ME cellphone banking application on his cellphone to access the service.

J2ME applications can use SMS, USSD or GPRS data services to communicate with the cellphone banking application server at the bank. GPRS data services have proven to be the bearer of choice for data communication because it supports synchronous cheap communication that is ideal to service a cellphone banking application.

Another great advantage of J2ME is that it supports the Security and Trust Services API [52] (SATSA) for J2ME. The SATSA security APIs are in part a subset of the J2SE security and cryptographic APIs, with a lot of influence from the Java Card [92] security API. The SATSA security APIs consist of two separate but related J2ME optional packages:

1. The Public Key Infrastructure (PKI) optional package.
2. The cryptographic (CRYPTO) optional package.

These APIs enable J2ME applications to:

- Work with public digital certificates, public and private keys, message digests and digital signatures.
- Create, store, and use user-credentials based on X. 509 digital certificates [128].
- Encrypt data using asymmetric and symmetric cryptography.

With the SATSA API, public key encryption algorithms can be implemented to secure data communication between the cellphone handset and the cellphone banking application server of the bank. J2ME applications can be signed by code signing certificates issued by trusted centres that will assure authenticity and origination of the application on the cellphone.

It is unfortunately not possible to retrieve the customer MSISDN or cellphone number through a J2ME application because it is not stored anywhere on the cellular handset but only inside the accompanying SIM card. Access to the SIM card is protected by encryption keys that are only known to the mobile network operator. The J2ME application can prompt the customer to capture his cellphone number but the customer can do that on any J2ME cellphone banking application and on any phone. This makes it difficult to implement a two factor authentication method for J2ME cellphone banking applications.

J2ME applications allows for the creation of very good graphical interfaces. The bank can deliver an incredible interactive presentation layer to the cellphone banking application that makes it attractive and user friendly to the customer. Utilisation of clear graphics can create a positive user experience by giving more comprehensive instructions on the functionalities available in the cellphone banking application.

A considerable challenge with J2ME applications is version control and the distribution of new releases of the application. The application is downloaded and installed into the memory of the cellphone. If a new feature needs to be added to the application, a new version must be designed containing the feature and then needs to be redeployed to all phones. The problem in a cellphone banking application is that some customers can have the old application installed while others have the latest version. It is very difficult to manage these different versions and because of this complexity there are limited successful J2ME cellphone banking applications deployed in the world. Customers perceive J2ME applications as complicated to first install the application and then to find it on the cellphone. Although it produces a great graphical experience, the complexities around distribution and support of the application makes it a less desirable channel for a cellphone banking application.

3.7 USSD channel

USSD [68] is the acronym for Unstructured Supplementary Services Data and is unique to GSM cellular networks. It is a standard feature build into the GSM specification to transmit information over the signalling channels of a GSM Network. USSD is a session based menu driven technology that can be used for multiple applications.

According to the website www.mobilein.com, USSD's key attributes are [44]:

- USSD is session and menu driven oriented, unlike SMS, which is a store-and-forward, transaction-oriented technology.
- Turnaround response times for interactive applications are shorter for USSD than SMS due to the session-based feature of USSD, and because it is NOT a store and forward service.
- Users do not need to access any particular phone menu to access services with USSD. They can enter the USSD command direct from the initial mobile phone screen.
- USSD commands are routed back to the home mobile network's HLR, allowing for the virtual home environment concept the ability for services (based on USSD in this case) to work just as well and in exactly the same way when users are roaming.
- USSD works on all existing GSM mobile phones.
- The STK, J2ME and WAP channels can utilise USSD as a channel to transmit application information between the phone and the application server.

USSD is an old cellphone channel that existed from the early days of GSM networks but was originally not commercially available to deliver applications. A great advantage of USSD services is that it is supported by all cellphone handsets available on any GSM network. This functionality relates as a considerable channel to deploy ubiquitous relevant cellphone applications like cellphone banking.

USSD Phase 1:

Originally USSD only supported the USSD Phase 1 structure that made it very complicated to deliver interactive menu driven applications. USSD Phase 1 is defined where only one request and response can be supported in a given USSD interaction session. As an example an USSD Phase 1 application can be used by a mobile network operator customer to request his prepaid airtime balance by dialling for example a command ∗121# on his cellular phone. This request is received by an application server in the GSM network that recognises this request as an airtime balance enquiry request. The application server route this request to the mobile operators Intelligent Network [88] (IN) to determine the balance for the specific MSISDN that initiated the request. The result is returned back to the customer in seconds and the session is terminated automatically.

Due to the wide availability of USSD Phase 1 on mobile handsets, mobile network operators utilise this bearer to implement customer support services internally to their subscriber base. Examples of these type of services include the ability for customers to retrieve their prepaid airtime balance, the ability to load additional prepaid airtime vouchers on cellphones and the ability to request "Please call me" services. All these services require only one request and response pair in an interaction session and USSD phase 1 was the ideal bearer to implement the required functionality.

USSD Phase 2:

The next step in the evolution of USSD was the Phase 2 structure that is a menu driven channel that can support multiple request and response messages in a specific USSD interaction session. A typical USSD Phase 2 session will usually last between 2 to 4 minutes. USSD Phase 2 allows for the creation of a USSD Menu that can prompt a customer to select a specific option and then the result is returned to the USSD application server for processing until a specific result is reached. Mobile network operators extended their customer support services through USSD Phase 2 that allowed for a single number to be dialled by a subscriber and then have the ability to select multiple service options through the USSD Phase 2 menu. Mobile network operators realised the commercial

opportunity through the USSD channel and started to promote it as a commercial service to third parties and invoice for the number of USSD sessions or length of the USSD sessions.

To make USSD commercially viable, mobile network operators required an interface into the SS7 networks that could convert GSM USSD request response messages to the TCP/IP Protocol that could be send to third party application servers to process these requests. Soon USSD gateway [120] providers arrived on the scene to fill this gap and today most of the mobile networks have at least one USSD Phase 2 gateway available for commercial use by third parties.

USSD utilises the voice spectrum in GSM networks and mobile network operators have to plan carefully for the voice capacity of their network to be able to deliver stable voice and USSD services over the same medium at the same time. To limit the number of USSD sessions, mobile network operators will shorten the USSD session time. As mentioned above, the industry standard is to only have USSD sessions of between 2 to 4 minutes. The USSD session time must be considered in developing a USSD base application. The USSD menu must be structured in such a way that the end user can execute 4 to 5 specific interactions in a given USSD session. USSD also has an interval timeout period and this is the maximum time that a user can take to respond to the USSD server in the request/response interaction. This timeout period is usually set to 30 seconds. Mobile networks have introduced the session and timeout periods to manage and predict the number of USSD connections that will exist on the mobile network at any given time to assist with capacity problems that can be introduced by inactive USSD sessions.

As described, the USSD channel is a menu driven channel that is accessed through a string that starts with a asterix ("*") and ends with a hash ("#") command. Examples of USSD dialling strings are *120#, *120*949#, *120*949*1#. A very nice feature of these USSD strings are that they can be stored inside the address book of the cellular handset for future use the same way as a customer would store contact numbers. This allows the cellphone user to store for example a USSD code for his cellphone banking

application in his telephone address book.

USSD Menu screens can display only 160 characters at a time and the screens must be optimised to project the right menu items across to the end user. USSD interaction can support both alpha and numeric characters but typing alpha characters requires different actions on different phones and makes it more complicated for the end user of the service. Numeric key response USSD interaction is fairly easy on most phones and it is recommended that any USSD application menu is designed to rather prompt numeric selections from the end user.

The USSD bearer is becoming more and more a favourable mobile network bearer channel for third parties due to its extensive reach to mobile handsets and the fact that no adjustments or downloads is required to the mobile handset to support a USSD service.

Security of USSD is implemented through encryption standards build into GSM networks. USSD request and response messages are transferred through Zone A and B in figure 2.1 in the GSM network and is encrypted with the A3 and A5 algorithms as explained in chapter 2. At the USSD gateway inside the mobile network, the protocol is translated from SS7 to TCP/IP implying that the message is in the clear at that moment in time. In Zone C, connectivity between the USSD gateway at the mobile network and the cellphone banking server is implemented through the TCP/IP network protocol. It is recommended that a VPN with the necessary security keys are implemented to secure the traffic that will be send across this connection.

Reviewing the security risk, it is clear that the major exposure is at the USSD gateway where the message protocol is converted from SS7 to TCP/IP. The network traffic will be in the clear at this moment in time and the bank needs to assure that the USSD Gateway of mobile operators are restricted so that the information traffic is not exposed to the outside world. It is suggested that mobile network operators and banks must sign a data security agreement to mitigate the risk and regular audits must take place to ensure the confidentially of customer data.

USSD is an ideal bearer for a cellphone banking application because it supports a menu driven application that can be deployed to all phones available in a given market. It has a potential security risk, but it is important to evaluate the risk involved to customer experience and reach, and there are ways to mitigate the risk for example through the introduction of transaction limits. A great feature of a USSD application is that it supports a server side approach that makes it very easy to introduce new features to the application that will be immediately available to all the customers that are allowed to access it.

Research conducted in 2004 revealed that the mobile networks in South Africa utilise USSD for customer support and that it worked on all phones and the service is delivered by dialling a text string that is in the format of ∗Operational code# or ∗123#. Figure 3.3 illustrates the menu flow of an example mobile network operator customer support menu.

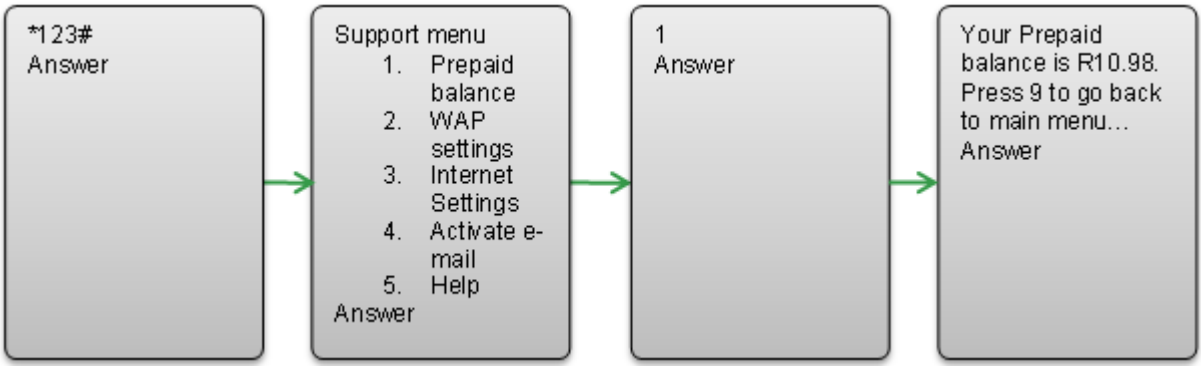

Figure 3.3: USSD Menu for a mobile network operator customer support

The unbanked market in South Africa was already using USSD services for some time because mobile operators used USSD strings to activate PIN based prepaid airtime vouchers. A prepaid mobile network customer would buy a PIN based airtime voucher at a local shop in the form of a scratch card. Once the prepaid airtime voucher is scratch open, the customer would capture a string that is in the format "∗121∗PIN based Voucher#". When a request is received from the phone, the airtime voucher will be validated in the

mobile network IN and credit the requesting phone with the associated prepaid airtime denomination.

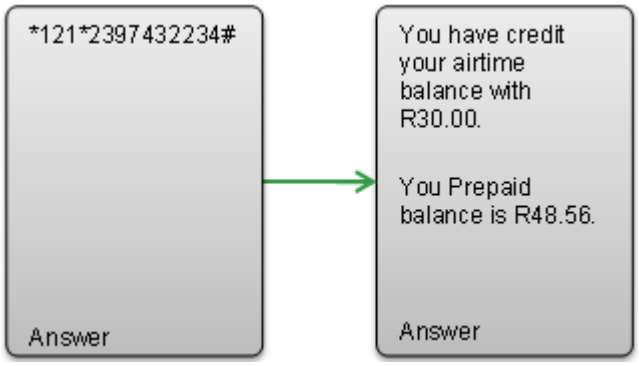

Figure 3.4: Example of a USSD airtime credit instruction from a prepaid subscriber phone

Further investigations into the USSD channel led to the finding that this interface could be used in a synchronous menu driven format for multiple applications like customer support, retail marketing and information display. At the time further USSD tests were conducted against the available cellphone brands in the South African market. These included brands like Nokia, Ericsson, Motorola and Samsung as well as Smartphone devices such as HTC and BlackBerry. The research USSD test results were all successful and the conclusion was that the USSD channel could be an ideal ubiquitous channel to be considered for launching a cellphone banking application for the unbanked. It worked on all major branded phones available in South Africa and it could rollout the solution to any cellphone without touching the mobile handset or the SIM card of the phone.

The timing for launching the WIZZIT service was perfect because all mobile operators in South Africa were at the time in the process to commercially launch USSD services through the Wireless Application Service Provider [125] (WASP) concept. This made it easy for WIZZIT to integrate to the USSD gateways of each of the three available networks Vodacom, MTN and Cell C.

Further investigation into USSD raised concerns around security, and WIZZIT almost

aborted the USSD approach. However, the ease of use of USSD as well as the awareness of the ∗123# mobile network operator support services strings in the unbanked market in South Africa still had great potential to deliver a cellphone banking solution.

The challenge was to find a solution to mitigate the risk at the USSD gateway inside the domain of the mobile network operator. Further discussions with the mobile network operators indicated that they rarely investigate the logs of the USSD gateway and that it is more used for fault finding situations if required and only in exceptional cases by senior staff members. The engineers that access these logs all have signed confidentially agreements with the mobile network operators to protect sensitive information as part of their employment contract. These engineers also have access to all telephone records and it is important for the network operator to assure confidentially of this sensitive information. WIZZIT accepted that although some people could see the logs, it was protected under confidentially agreements limiting the security risks involved.

WIZZIT continued investigations to find solutions to make the USSD channel even more secure, and realised the potential to use two different channels in combination to deliver a financial transaction. The solution was designed in a way that every USSD cellphone banking transaction that has a financial impact to the customer bank account will generate a SMS alert or confirmation to the customer through the Mobile Terminating SMS channel. The customer will instantaneously know if the SMS alert is valid for the transaction or if somebody else is doing an unauthorised transaction and could contact the WIZZIT call center to stop his cellphone banking immediately.

For further security, the solution was designed to enforce daily transaction limits on the USSD bearer channel. In other words, the customer can only transfer money to a set daily limit and in that way the bank have a controlled risk if fraudulent activity occurs on the customer account.

The pricing for USSD services in South Africa was agreed by all networks at 20 cents per 20 seconds. Most transactions in WIZZIT can be conducted in less than 60 seconds that imply a cost of maximum 60 cents per transactions. Compared to the cost of getting

into a taxi to go to the nearest ATM, the cost for USSD is perceived as cheap and the customer can access his bank from the convenience of his home.

This approach allowed WIZZIT during 2004 to use for the first time in South Africa two GSM bearer channels to implement a cellphone banking application and to launch it successfully to the unbanked population in the country. Although the original plan was to focus on the unbanked, a number of banked people started to use the product due to the ease of use with the USSD selected application.

3.8 Android Apps

At present, Android is a familiar concept making inroads as the mobile handset operating system on a large number of cellular handsets. The perception exists that Google is the owner of Android but during 2005 Google bought a number of start-up companies in the technology arena. One such a company was Android Inc. which was co-founded by Andy Rubin, that is today the director of mobile platforms at Google [25].

On 5 November 2007, a broad alliance of leading technology and wireless companies joined forces to announce the development of Android, the first truly open and comprehensive platform for mobile devices. This alliance shared a common goal of fostering innovation on mobile devices to give consumers a far better user experience than the current mobile platforms. By providing developers with a new level of openness that enables them to work more collaboratively, Android will accelerate the pace at which new and compelling mobile services are made available to consumers. This collaboration project is known as the Open Handset Alliance and the creator of the Android mobile operating system. Founding members include companies like Google, T-Mobile, HTC, Motorola and China Mobile [51].

The Android operating system is built on a Linux kernel with the Dalvik virtual machine that is a register based virtual machine to execute the applications. Dalvik is designed

to allow multiple VM instances to run at the same time and it is optimised to support low memory requirements. Android applications or so called Apps [1] are developed in a JAVA integrated development environment like Eclipse and compiled into .dex (Dalvik Executables) files that will be packed into a single .apk (Android Package) file on the mobile device [22].

The Android system requires that all installed applications must be digitally signed with a certificate whose private key is held by the applications developer. Android uses the certificate as a method of identifying the author of an application and can be used to determine trust relationships between applications. It is important to note that the certificate does not need to be signed by a certificate authority [5]

Software developers can design and develop supported Android Apps that end users can download and install on their Android supported cellular handsets. Android cellular handsets are classified as evolved high technology phones and were originally targeting the top end of the market but today supply affordable Smartphone devices. According to an article on the website Network World, almost 51.9 million Android-based phones shipped in the second quarter of 2011, giving it a 48% market share of the phones shipped in that quarter [59].

Although Android cellular handsets can support innovative cellphone banking applications, the reach of these handsets are still limited on the African continent. The manufacturers of Android devices are working hard to make these phones available to the lower end of the market and there are now Android phones available for less than US Dollar 100. Android is definitely a cellphone banking application platform to consider for the future as the Smartphone devices become more generally available in the market.

In September 2011, the author visited Rabobank in the Netherlands and met with one of the architects of the Rabobank Mobile banking and payments applications, David Jan Janse. Janse mentioned that they had extensive uptake in the usage of their Apple iPhone application but since the launch of their Android App, customer uptake has doubled week on week. This is a clear indication of the potential of Android Apps in

future [38].

3.9 Apple iPhone and iPad Apps

Apple launched in June 2007 the first Apple iPhone version into the market [18]. Subsequent versions of the iPhone were released over the years and the latest Apple iPhone 4S has been launched in October 2011. Apple is projected to lead all Smartphone device manufacturing shipments in 2011 by shipping an astonishing number of 86.4 million handsets into the market world-wide [50]. Apple launched on the 3rd of April 2010 the first Apple iPad into the market [19]. The Apple iPad is a tablet computer that allows users to download various Apple applications or so called Apps [1] from the Apple Appstore [72]. Some models of the Apple iPad are released with GSM network connectivity that allows the end user to connect through GSM GPRS data services while on the move.

Due to these extensive numbers of Apple iPhone and iPad handsets available in the market, a cellphone banking Apple App is a definite consideration as an alternative channel for banking. Apple iPhone and iPad devices are expensive and are mainly used by the high end affluent market. An Apple cellphone banking App can be developed and distributed through the Apple Appstore to all the different Apple devices. Apple Apps can be developed to deliver clear graphical user interfaces and communication with a cellphone banking server and can be routed through a secure internet connection delivered either through the GSM or Wireless capabilities of the Apple device.

It is recommended that Apple App developers implement code signing before the distribution of the App. Code signing is a Apple security technology that proof that an application was developed by a specific developer. If an Apple App is signed, the system can detect any change to the App whether it was introduced on purpose for an upgrade or if malicious code was added. To sign code, a code signing digital identity is required that consist of a private cryptographic key plus a digital certificate. A code signing digital identity can be obtained through a certificate authority like VeriSign,RSA

or Thawte [23].

During July 2011, First National Bank was the first bank in South Africa to launch a Smartphone device App banking application [9]. Although the application is available on a number of Smartphone devices, it was the first application of its kind to be available on Apple iPhone and iPads in South Africa. Internationally a number of banks are considering building similar applications and the Rabobank of the Netherlands is one of the leaders of bringing banking to Apple iPhone devices.

3.10 BlackBerry Apps

BlackBerry phones from Research In Motion [60] (RIM) are daily used by millions of people around the world to make phone calls but more importantly to access their e-mails remotely. The first BlackBerry device was introduced in 1999 as a two way pager. The Smartphone version as we know them today were released in 2003 and supported push e-mail, mobile telephone, text messaging, Internet faxing and Web browsing [74].

Research In Motion released a product called BlackBerry Enterprise Server [74] (BES) that assist with integration into corporate companies e-mail applications like Microsoft Exchange, Lotus Domino and Novell GroupWise. BES serves as an e-mail relay to assure that company staff members always have access to their e-mail remotely by providing push e-mail to the BlackBerry device. BES monitor the e-mail Inbox of the user and when a new e-mail arrives, it is forward to the RIM's Network Operations Center that will then forward it to the users mobile network operator. The mobile operator lastly then deliver the incoming e-mail to the BlackBerry device of the user.

To extend the well known BlackBerry e-mail services beyound the corporate world, RIM introduced a service called BlackBerry Internet Service [74] (BIS). BIS allow the normal individual end user to experience the BlackBerry e-mail service by configuring up to 10 e-mail accounts and to receive pushed e-mails from these accounts. The BIS service

additionally allows for unlimited internet browsing from the BlackBerry device Internet browser incorporated in the fix monthly cost of the service.

RIM extended further options of communication to their users by introducing a proprietary solution for sending and receiving encrypted instant messages, voice notes, images and videos. This service is known as BlackBerry Messenger or BBM.

Third party developers can develop applications for the BlackBerry phones. If an application requires restricted BlackBerry API functionality, it must be digitally signed by an associated developer account at RIM. The signing procedure guarantees the authorship of the application but does not guarantee the quality or security of the code.

BlackBerry has launched BlackBerry App World on 1 April 2009 as an application distribution service. This service provides BlackBerry users with an environment to browse, download and update third party applications [75].

Although BlackBerry has received stiff competition from Apple and Android products world wide, it is focussing on growth in the developing market of Africa [4]. Part of their success formula is to charge a flat fee for BIS that supply unlimited internet access to the user. This fee structure plus the growth in BlackBerry Messenger makes this a viable solution to a market where internet access is limited and expensive.

3.11 Comparison of the GSM channels for cellphone banking

There are mainly four areas to consider when evaluating the different GSM channels that can be used for the implementation of a cellphone banking application.

The first area of consideration is the security implementation in the relevant GSM channel to assure non-repudiation of transactions originated by customers of the bank. Each GSM bearer channel implements different levels of security. Security of customer and

transaction data in a cellphone banking application is extremely important. The balance should be found that the requirement of a high security implementation does not jeopardise the usability of a cellphone banking application. In the past, banks considered SIM Toolkit applications that used secure SMS for the transport of data as the only secure enough GSM channel to deliver a cellphone banking application. Customers did not use this channel because of the expensive SMS costs and it resulted in the failure of this high security approach.

The second area of consideration is the usability of the GSM channel with its relevant user interface to deliver the cellphone banking application on the customer cellular handset. If the cellphone banking application is easy accessible and user friendly on the cellular handset, customers will continue to use the application on a regular basis. Special care should be given in the design of such an application to ensure ease of use to deliver a successful cellphone banking application.

The third area of consideration is the ease of maintenance of the cellphone banking application from a bank perspective. Factors to consider here is first of all the effort involved in the deployment of the application to the different customer handsets. Does this deployment consider for example the change of SIM cards like in the case of a STK application or can the application be accessed on all phones over the air like in the case of USSD? Then, once the application is deployed to the customer handsets, how easy will it be to support the customers that are using the application? Another consideration regarding maintenance of a cellphone banking application is how easy it is to upgrade the features of the application. In other words, the maintenance of the cellphone banking application imply the effort of deployment, on-going support of customers and how upgrades are handled for future enhancements.

The fourth area of consideration is to determine the possible customer reach of each GSM channel to evaluate the potential market segment for a cellphone banking application. The intention is that the bank must select a GSM channel that will reach as many as possible cellular handsets in the market. An Apple iPhone application could be a

great channel in first world countries due to the number of iPhone devices used in these markets but USSD on the other hand is more relevant in third world countries because the USSD technology works on any GSM handset that is available in the market.

	Security	Usability	Ease of Maintenance	Customer reach
STK	High	Medium	Low	Medium
WAP	High	High	High	Medium
Voice	Medium	Low	High	High
SMS	Low	Low	Low	High
J2ME	High	High	Low	Medium
USSD	Medium	High	High	High
Android	High	High	Medium	Low
Apple	High	High	Medium	Low
BlackBerry	High	High	Medium	Low

Figure 3.5: Comparison of available GSM channels

In Figure 3.5, a comparison is made between the different mobile network bearer channels based on Security, Usability, Ease of Maintenance and Customer reach to deploy a cellphone banking application. Each area is rated as high, medium or low depending on the success of each criteria for each specific channel.

STK channel:

The STK channel is rated high from a security perspective because end to end encryption can take place with the secure key pairs loaded on the SIM card. The STK channel is rated as medium from a usability perspective because it provides a menu driven, offline

user interface that does not support any graphics. Maintenance from a rollout perspective is cumbersome because the customer SIM card must possibly change and it is difficult to download the application successful over the air with a number of encrypted SMS messages. The SIM card belongs to a specific mobile network operator and a STK application can only be stored on the SIM card if the mobile network operator and the bank agree to share space on the SIM card for the application. Although every single GSM cellphone has a SIM card, customer reach is rated as medium because it does not guarantee that the SIM cards in the market can support a number of STK applications due to the size available on the SIM card.

WAP Channel:

The security of the WAP channel is rated high because the WAP channel allow for the implementation of SSL certificates that can verify the origination of the application and encrypt the information that is send over the GSM network. The WAP channel is rated high from a usability perspective because it allows constructing a graphical orientated user interface that makes it easy for the customer to select the different available options. Ease of maintenance is also rated as a high on the WAP channel because the application runs in the Internet browser of the phone. The WAP channel enable changes and enhancements to be made on the cellphone banking application server and it will be immediately available to all cellphone handsets without touching it. The Customer reach of a cellphone application is rated as medium at this stage because there are still cellular phones in the market that does not support internet browsing. It has to be mentioned that this is changing rapidly because of the extensive deployment of Smartphone devices that is becoming daily more affordable.

Voice Channel:

The Voice channel is rated medium from a security perspective. The channel is encrypted with the GSM encryption algorithms but it is not possible to enforce end to end encryption. The Voice channel is rated low from a usability perspective because the IVR menus need to be announced every time before the customer can make a selection. This increases the time of the voice call and at the same time increase the cost to the customer. Maintenance for the voice channel is rated high, because the menu structure of the IVR can be changed on the Cellphone banking application server and it will become immediately available to all users that interact with the system. Customer reach for the Voice channel is rated high, because it is available on any GSM cellular phone in the market. The biggest downfall of the voice channel is the high costs associated to interact over the Voice channel with the cellphone banking application.

SMS Channel:

The SMS channel is rated low from a security perspective because the cellphone banking PIN must be captured in each SMS request and it is stored inside the phone SMS outbox as unencrypted. The SMS channel is rated low from a usability perspective because it requires extensive training of customers to capture the cellphone banking request SMS messages in the correct format. The maintenance factor is rated as low. Although it is easy to make changes to the cellphone banking application on the application server, these changes needs to be communicated and trained to customers before they will be able to use the system after upgrades. The customer reach of the SMS channel is rated as high because the channel is available on every GSM cellular handset available in the market.

J2ME Channel:

J2ME supports the implementation of end to end encryption of customer data and provide a high rating for security. The J2ME channel is rated high from a usability perspective. The J2ME environment supports good graphical menus that make it easy for the customer to use the application. Maintenance of the J2ME channel is rated as low because it is perceived as difficult to rollout the J2ME application on different handsets due to the different functional support for each handset type. It is also difficult to update the application because it requires a full download of the application and a reinstallation on the cellular phone. The customer reach of J2ME is rated as medium. Most cellular handsets available on the market support the execution of J2ME applications in a JAVA Virtual Machine environment but older phones can have problems with J2ME applications.

USSD Channel:

The USSD channel is rated medium from a security perspective because it supports the GSM encryption algorithms but cannot enforce end to end encryption. The USSD channel is rated high from a usability perspective because it can be easily accessed and it supports a menu structure that makes it easy for the customer to select different options. The ease of maintenance on a USSD channel based application is rated high. The deployment of the application requires limited or no effort because it is already supported on all cellular handsets. It is also easy to make changes on the cellphone banking application server and it becomes immediately available to all customers. USSD is rated high from a customer reach perspective because the channel is available on any cellular phone by dialling a specific USSD code. The USSD channel works on the oldest available cellular handsets to the latest Smartphone device technology.

Android Apps:

Deployment of an Android App for cellphone banking is rated high from a security perspective because the application will be downloaded to the cellphone handset and a session key can be used to encrypt messages between the phone and the cellphone banking server at the bank. An Android App is rated high from a usability perspective because the Interface can be implemented with an nice graphical user friendly interface. Ease of maintenance is rated as medium because the application must be downloaded to the cellphone handset and new versions must be downloaded over the air to keep the Application up to date. Customer reach is still rated as low because the limited number of Android phones in the market but this will definitely change as cheaper Android phones reach the market. Overall an Android App approach has great potential for future as more Android phones reach the market.

Apple iPhone and iPad Apps:

Apple Apps [72] are rated high from a security perspective because it can support as well session key approach to encrypt messages between the handset and the cellphone banking server at the bank. Apple Apps introduce great graphical user interfaces that supports as well a high rating from a usability perspective. Ease of maintenance is rated as medium because the application must be downloaded for the first time to the phone over the air and afterwards new versions needs to be downloaded as well. New versions of the downloaded Apple Apps become available on a regular basis and the upgraded versions must be downloaded resulting for the end user in additional data costs. It must be mentioned that the Apple App Store was the first of its kind in the world and it is relatively easy to get new Apple Apps and to maintain and distribute new versions of the Apple Apps. Customer reach is rated as low because Apple iPhones and iPads are more expensive devices and mainly used by the higher end of the population in a country. There are also a number of countries in the world where the Apple iPhone and

iPad devices are not formally distributed by the local network operators.

BlackBerry Apps:

BlackBerry Apps implement end to end encryption for all data traveling between the device and the mobile network operator and are therefore rated high from a security perspective. A session key can also be implemented on top of the standard encryption to encrypt messages between the handset and the cellphone banking server at the bank. A BlackBerry App supports a good user interface and the device has the well known BlackBerry QWERTY keyboard that supports a high rating from a usability perspective. Ease of maintenance for BlackBerry is rated as medium because the application must be downloaded to the cellphone handset and new versions must be downloaded over the air to keep the application up to date. Although the data costs will be included in the BIS monthly service, the user still has the frustration to download the latest version through the BlackBerry App World. Customer reach for BlackBerry phones are still rated as low although BlackBerry has gained good market share in recent years with more affordable devices that bring Smartphone capability to the lower end of the market. RIM must first partner with a mobile network operator in a country before the BlackBerry services become available to the subscribers of the mobile network operator.

Conclusion:

With the introduction of additional security features like transaction limits and transaction alert notifications through SMS, the USSD bearer currently holds the biggest potential reach for a cellphone banking application. In the opinion of the author, cellphone web browser based applications can in future play a bigger role as the speed of data networks increase and web browsers enhance on cellphones. STK had limited success over the past years and are seldom considered for a cellphone banking applications due to the close integration with the mobile network operators. Great expectations originally

surrounded J2ME as a cellphone banking channel, but the complexity of downloading applications over airwaves and the different supported versions of J2ME on different cellphone handsets made it too complex to be considered as a cellphone banking channel. Android has great potential for the future because members of the Open Handset Alliance are bringing more affordable Android Smartphone devices to the market. The distribution of Android phones will take time but it has the potential to reach poorer communities because people consider cellphone upgrading as a priority item. Although Apple has great success with their cellphones worldwide, it is still a very expensive product in developing countries and rather target the top end user. BlackBerry phones bring great Smartphone capabilities to the market and lower end devices are more affordable but it is still more known as a business application device although BlackBerry Messenger is becoming more and more favourable in the youth market.

Chapter 4

Presentation layer used in WIZZIT

As described in previous chapters, WIZZIT investigated various cellphone GSM channels before launching a cellphone banking application. The final selection fell on USSD due to the ease of rolling it out to a large customer base with no need to change anything on the customer phone. In this section of the thesis, the focus is on the design of the presentation layer to be acceptable and user friendly to ultimately ensure continuous usage of the service by the end customer.

4.1 Background

The author made an unique and truly African discovery while employed by one of the local Namibian Banks. The bank had an Automatic Teller Machine [13] (ATM) installed at the Oshakati branch in the North of the country, where the biggest portion of the Namibian population is located. Unfortunately this is also the most uneducated portion of the Namibian population living in this region. Due to the wide spread location of communities, schooling is not a high priority. This particular ATM's screen was out of order for a couple of weeks and the customers were unable to see messages being displayed on the screen of the ATM. The most amazing thing was that the ATM continued to

process large numbers of transactions during this period before bank officials realised that the screen was actually not functioning properly.

The bank designed their ATM screens in such a way that it was easy to do banking transactions and the uneducated customers of the bank became familiar with the screen patterns of transactions. When the ATM screen went out of service, they merely continued to use the service successfully as they followed the sequence flow of the actions required and never actually read the instruction in the first place because they were illiterate. This observation provided proof to the author that it is important to educate a customer at the launch of a new service but as soon as they get use to the service, the natural behaviour of using the service will continue to exist.

The screen flow designs at WIZZIT were based on this experience and the approach in mind was to ensure the launch of a successful service to the unbanked population of South Africa that could also be uneducated.

4.2 The USSD customer interface

It was a priority to make the user interface on USSD very easy for the end user to access the WIZZIT cellphone banking service. During the screen design process, extensive time was dedicated in designing the user interface to allow the customer to complete a transaction within seconds. The reason for this approach was to enable the customer to complete a few transactions within the USSD session time out period that is set by the Mobile Network Operators. This USSD session time out period is usually set by the Mobile Network Operators to be around 4 minutes.

Another challenge around a USSD menu interface is that the interval timeout between USSD screens cannot exceed 30 seconds. This implies that the customer must be able to capture and respond within 30 seconds to have a successful USSD service interaction.

Figure 5.1 displays the USSD menu that is used by WIZZIT since its inception. The

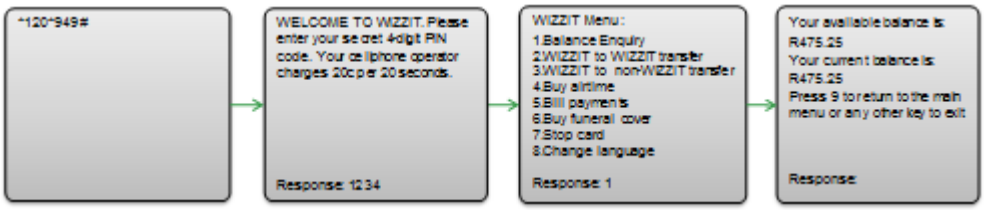

Figure 4.1: The WIZZIT USSD cellphone banking menu

menu is optimized to complete a transaction within a maximum of six request/respond interactions. The menu items have been named to describe the actions that a customer would like to execute on the cellphone banking service. For example, when a customer wants to send money to another WIZZIT customer, he will select option 2 that states WIZZIT to WIZZIT transfer on the screen, and enter the cellphone number of the WIZZIT customer, then enter the amount, confirm the transaction and the transaction will be completed. The major difference in comparison to other existing cellphone banking offerings is that the customer is requested to capture the cellphone number of the person that he wants to send money to. The cellphone number acts as an alias for the bank account number of the receiving customer. Natural behaviour of people is to rather remember another person's cellphone number than his physical bank account number.

It can also be observed from the WIZZIT USSD menu that each menu item has a corresponding number. The reason for this is that USSD supports number selection responses much easier than alphabetical characters. The customer will select the corresponding number of the action that they would like to execute. Once the menu item is selected, the USSD screen flow will guide and prompt the customer to capture the required information to execute the transaction successfully.

Another great feature of USSD is that you can capture the initiation number for an USSD service inside the telephone book of the cellphone handset like a normal contact. To illustrate this functionality, the customer can create a new phone book entry "WIZZIT Banking" with the number $*120*949\#$ in the telephone book of his cellphone and then just lookup this contact in the telephone book and dial it every time access to the WIZZIT

cellphone banking service is required. WIZZIT has trained their agents to create this phone book entry for new customers to make it easier for them to access the service on a regular basis.

All of these features make the menu driven USSD bearer channel, a very acceptable channel to reach a large number of the existing cellphone handsets on the market and made it an ideal solution to deliver the WIZZIT cellphone banking service.

4.3 WIZZIT USSD Short codes

The process of pre-capturing a payment instruction and saving it in the phone book of the cellphone is defined as creating WIZZIT Short Codes. If a customer pays regular money to another WIZZIT customer, he has the opportunity to define the payment instruction in his telephone book as a contact entry. An example would be to send money monthly to person with cellphone number 0829985847. The WIZZIT customer will create a new telephone book entry "WIZ Joe Soap" and capture the string ∗120∗949∗2∗0829985847# as the number of this new contact. Once the customer needs to transfer money to Mr. Joe Soap, he will search for the entry "WIZ Joe Soap" in the phone book entries and dial the selected number. As illustrated in figure 5.2, the WIZZIT USSD menu first request the PIN number of the customer and then continues to proceed from the point in the menu that was not captured, in this case the amount of the payment. These WIZZIT Short codes made it easier for the unbanked customers to learn the functionalities in order to make regular payments from their cellphones.

The ability to create the WIZZIT Short Codes is similar as creating a beneficiary for regular payments in an internet banking application. Customers can predefine all their regular payments in their phone book and execute the payment when required.

Whenever a WIZZIT USSD short code is executed, the application will always prompt the customer to capture his WIZZIT cellphone banking PIN for authentication purposes.

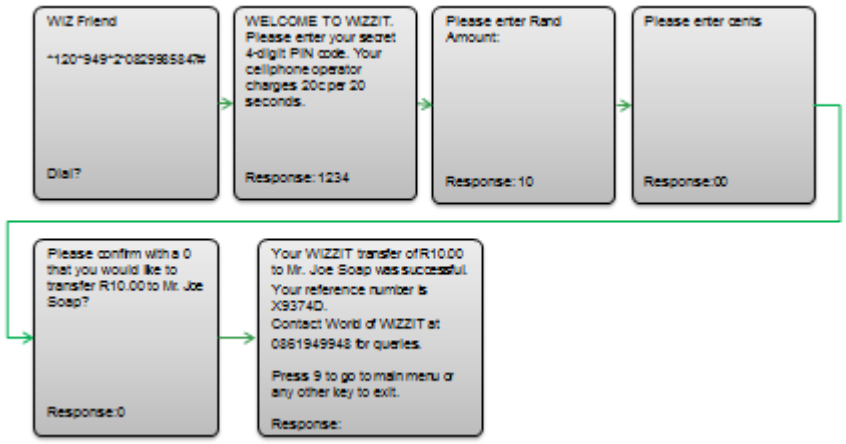

Figure 4.2: Defining a WIZZIT short code as a phone book entry

In this way, the payment is secured and although multiple beneficiaries can be loaded in the cellphone telephone book, each originating transaction must be authenticated by the cellphone banking PIN of the WIZZIT customer.

4.4 Enhancement of security through cellphone banking PIN

An unique feature of USSD as a cellphone banking channel is that no history of USSD interactions are stored in the memory of the cellphone. This feature allows the application to capture a cellphone banking PIN at the beginning of each cellphone banking session and protect the customer from a fraudulent third party that will search the history of the cellphone to obtain the customer cellphone banking PIN.

A problem related to the capturing of a cellphone banking PIN in USSD is that the characters of the PIN number are displayed in the clear during the capturing process on the screen of the cellphone. In other words, a second person overlooking a customer cellphone screen while he is capturing his cellphone banking PIN will see the number fully in the clear. WIZZIT address this security risk by educating the customers during the

registration process, that the person must never capture his/her cellphone banking PIN in front of other people on their cellphone. Customers must realise that the cellphone banking PIN is the key to provide access to their bank accounts and in banking the unbanked, WIZZIT educate the customer to ensure that his cellphone banking and card PIN always stay a secret to himself.

4.5 Different language support through the cellphone banking frontend

South Africa is known as the rainbow nation and is one of only a few countries in the world where there is more than one official language. WIZZIT has decided that as part of their customer service orientated approach that they will serve customers in all 11 official languages of South Africa. This philosophy was extended to the cellphone banking channel and WIZZIT became the first bank in South Africa to offer cellphone banking in all the official languages spoken in South Africa.

Figure 5.3 illustrates the steps that a customer would follow to change the language for the cellphone banking application on his phone. When the customer interacts with the WIZZIT cellphone banking service, the application determines the selected preferred language and during interaction with the service the application renders the screens according to the appropriate language tags.

This capability for various language support made it very easy to deploy the solution in different countries.

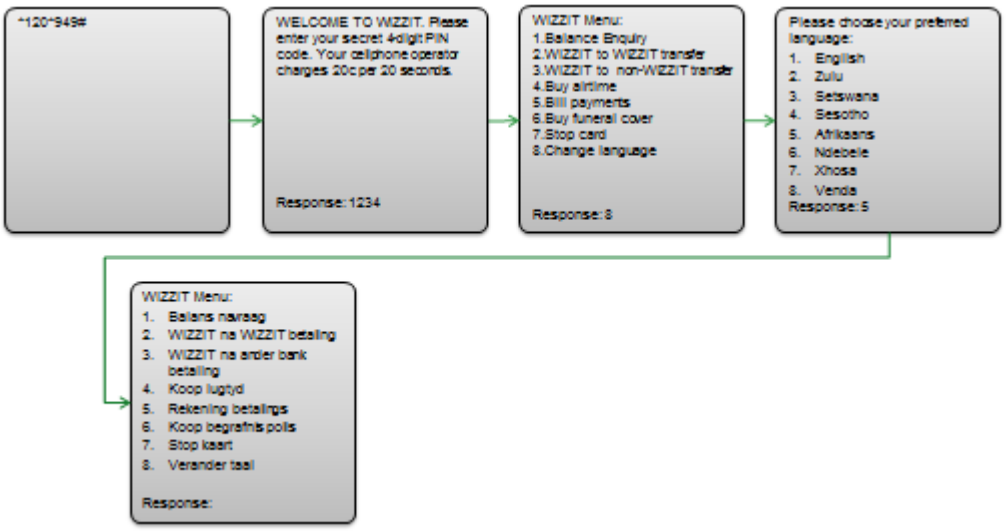

Figure 4.3: Support for different languages on WIZZIT Menu

4.6 Introduction of new bearer channels like WAP and JAVA

WIZZIT originally only offered a USSD customer interface, but as newer phones arrived on the market and GPRS speed increased, the support for JAVA J2ME and WAP applications became more relevant. The evolution of mobile data services from GPRS to Edge and the ability of 3G to support these GSM bearer channels influenced WIZZIT's decision to extend their offerings to both J2ME and WAP applications.

During the development of these new bearer channels, customer surveys revealed the need to keep the cellphone banking Menu layout the same for all bearer channels in order to avoid confusing customers by the different presentation layers. Both J2ME and WAP applications were designed to render the screens in the same way as the USSD cellphone banking application. The benefit of this approach was that the support for different languages was inherited by the new J2ME and WAP front ends. This approach has now become the technology architecture standard used by WIZZIT and the same approach is followed for implementing presentation layers in pilot projects for Android

and iPhone applications.

4.7 Conclusion of the WIZZIT approach

The WIZZIT cellphone banking offering was designed from the conceptualisation phase with the customer in mind in order to provide a user friendly and understandable product. Special attention and effort went into optimisation of the screens in a way that the customer can execute a transaction in a very short period of time to reduce cost of transactions through access to the GSM bearer channels. USSD was selected as a bearer channel due to its functional capability to reach every available cellphone in the South African market. Today, WIZZIT is known as the pioneer in reinventing the cellphone banking industry, with a successful model of delivering financial services to the bottom end of the pyramid.

WIZZIT is the only African company to feature in Monitor Group's published book "101 Innovation Breakthroughs" and is featured alongside very well known companies such as Google, Facebook, Coca Cola and Manchester United [33].

Chapter 5

Different types of cellphone banking approaches

5.1 Introduction

The original requirement of the cellphone was focused on voice communication that would allow connection mobility. It has become the single device that billions of people all find a necessity in modern life and it is expected that more than 7 trillion SMS messages will be sent in 2011 [15]. These figures indicate how the cellphone has become an integral part of our modern life style.

In South Africa, GSM technology was first demonstrated in 1993 by Telkom and in 1994 the first two cellular networks MTN and Vodacom were launched in South Africa [69]. A number of innovative GSM ideas were first launched in South Africa, such as the pioneering work from Vodacom to introduce data/fax services in 1994 to its customer base, making it the first mobile network in the world to offer the service [69].

As cellular networks evolved specifically around data offerings, new applications started to feature. At the same time the cellphone handsets progressed to more advance devices

that can support voice, data and fax services. Bill Gates, founder of Microsoft, had a vision that small handheld computing devices loaded with the Microsoft operating system will be used by people around the world as a daily tool to manage their lives. In November 1996, Microsoft released Windows CE (Compact Edition) to enter the Personal Digital Assistant (PDA) market [70]. Today, Smartphone devices are a reality and most people managed their diaries, e-mails, instant messaging and voice communication through their cellphones.

It was just a matter of time before the potential to use the cellphone for financial transactions would be realised and explored. As mentioned in Chapter 3, bearer channels like SMS, STK, WAP, USSD and J2ME can be deployed to enable financial transactions from the customer cellphone. STK applications were a preferred bearer channel in the early days of cellphone banking due to the added end to end security, but the available space on the 8K and 16K SIM cards to host the applications remained a challenge.

Gartner predicts that the number of cellphone payment users will surpass 141.1 million in 2011. According to Gartner, "In developing markets, high cellphone device penetration and low banking penetration creates favourable conditions for cellphone payments but players need to carefully plan their strategies. SMS and USSD will remain the dominant technologies in these markets, with money transfers and prepaid airtime credits driving transaction volumes. WAP will remain the mobile access technology of choice in developed countries" [20].

The cellphone banking space evolved in recent years to three types of approaches for launching a cellphone banking or payment application, namely:

- Bank led model
- Mobile Network Operator led model
- Combination of a Bank and Mobile Network Operator led model

The next few paragraphs will provide a short description of each of these three models.

5.2 Bank led model

In a bank led cellphone banking and payment solution, a bank decides to launch an application to the existing customer base of the bank. Typically, in the case of a bank led model, the cellphone banking application can be available through any participating mobile network operator in the country to the subscribers of this network. In other words, the offering will be mobile operator inclusive to all that would like to participate.

The bank utilizes the infrastructure of the participating mobile network operators to deliver the cellphone banking application to the bank's customers. In the case of a bank led model, there is usually a fully functional bank account behind the application where the currency value of the customer is stored and the cellphone banking application acts as an interface to the bank account. Banks can offer enquiry services as well as payment options through this channel.

5.3 Mobile Network Operator led model

In the case of a mobile network operator led model, a cellphone electronic wallet [80] is introduced to only the subscribers of the network. This type of implementation is mainly geared to deliver transactions for low value payments, money transfers and airtime purchases. Due to Know Your Customer (KYC) [96], Anti Money Laundering (AML) [71] and banking regulations, a bank needs to be involved in hosting the control float account of the total value of the combined cellphone electronic wallets. A potential customer that is not part of the mobile network will be required to join the network to participate in the cellphone electronic wallet solution.

Mobile network operators consider a cellphone electronic wallet solution as a method to reduce churn of customers away from them. The M-Pesa cellphone wallet launched through Safaricom and Vodafone in Kenya is the most successfully known network operator model. Subsequently Airtel, another mobile network operator on the African

continent, has launched their Airtel Money cellphone electronic wallet in a number of African countries and similar wallets are running in Philippines as G-Mobile and Smart Money.

5.4 Combination of a bank and mobile network operator led model

In the case of a combined bank and mobile network operator led model, a bank and a mobile network operator in a country combine forces to launch either a cellphone electronic wallet or a cellphone banking solution. In this approach, the potential customer must have a bank account with the bank but at the same time has to be a subscriber of the mobile network operator. The best known example of such an approach on the African continent is the MTN Mobile Money initiative that was launched by Standard Bank of South Africa and MTN South Africa in 2005 [26].

Unfortunately, this approach was not very successful in South Africa and the initiative was aborted in 2010. MTN Mobile Money projects on the African continent generate good transaction volumes and show the potential to be more successful than in South Africa.

5.5 Summary

The author strongly believes in the bank led model as the preferred cellphone banking application medium. The cellphone banking system can be designed in an user friendly way that has the potential to attract and retain previously unbanked people, turning the person into an economic citizen of the relevant country. Although the M-Pesa model in Kenya was mainly focused and implemented as a payment meganism, recent research has shown that the major need for their subscribers are a savings product to earn interest on

the money that is available in their cellphone electronic wallet. In Kenya this requirement identified by the market has led to the joint venture between Safaricom M-PESA and Equity bank to offer a savings product to the subscribers of the service. The service is known as M-Kesho and it was launched in May 2010 [61].

According to research done by World Wide Worx in 2011, 44% of cellphone users in urban areas of South Africa are currently using cellphone banking, compared to 27% in 2010 [130]. The increase in cellphone banking users will replicate across the African continent as more banks rollout cellphone banking applications. The reason for this is that internet access on the African continent is extremely limited but cellphone penetration is very high.

A big part of the evolution of cellphone banking is to expand activity towards payment solutions where customers have the functionality to make payments for goods and services with their cellphones. To support this extension of cellphone banking, a strong merchant strategy is necessary, including a set of common standards between different participants to enable these cellphone payments.

In the last few years, contactless card payments evolved dramatically and even extended to Near Field Communications [100] (NFC) pilots utilizing the cellphone as a payment device for small value payments. The NFC technology is expensive and will make it difficult to embrace as an affordable solution in third world countries. According to Gartner "developed countries are enthusiastic about opportunities in NFC, but mass market adoption is at least four years away, as service providers must first convince consumers to pay with cellphones instead of cash and cards" [65]. The author is of the opinion that NFC rollouts in rural Africa is at least another decade into the future, unless internet rollout to the uneducated masses explode overnight. The NFC technology is built on the card payment paradigm and the challenge on the African continent is that card payment acceptance is very limited. NFC technology only utilize the cellphone as a payment mechanism, but the lack of sophisticated internet links in rural Africa does not mean that Africa cannot develop alternatives to NFC in order to successfully address

the needs and requirements of the African continents user base.

Development of cellphone operating systems will introduce new bearer channels in future that will be different from the traditional GSM originated bearer channels. The evolution of data services on mobile networks will make it more economical to start introducing internet browser enabled cellphone banking and payment solutions. Currently incredible innovative cellphone banking applications can be delivered to iPhone, Android and Blackberry devices with their own device proprietary supported applications. The future predicted extensive reach of the open source Google Android mobile phone operating system will make it much easier to extend cellphone banking applications to the mass market. Unfortunately these growth predictions will take some time before it will be a reality to have Android Smartphone devices in the hands of the mass market.

The important lesson learned in the deployment of a successful cellphone banking application is to evaluate all the bearer channels available at the time and to utilise the bearer that will reach the largest number of cellphone handsets with limited interaction if any from the supplier of the service. A recommendation is to consider a cellphone banking platform that can support all existing and possible future channels.

Chapter 6

Cellphone banking arena

6.1 History of cellphone banking in South Africa

Banks used to be synonymous with branches as customers had to physically visit a bank branch to execute banking transactions. As part of the investigation on cellphone banking, cognisance needs to be given to the evolution of the banking industry over the last 30 years around the world.

Banks started to offer 24/7/365 banking in the mid to late 1980s with the introduction of the Automatic Teller Machine (ATM) [13]. Customers still had to physically visit these ATMs that were usually located outside a bank branch. The reason for this location was to allow the branch to load the ATM with money on a regular basis so that the service could be offered to customers after hours. The introduction of ATMs by the banking industry were considered ground breaking efforts in providing customers access to their bank accounts 24 hours a day.

In the 1990s, the Internet was introduced. Tim Berners Lee was the individual leading the development of the World Wide Web, defining the Hypertext Markup Language - HTML, the Hypertext Transfer Protocol - HTTP [86] and the Universal Resource Locators - URL. All these specifications and developments were made during 1989 to

1991 and Tim Berners Lee is known today as the father of the world wide web [14]. Banks started to realise during the mid 1990s that this could be a revolutionary delivery channel to bring 24/7/365 orientated banking to their customers.

In South Africa, all major banks introduced internet banking during the late 1990s, utilising clever marketing strategies to promote their new banking delivery channel. For example, ABSA at the time became an internet service provider that offered internet access services as an Internet Service Provider (ISP) free of charge for ABSA customers. Bundled into the internet services was ABSA's internet banking and this approach enabled ABSA to reach high volumes of internet banking customers. In July 2008, ABSA became the first bank in South Africa to reach 1 million internet banking customers [46]. Large sums of money, time and effort were invested by the banks in South Africa to launch great internet banking services to their affluent customers that had internet access at the time.

Vodacom was granted one of two GSM network licences in September 1993 and they opened their services commercially to the public on 1 June 1994 [3]. It is interesting to note that Vodacom's original business case was projected to reach approximately 250 000 subscribers within 10 years in South Africa. Within the first month of operation Vodacom attracted more than 50 000 subscribers and by October 1994 managed to double this figure to more than 100 000 subscribers. During 1996 and 1997 Vodacom developed the concept of prepaid airtime services and became the first network in the world to offer such a product [3].

MTN received their GSM South African network license in 1993 and launched their services in 1994. Today MTN is present in 21 countries with a subscriber base of more than 152 million people [45].

The introduction of prepaid phone services rapidly grew the customer base of both Vodacom and MTN in South Africa, and was favourably accepted by the poorer communities. Today South Africa has a 100% penetration level in cellphone reach [45].

During the early 2000's, both Vodacom and MTN invited the large South African banks to launch cellphone banking applications through STK applications. The STK cellphone banking services were limited to balance enquiry, mini-statement and inter account transfer transactions. The biggest constrains to these solutions were the physical memory space available on the 8 and 16 kilobytes SIM cards to store the cellphone banking application. These 8 and 16 kilobyte SIM cards were the industry standard at the time used by the mobile network operators to link subscribers to their network.

The STK cellphone banking applications had to be small in memory size and was downloaded to the SIM cards by sending an array of binary SMS messages to the customer cellphone over the air. This method of downloading the cellphone banking application OTA through binary SMS messages caused frustration to the end user customers because not all the SMS messages did always arrive on the subscriber handset. In these situations, the STK cellphone banking application would not install correctly and the customer could not use the application and the process had to be repeated.

The STK cellphone banking application interacted with the cellphone banking application server through encrypted SMS messages that made the execution of transactions very expensive to the end user. Some transactions required up to 5 SMS messages to complete and the end user had to pay for the transmission of these messages.

The customer acceptance of these STK based cellphone banking applications was disappointingly low and concluded in a failure of launching successful STK based cellphone banking applications in South Africa in the early 2000s.

The mobile network operators in South Africa enhanced their networks and introduced GPRS data services in 2002. MTN was the first network to launch GPRS services in July of 2002 [16]. Vodacom launched their GPRS data services in October 2002 [17]. With the introduction of GPRS services, new internet based services could be launched and the mobile network operators implemented WAP gateways. Again the major banks in South Africa explored these new GSM services and launched Internet browser based cellphone banking services. Most of these cellphone banking offerings were downscaled

versions of the banks existing internet banking applications and with the small screen of the mobile phone and slow speeds of GPRS services in place, this approach headed for another failure in launching successful cellphone banking offerings in South Africa. These cellphone banking solutions were focused on the more affluent customers that could afford the latest mobile handsets that supported internet browsing through the wireless application protocol.

In light of these unsuccessful attempts to launch a yet to be successful cellphone banking offering, an executive at one of the largest banks in South Africa mentioned to the author in 2004 that the idea of WIZZIT to launch a cellphone banking application for the unbanked is like mounting a horse that will never ride. This comment was based on the fact that the bank in discussion had more than 4 million customers at the time in South Africa and only 100 000 registered for their cellphone banking service of which only 10 000 used the service on a regular basis.

6.2 A new era for cellphone banking in South Africa

6.2.1 WIZZIT banking the unbanked

After two years of research and planning, WIZZIT launched a USSD based cellphone banking product in November 2004 mainly targeting unbanked people that had older phones. The USSD technology ensured that the application could work on these older phones. This was the first ever cellphone banking service in the world that used the USSD bearer channel and SMS notifications to reach unbanked people in a country. The launch of the service proved to be successful and in August 2005 WIZZIT reached 50 000 users that used the service at least once a month [21]. Another unique feature of the WIZZIT offering is the concept of using agents of the bank, called “WIZZkids”, to open bank accounts at the customer’s house or work place. These agents uses a cellphone based USSD application to complete the customer registration process. Today, this process is

known as branchless banking and there are various discussions around this concept for banks to extend their banking offering into rural areas.

6.2.2 FNB Cellphone Banking

First National Bank launched in the early 2000s a highly successful service that notifies customers about financial transactions processed on their accounts through SMS alerts. They named this service appropriately "InContact". Today it is known that they distribute SMS notifications to more than 5 million customers. First National Bank claim that they send out about 65 million "inContact" SMS notifications per month to their customers in all their subsidiaries in Southern Africa.

In May 2005, First National Bank of South Africa launched their latest entry to cellphone banking services that was based on USSD as bearer channel together with SMS transaction notifications. First National Bank spend large amounts of marketing costs on their new cellphone banking channel to reach their existing customer base and today they have more than 3 million customers using the service [8]. The launch of the FNB cellphone banking service through the USSD GSM channel embraced the WIZZIT approach to use a less secure but rather user friendly and far reaching cellphone channel like USSD.

In October 2009, FNB launched their cellphone based e-wallet solution [10]. This solution allows any FNB customer to send money from his normal bank account to any cellphone number in South Africa irrespective of the mobile network operator. The receiving person receives immediately an SMS notification informing him of the funds received in his FNB e-wallet. The customer can view his funds immediately by dialling the USSD code $*120*690\#$ from his cellphone. The most innovative feature of this FNB e-wallet solution is that the receiving customer can visit any FNB ATM, generate a reference number on the cellphone wallet application, capture it into the ATM and receive immediately money in cash without inserting a card into the ATM. With more than 4000 FNB ATM available

in South Africa, this solution is most probably one of the most convenient money transfer applications currently available in South Africa.

6.2.3 MTN Mobile Money

In 2005, Standard Bank and MTN brought a new approach to the market when they launched MTN Money in South Africa [26]. This was the first time on the African continent that a bank and a mobile operator put their strengths together to launch a cellphone banking application. This product was launched at the time to reach as well the untapped unbanked population of South Africa.

The MTN Money solution was deployed on a SIM Toolkit application and it was only offered to subscribers of the MTN Network. MTN customers with 8K and 16K SIM cards had to swap their SIM cards at MTN shops at their own cost in order to upgrade to 32K SIM card that had the MTN Money application embedded onto the SIM card. This required effort to first do a SIM swap proved a barrier for entry to the service, as the expense to the customer was in access of R100 to complete this exercise.

MTN Customers that had already 32K SIM cards could download the application through 17 binary SMS messages that had to arrive in sequence on the cellular handset to ensure the correct installation of the application. In many instances the download of the application did not work properly and MTN subscribers just ignored the service.

MTN and Standard Bank incurred large capital expenditure to market the solution in South Africa, but decided to aboard the MTN Money offering at the beginning of 2010 in South Africa due to limited success. MTN continued to deploy the solution in other African countries and it seems as if there is more success outside the boarders of South Africa, but it would be interesting to monitor the results for comparison to the experience in South Africa.

6.2.4 Nedbank

Nedbank participated with Vodacom and MTN in the early days to launch a WAP based solution with limited success. In 2007, they launched a new cellphone banking channel that was based on the USSD network but marketed it as SMS banking for the lower end of the market [47]. There is very limited information available on the success that Nedbank has achieved with the launch of this cellphone banking channel. It is known that Nedbank still uses their WAP cellphone banking application for more affluent customers that has higher end cellphone handsets.

6.2.5 Standard Bank

Standard bank also participated with Vodacom and MTN in the early days of cellphone banking to launch a WAP based cellphone banking application. The application had limited uptake and Standard bank launched in 2009 in addition to these efforts a USSD Cellphone banking application to the market. Information on the success of the Standard Bank cellphone banking applications is not available in the public domain. Standard Bank further launched in late 2009 through one of their subsidiaries in South Africa a cellphone wallet solution called “Mimoney”. This product is an cellphone electronic wallet based solution that can be used to buy goods and services. There were pilots with Mimoney and Ster Kinekor to purchase movie tickets, but to date there is limited information available about the success of this service.

6.2.6 ABSA

Although ABSA was very innovative in the launch of Internet banking and internet services, the same did not apply in their approach towards cellphone banking. ABSA followed the approach of the FNB “inContact” SMS service and launched a similar SMS notification service called “Notify Me”. ABSA participated with Vodacom and MTN to

launch a STK cellphone banking application in the early 2000s. In 2006 ABSA launched a WAP based cellphone banking application that was based on their internet banking channel and the presentation was scaled down to be accessible from cellular handsets.

In 2008 ABSA expanded the reach of their cellphone banking service through the introduction of a USSD based cellphone banking application. In 2010 ABSA launched an innovative money transfer service called "Send Money" that allows an ABSA customer to send money to another person with a cellphone number in South Africa. The receiving person will receive an SMS notification with redemption tokens that can be used at any ABSA ATM to receive the money in cash. This is a very similar approach to the FNB e-wallet solution and product.

6.3 Cellphone banking offerings in other parts of the World

6.3.1 Philippines G-Cash and SmartMoney

A number of successful cellphone payment applications were launched during the past few years in other parts of the world. G-Cash and Smart Money were launched in the Philippines in the early 2000s. Both these cellphone services were based on a cellphone electronic wallet offering that were predominantly used for payments at merchants. G-Cash and Smart Money spend great effort in building merchant networks that can accept their cellphone currency, leading to the successful acceptance in the Philippines for cellphone payments. Both these initiatives in the Philippines were driven by local mobile network operators and not by the banks in the country. The focus was to make payments easier by using a cellphone instead of bank cards or cash. The Philippines are known as one of the leading countries in the world that set the pace in cellphone payments [40].

6.3.2 M-PESA

In 2007, Vodafone launched M-Pesa in Kenya through their subsidiary mobile network operator Safaricom [37]. M-Pesa is a cellphone electronic wallet solution that needs an extensive network of merchants that can be used for Cash-in and Cash-out services. Cash-in is defined as the action for a customer to deposit money into his electronic wallet at any participating merchant. Cash-out is defined as the action for a customer to withdraw money out of his electronic wallet at any participating merchant.

M-Pesa in Kenya is today seen as the biggest success story of a cellphone electronic wallet application in any country of the world. The M-Pesa electronic wallet solution is based on a STK application that is embedded on the SIM card and transactions are processed through the WIG of the mobile network operator. Safaricom had at the time of the launch a market dominance of more than 80% of the Kenyan cellphone market [41]. The use of M-Pesa as a money transfer solution spread like wild fire in Kenya and today have more than 13 million registered customers.

Safaricom and Vodafone launched the M-Pesa service in Kenya to reduce churn of subscribers to join other mobile network operators in the country and today there are big question marks about anti-competiveness around the solution. Vodafone subsequently launched the service in Pakistan, Tanzania and South Africa. The M-Pesa service has very limited success in the other countries and it is believed that the market dominance of Safaricom in Kenya was the major catalyst for the success.

M-Pesa was launched recently in South Africa through Vodacom, a subsidiary of Vodafone, but banking regulations stipulated that only registered banks in South Africa may issue e-money [11]. To comply with this new regulation, Vodacom and Nedbank have joined forces to launch the South African version of M-Pesa. The M-Pesa service in South Africa had limited success by only registering around 100 000 customers in the first few months of operation that generated limited transaction activity [43].

Market indicators are that it will have limited success because the card payment infrastructure in South Africa is much more advanced than in countries like Kenya and Tanzania. There are more than 600 000 bank card point of sale devices in South Africa and more than 15 000 ATMs to access cash with a bank card. M-Pesa acceptance is very limited and potential customers don't see a need for the service to be used in the informal sector.

Recent research on the M-Pesa model in Kenya indicated an interesting factor. The biggest need of the users of the service was to save money and to receive interest on their deposit in the cellphone wallet. Mobile payment solutions on its own have limitations, but the combination of cellphone banking and cellphone payments has great potential if a deposit acceptance network of merchants can be provided.

6.3.3 ZANACO XAPIT solution Zambia

ZANACO is the largest commercial bank in Zambia with quite a number of branches available in the country. In 2007, ZANACO approached WIZZIT in South Africa to explore the opportunity to launch a similar "WIZZIT like" service in Zambia. ZANACO decided to brand the service as XAPIT pronounced as "ZAP IT" that imply speed of moving something.

Zambia has approximately a population of 11 million people and according to research done by Finmark Trust about 7 million people are bankable in the country. The shocking reality is that approximately just over 1 million people in Zambia today have a bank account. ZANACO's plan was to use XAPIT to reach to this unbanked population of the country and grow their customer base by means of this innovation.

Airtel is a mobile network operator with GSM networks in a number of African countries. At the time of the launch of the ZANACO XAPIT service in 2008, Airtel had approximately 80% market share of the Zambia cellphone market and MTN had just launched in the country. Airtel was the only mobile network that had a USSD Phase 2 gateway

in place at the time. ZANACO decided to launch a USSD cellphone banking application for Airtel customers and selected WAP and J2ME cellphone banking applications for the MTN customers. It was interesting to note the highly successful uptake of the product through both Airtel and MTN subscribers on different GSM channels. Statistics show that the ZANACO XAPIT cellphone banking customers conduct on average more than 10 transactions per month; this is perceived as an exceptional figure for a cellphone banking application.

Customers confessed that the XAPIT cellphone banking application changed their lives and the way that they have purchased services such as prepaid airtime in the past. Before XAPIT, they would have purchased airtime on a weekly basis but it usually happened that they used all the prepaid airtime available on the first day. With XAPIT, they can now buy in smaller value denominations airtime per day and that makes it much easier for them to control their talk time.

It is interesting to note that MTN customers in Zambia did not see the WAP and J2ME applications as an inhibiting factor to access the ZANACO XAPIT service. MTN has subsequently implemented an USSD Phase 2 gateway and the ZANACO XAPIT service is now offered to the MTN customers as well through the USSD bearer channel. Comparison of MTN Zambia XAPIT transaction volumes before and after the introduction of the USSD service indicated an increase in transaction volumes.

6.3.4 NMB Mobile Tanzania

NMB bank in Tanzania is one of the fastest growing banks on the African continent with an annually growth of approximately 400 000 new customers. The bank has a branch network of 108 branches throughout Tanzania and approximately 300 ATMs to serve their existing customer base of approximately 1.4 million customers. The existing ATM and branch network could not support the demand from the customers and the bank decided to launch a cellphone banking channel based on the same USSD interface used

by WIZZIT in South Africa.

NMB had a concerning problem with customers standing in queues in branches and at ATMs for basic banking functions like balance enquiries and transfers. The NMB Mobile service was launched in July 2009 in Tanzania and managed to triple the bank's transaction volumes within the first 6 months of operations [49]. The NMB Mobile service allows customers to do balance enquiries, person to person transfers, purchase airtime and prepaid electricity. Before these transactions were only available at the 300 ATMs, but today the customers can do this from the convenience of their homes on their cellphones. For simplicity, the bank decided to only rollout an USSD interface to their customers to make sure that the service has a huge uptake and to reduce the long queues in the branches and at the ATMs.

6.3.5 Google Wallet

Google also entered the cellphone payment space and according to the news website ComputerWeekly.com, Google has announced an application that turns mobile phones into a virtual wallet in partnership with Citi Bank, MasterCard, First Data and Sprint [7]. Google Wallet utilise NFC technology to allow a customer to swipe his cellphone at any MasterCard PayPass [42] accepted terminal for payments for goods and services. A customer needs to link his credit card details of a participating bank in the Google Wallet App on the phone. The phone needs to support the NFC technology and once a customer swipe the phone at a terminal, the Google Wallet will prompt the customer to select the linked Credit Card for the actual payment.

The Google Wallet vision is to be an open commerce ecosystem. The idea is that the customer will link eventually all the physical cards in his wallet into the virtual wallet in the Google Wallet App. The Google Wallet environment supports loyalty points and customers can receive vouchers from retailers that can be redeemed at stores.

Although the Google Wallet has great potential, it is very sophisticated and should

be considered rather as a first world solution. NFC technology is still not relevant in developing countries and the solution is built on the traditional plastic bank card paradigm. In Africa for example, card issuing and acquiring infrastructure is limited and for that reason the Google Wallet will not be a viable solution for payments for the foreseeable future.

6.3.6 Summary

It is an interesting observation that the four main banks in South Africa are now all offering cellphone banking through the USSD GSM channel. The subsequent launch of USSD based cellphone banking by the larger banks in South Africa embraced the approach introduced by WIZZIT. First National Bank is perceived as the dominant player in the cellphone banking market in South Africa with regular innovative ideas that are deployed to bring banking closer to people. Today, South Africa is known as one of the leading countries in the world that set the pace in the cellphone banking arena. In the rest of the World, the mobile network operator led model Vodafone M-PESA in Kenya is very successful but to date they have not manage to replicate the success in any other country.

Chapter 7

Conclusion

Cellular phone technology has evolved in the last decade from just a voice communication media to a daily tool that can be utilised for a wide variety of functions. These functions include listening to music, browse the internet, take pictures with the camera, use the Global Positioning System [84] (GPS) to get direction and more recently a tool for doing banking remotely. The banking industry explored the opportunity to expand their financial transaction channel offerings to cellphones with limited success in the early days, mainly due to complexity to reach the end user. STK were the first GSM bearer channel to be explored but the difficulty in downloading and maintaining the application on the end user phone restricted the success of this approach.

The WAP bearer channel was subsequently explored but due to limited support of proper web browsers on cellphones at the time combined with the slow speed of data services restricted the success of this approach. Today, with the increase in mobile data services, WAP is becoming a very relevant GSM bearer channel to consider for a cellphone banking application. A key consideration in a WAP cellphone banking approach is to keep the application simple and not to mimic an existing internet banking site. Firstly the screen of the cellphone is too small to guide around the site and the keypad of the cellphone is limited if you compare it to a mouse and a keyboard of a standard Personal Computer.

From a security point of view the introduction of SSL certificates through the internet browser onto the phone will assure end to end encryption.

The GSM USSD bearer channel was first used in 2004 for a cellphone banking application by WIZZIT in South Africa to reach the unbanked. Although USSD was initially part of the integral design of GSM networks, it was not immediately considered by banks due to the possible security risk in the lack of full end to end encryption. A great benefit of USSD is that it is a server side application that works on basically all GSM cellular handsets and this feature makes it an ideal channel for launching a cellphone banking application. The unbanked population of a country are normally poorer people that will use old entry level cellphones, and the USSD cellphone banking application works on the oldest of cellphones as well as the latest Smartphone devices available in the market.

Since the launch of WIZZIT in 2004, a number of new enhancements on GSM phone handsets took place. These include the introduction of Windows Mobile on Smartphone devices, the launch of the first iPhone, the wider usage of BlackBerry cellphones beyond corporate customer networks. In addition to these enhancements, the launch of Android from the Open Handset Alliance together with the first handsets supporting the new mobile phone operating system occurred. During all these enhancements and replacements over recent years, the WIZZIT USSD cellphone banking application stayed relevant and able to function perfectly on every new cellphone operating system or new cellular handset device. This experience proves the ubiquitous advantage of an USSD cellphone banking offering.

Today, all banks in South Africa that offer a cellphone banking application offer it as well through a USSD channel that proves that WIZZIT's visionary approach in 2004 was the right choice. To date, WIZZIT's technology has registered more than 1.5 million customers for its cellphone banking service in different countries and most of these customers come from the unbanked sector of the world population. The successful reach of WIZZIT turned the USSD bearer channel into the inherit standard to launch a cellphone

banking application worldwide. Quoting Gartner "Short Message Services and Unstructured Supplementary Services Data will remain the dominant technologies in developing countries" [65].

Cellphone banking has evolved on the African continent from just being an additional channel for banking to one of the new focus areas for the banking industry to extend their market segments. Today there is a wave of innovation on this front that was started by WIZZIT in 2004, followed by First National Bank in 2005 and in 2007 M-Pesa through Safaricom in Kenya launched the successful deployment of a cellphone electronic wallet solution. Today, the M-Pesa solution in Kenya has more than 13 million users and it is still growing [32]. Although the M-Pesa approach is a mobile network led model, it created a lot of interaction among banks in Africa and worldwide, and most of the banks are either considering the implementation of a cellphone banking solution or they are already in the process of doing so.

Cellphone banking has reached the African continent and is changing people's lives dramatically. The author was involved in a number of cellphone banking project launches in different countries. It is amazing to witness the excitement and passion when previously unbanked people start using their cellphone to do banking services, and discovering the steps into cellphone commerce by purchasing prepaid airtime or electricity from their cellphones in the comfort of their own homes. In Zambia the average number of customer cellphone banking usage per month is more that 10 transactions, this completely outnumber the average number of ATM withdrawals that average only 2 transactions per month.

The author is of the opinion that cellphone banking is busy changing the lives of a large number of people by bringing banking and electronic payments closer to them on a 24/7 basis. On the African continent there are 4 factors that stimulate the successful uptake of cellphone banking offerings:

- Low penetration of banking infrastructure

- Low income per capita
- Low internet penetration
- High mobile penetration

In a study from the analyst house Gartner, it was revealed that in 2009, 73.4 million people have used their phones to do cellphone payments. The 2008 figures were 43.1 million- and indicate an increase of 70% [64]. Based on these figures, Gartner predicts that the number of people making cellphone payments in 2011 will be 141.1 million [65].

Cellphone banking is becoming the preferred solution for banks to extend their banking offerings and it has the benefit to reach people that did not have a bank account before. The accessibility of cellphone banking will assist the growth of cellphone payments especially on continents like Africa where card infrastructure is limited or non-existent. The African continent has a great penetration rate of cellphones but a very low number of people are banked. This creates the opportunity for banks on the continent to extend their offering beyond their existing customer base to the so called unbanked market by offering them a cellphone banking solution. In this approach, the bank will go to the people instead of today's norm where banks expect customers to come to the bank.

In conclusion, cellphone banking at the bottom of the economic pyramid is a reality today, through the rollout of cellphone banking services to the mass unbanked population. Concluding in the words of Ramaphosa: "Provide a person with a bank account and you make that person an economic citizen of society".

Bibliography

[1] about.com. *Definition of Apps*. http://google.about.com/od/a/g/apps_def.htm.

[2] Statistics South Africa. *Mid-year population estimates 2010*. http://www.statssa.gov.za/publications/P0302/P03022010.pdf, 2010.

[3] africanwireless.com. *History of Vodacom*. http://www.africanwireless.com/vodacom_history.htm.

[4] Duncan Alfreds. *RIM eyes BlackBerry Africa growth*. http://www.news24.com/SciTech/News/RIM-eyes-BlackBerry-Africa-growth-20110929, Sep 2011.

[5] android.com. *Signing your applications*. http://developer.android.com/guide/publishing/app-signing.html.

[6] Answers.com. *Definition of unbanked*. http://www.answers.com/topic/unbanked.

[7] Warwick Ashford. *Google launches Google Wallet for NFC mobile payments*. http://www.computerweekly.com/Articles/2011/05/27/246801/Google-launches-Google-Wallet-for-NFC-mobile-payments.htm, May 2011.

[8] First National Bank. *FNB bags 3 million Cellphone Banking Customers*. https://www.fnb.co.za/news/archive/2011/20110527bags.html, May 2011.

[9] First National Bank. *FNB launches first Banking App in South Africa*. https://www.fnb.co.za/news/archive/2011/20110720app.html, Jul 2011.

[10] First National Bank. *FNB's eWallet shoots the lights out*. https://www.fnb.co.za/news/archive/2011/20110214ewallet.html, Feb 2011.

[11] South African Reserve Bank. *Position Paper on Electronic Money*. http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/PositionPaper/PP2009_01.pdf, Nov 2009.

[12] World Bank. *Mobile phone subscribers (% of total population) - South Africa*. http://www.google.co.za/publicdata/explore?ds=d5bncppjof8f9_&ctype=l&strail=false&bcs=d&nselm=h&met_y=it_cel_sets_p2&scale_y=lin&ind_y=false&rdim=country&idim=country:ZAF&ifdim=country&tstart=-287114400000&tend=1290722400000&hl=en&dl=en&icfg&uniSize=0.035&iconSize=0.5, 2009.

[13] Mary Bellis. *Automatic Teller Machines - ATM*. http://inventors.about.com/od/astartinventions/a/atm.htm.

[14] Mary Bellis. *The History of the Internet*. http://inventors.about.com/od/istartinventions/a/internet.htm.

[15] John Brownlee. *7 trillion SMS messages will be sent in 2011*. http://www.geek.com/articles/mobile/7-trillion-sms-messages-will-be-sent-in-2011-20101231/, Dec 2010.

[16] cellular.co.za. *MTN Launches GPRS in South Africa*. http://www.cellular.co.za/africa/south-africa/mtndatalive.htm, Jul 2002.

[17] cellular.co.za. *Vodacom SA launches GPRS*. http://www.cellular.co.za/news_2002/101702-vodacom_launches_gprs.htm, Oct 2002.

[18] MacCentral Chris Barylick, Mathew Honan. *iPhone release brings out the crowds.* `http://www.macworld.com/article/58682/2007/06/iphone_crowds.html`, Jun 2007.

[19] cnet.com. *Apple iPad launch day*, Apr 2010.

[20] Tamsin Cracknell. *Figures at your fingertips. Brainstorm*, 11:8, 2011.

[21] Ann Crotty. *WIZZIT has done its homework, says Mphahlele.* `http://www.nextbillion.net/archive/files/WizzitBusinessReport.pdf`, Sep 2005.

[22] dalvikvm.com. *Dalvik Virtual Machine.* `http://www.dalvikvm.com/`.

[23] developer.apple.com. *Code Signing Tasks .* `http://developer.apple.com/library/mac/#documentation/Security/Conceptual/CodeSigningGuide/Procedures/Procedures.html#//apple_ref/doc/uid/TP40005929-CH4-SW2`.

[24] John Staley Director Equity Bank Kenya. *Discussion regarding cellphone banking in Kenya*, July 2011.

[25] Ben Elgin. *Google buys Android for Its Mobile Arsenal.* `http://www.businessweek.com/technology/content/aug2005/tc20050817_0949_tc024.htm`, Aug 2005.

[26] finextra.com. *Standard Bank and MTN launch mobile banking JV.* `http://www.finextra.com/news/fullstory.aspx?newsitemid=14095`, Aug 2005.

[27] Finscope. *Finscope South Africa 2009.* `http://www.finscope.co.za/documents/2009/Brochure_SA09.pdf`, 2009.

[28] Mobile Payment Forum. *Risks and Threats Analysis and Security Best Practices Mobile 2-Way Messaging Systems.* page 46, May 2003.

[29] WAP Forum. *Wireless Application Protocol White Paper.* `http://www.wapforum.org/what/WAP_white_pages.pdf`, Jun 2000.

[30] Gemalto. *SIM Application Toolkit Description.* http://www.gemalto.com/techno/stk.

[31] Henny Rahardja Gottert and Colby. *World Bank WIZZIT film - Banking the Unbanked in South Africa*, 2007.

[32] Fiona Graham. *M-Pesa: Kenya's mobile wallet revolution.* http://www.bbc.co.uk/news/business-11793290, Nov 2010.

[33] Monitor Group. *101 Innovation Breakthroughs.* http://www.innovation-management.com/downloads/innovation_101_intro.pdf.

[34] gsm security.net. *GSM security questions.* http://www.gsm-security.net/gsm-security-faq.shtml.

[35] gsmworld.com. *GSM Services.* http://www.gsmworld.com/technology/services/index.htm.

[36] Puneet Gupta. *Short Message Service: What, How and Where?* http://www.wirelessdevnet.com/channels/sms/features/sms.html.

[37] Nick Hughes and Susie Lonie. *Mobile Money for the Unbanked.* http://www.changemakers.com/pt-br/system/files/InnovationsArticleonM-Pesa_0.pdf, Oct 2007.

[38] Architect Rabo Mobile payments Janse, David Jan. *Discussion regarding mobile payments at Rabobank in the Netherlands*, Sep 2011.

[39] Tracy Kitten. *Reaching the unbanked: Learning from South Africa.* http://www.atmmarketplace.com/article/133704/Reaching-the-unbanked-Learning-from-South-Africa-s-FIs, 2005.

[40] kpmginsiders.com. *Mobile payments in Asia Pacific.* http://www.kpmginsiders.com/pdf/Mobile_payments.pdf.

[41] Ignacio Mas and Dan Radcliffe. *Mobile Payments go Viral: M-PESA in Kenya*. http://siteresources.worldbank.org/AFRICAEXT/Resources/258643-1271798012256/M-PESA_Kenya.pdf, Mar 2010.

[42] MasterCard. *MasterCard Paypass*. http://www.mastercard.us/paypass.html#/home/.

[43] Duncan McLeod. *M-Pesa disappoints for Vodacom SA*. http://www.techcentral.co.za/m-pesa-disappoints-for-vodacom-sa/23167/, May 2011.

[44] mobilein.com. *Unstructured Supplementary Services Data*. http://www.mobilein.com/ussd.htm.

[45] mtn.co.za. *History of MTN*. http://www.mtn.co.za/ABOUTMTN/Pages/MTNSA.aspx.

[46] mybroadband.co.za. *Internet banking growth continues*. http://mybroadband.co.za/news/general/4634-internet-banking-growth-continues.html, Jul 2008.

[47] nedbank.com. *Nedbank introduces SMS banking, absolutely free for a year*. http://www.nedbank.com/website/content/mediareleases_group/mediareleases/media2007/mediaReleases_2007_06_27.html, Jun 2007.

[48] Jakob Nielsen. *Mobile usebility*. http://www.useit.com/alertbox/mobile-usability.html.

[49] nmbtz.com. *Launch of NMB Mobile*. http://www.nmbtz.com/index.php?option=com_content&view=article&id=123:launch-of-nmb-mobile&catid=41:top-headlines&Itemid=184, Jun 2009.

[50] Sam Oliver. *Apple forecast to lead 2011 smartphone shipments with 86.4M iPhones*. http://www.appleinsider.com/articles/11/09/06/apple_forecast_to_lead_2011_smartphone_shipments_with_86_4m_iphones.html, Sep 2011.

[51] openhandsetalliance.com. *Industry Leaders Announce Open Platform for Mobile Devices*. http://www.openhandsetalliance.com/press_110507.html, Nov 2007.

[52] C. Enrique Ortiz. *The Security and Trust Services API (SATSA) for J2ME: The Security APIs*. http://developers.sun.com/mobility/apis/articles/satsa2/#using, Sep 2005.

[53] pcmag.com. *Definition of IVR*. http://www.pcmag.com/encyclopedia_term/0,2542,t=IVR&i=45521,00.asp.

[54] pcmag.com. *Definition of short code*. http://www.pcmag.com/encyclopedia_term/0,2542,t=short+code&i=60145,00.asp.

[55] phonescoop.com. *Definition of Mobile-Originated Short Message Service*. http://www.phonescoop.com/glossary/term.php?gid=87.

[56] phonescoop.com. *Definition of Mobile-Terminated Short Message Service*. http://www.phonescoop.com/glossary/term.php?gid=261.

[57] phonescoop.com. *Definition of SMPP*. http://www.phonescoop.com/glossary/term.php?gid=257.

[58] C.K. Prahalad. The fortune at the bottom of the pyramid. Wharton School Publishing, 2005.

[59] Brad Reed. Android market share nears 50 percent worldwide. http://www.networkworld.com/news/2011/080111-canalys.html, Aug 2011.

[60] rim.com. *Research In Motion*. http://www.rim.com/.

[61] Jim Rosenberg. *M-PESA meets microsavings with Equity Bank deal in Kenya*. http://technology.cgap.org/2010/05/18/m-pesa-meets-microsavings-with-equity-bank-deal-in-kenya/, May 2010.

[62] SearchNetworking. *Home Location Register*. http://searchnetworking.techtarget.com/definition/Home-Location-Register.

[63] Victoria Shannon. *15 years of text messages, a 'cultural phenomenon'*. http://www.nytimes.com/2007/12/05/technology/05iht-sms.4.8603150.html, Dec 2007.

[64] Conn Stamford. *Gartner Says Number of Mobile Payment Users Worldwide to Increase 70 Percent in 2009*. http://www.gartner.com/it/page.jsp?id=995812, May 2009.

[65] Conn Stamford. *Gartner Says Worldwide Mobile Payment Users to Reach 141 Million in 2011*. http://www.gartner.com/it/page.jsp?id=1749114, Jul 2011.

[66] Daniel A. Tauber. *What is J2ME?* http://onjava.com/pub/a/onjava/2001/03/08/J2ME.html.

[67] Telecomspace. *Signaling System 7 (SS7)*. http://www.telecomspace.com/ss7.html.

[68] telecomspace.com. *Definition of USSD*. http://www.telecomspace.com/messaging-ussd.html.

[69] telecomspace.com. *GSM History*. http://www.telecomspace.com/gsm-history.html.

[70] Chris Tilley. *The History of Windows CE*. http://www.hpcfactor.com/support/windowsce/.

[71] Wikipedia. *Anti Money Laundering (AML)*. http://en.wikipedia.org/wiki/Money_laundering.

[72] Wikipedia. *Apple App Store*. http://en.wikipedia.org/wiki/App_Store_%28iOS%29.

[73] Wikipedia. *Application Programming Interface*. http://en.wikipedia.org/wiki/Application_programming_interface.

[74] Wikipedia. *BlackBerry*. http://en.wikipedia.org/wiki/BlackBerry.

[75] Wikipedia. *BlackBerry App World*. http://en.wikipedia.org/wiki/BlackBerry_App_World.

[76] Wikipedia. *Bluetooth*. http://en.wikipedia.org/wiki/Bluetooth.

[77] Wikipedia. *Central Processing Unit*. http://en.wikipedia.org/wiki/Central_processing_unit.

[78] Wikipedia. *Connected Device Configuration*. http://en.wikipedia.org/wiki/Connected_Device_Configuration.

[79] Wikipedia. *Connected Limited Device Configuration*. http://en.wikipedia.org/wiki/CLDC.

[80] Wikipedia. *Electonic Wallet*. http://en.wikipedia.org/wiki/Digital_wallet.

[81] Wikipedia. *First generation 1G*. http://en.wikipedia.org/wiki/1G.

[82] Wikipedia. *Fourth generation 4G*. http://en.wikipedia.org/wiki/4G.

[83] Wikipedia. *General Packet Radio Service*. http://en.wikipedia.org/wiki/General_Packet_Radio_Service.

[84] Wikipedia. *Global Positioning System*. http://en.wikipedia.org/wiki/Global_Positioning_System.

[85] Wikipedia. *HyperText Markup Language*. http://en.wikipedia.org/wiki/HTML.

[86] Wikipedia. *HyperText Transfer Protocol* . http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol.

[87] Wikipedia. *Integrated Development Environment*. http://en.wikipedia.org/wiki/Integrated_development_environment.

[88] Wikipedia. *Intelligent Network*. http://en.wikipedia.org/wiki/Intelligent_Network.

[89] Wikipedia. *Interactive Voice Response*. http://en.wikipedia.org/wiki/Interactive_voice_response.

[90] Wikipedia. *International Mobile Subscriber Identity*. http://en.wikipedia.org/wiki/IMSI.

[91] Wikipedia. *Java*. http://en.wikipedia.org/wiki/Java_(programming_language).

[92] Wikipedia. *Java Card*. http://en.wikipedia.org/wiki/Java_Card.

[93] Wikipedia. *JAVA Midlet*. http://en.wikipedia.org/wiki/MIDlet.

[94] Wikipedia. *Java Platform Micro Edition*. http://en.wikipedia.org/wiki/Java_Platform,_Micro_Edition.

[95] Wikipedia. *JAVA Servlet*. http://en.wikipedia.org/wiki/Java_Servlet.

[96] Wikipedia. *Know your customer (KYC)*. http://en.wikipedia.org/wiki/Know_your_customer.

[97] Wikipedia. *Long Term Evolution*. http://en.wikipedia.org/wiki/3GPP_Long_Term_Evolution.

[98] Wikipedia. *Mobile Information Device Profile*. http://en.wikipedia.org/wiki/MIDP.

[99] Wikipedia. *MSISDN*. http://en.wikipedia.org/wiki/MSISDN.

[100] Wikipedia. *Near Field Communication*. http://en.wikipedia.org/wiki/Near_field_communication.

[101] Wikipedia. *Non-repudation*. http://en.wikipedia.org/wiki/Non-repudiation.

[102] Wikipedia. *Over the air programming*. http://en.wikipedia.org/wiki/Over-the-air_programming.

[103] Wikipedia. *Personal Identification Number*. http://en.wikipedia.org/wiki/Personal_identification_number.

[104] Wikipedia. *QWERTY keyboard layout*. http://en.wikipedia.org/wiki/QWERTY.

[105] Wikipedia. *Second generation 2G*. http://en.wikipedia.org/wiki/2G.

[106] Wikipedia. *Secure Socket Layer*. http://en.wikipedia.org/wiki/Secure_Sockets_Layer.

[107] Wikipedia. *Short Message Peer-to-Peer Protocol*. http://en.wikipedia.org/wiki/Short_message_peer-to-peer_protocol.

[108] Wikipedia. *Short Message Service*. http://en.wikipedia.org/wiki/SMS.

[109] Wikipedia. *Short Message Service Center*. http://en.wikipedia.org/wiki/Short_message_service_center.

[110] Wikipedia. *SIM*. http://en.wikipedia.org/wiki/Subscriber_Identity_Module.

[111] Wikipedia. *SIM Application Toolkit*. http://en.wikipedia.org/wiki/SIM_Application_Toolkit.

[112] Wikipedia. *Smartphone*. http://en.wikipedia.org/wiki/Smartphone.

[113] Wikipedia. *TCP/IP Internet Protocol*. http://en.wikipedia.org/wiki/TCP/IP.

[114] Wikipedia. *Third Generation Partnership Project*. http://en.wikipedia.org/wiki/3GPP.

[115] Wikipedia. *Thrird generation 3G*. http://en.wikipedia.org/wiki/3G.

[116] Wikipedia. *Two-factor authentication*. http://en.wikipedia.org/wiki/Two-factor_authentication.

[117] Wikipedia. *Universal Resource Locator*. http://en.wikipedia.org/wiki/Url.

[118] Wikipedia. *Unstructured Supplementary Service Data*. http://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data.

[119] Wikipedia. *USIM Application Toolkit*. http://en.wikipedia.org/wiki/USIM_Application_Toolkit.

[120] Wikipedia. *USSD Gateway*. http://en.wikipedia.org/wiki/USSD_Gateway.

[121] Wikipedia. *Virtual Private Network*. http://en.wikipedia.org/wiki/VPN.

[122] Wikipedia. *WAP Gateway*. http://en.wikipedia.org/wiki/WAP_gateway.

[123] Wikipedia. *Web service*. http://en.wikipedia.org/wiki/Web_service.

[124] Wikipedia. *Wireless Application Protocol*. http://en.wikipedia.org/wiki/Wireless_Application_Protocol.

[125] Wikipedia. *Wireless Application Service Provider*. http://en.wikipedia.org/wiki/Wireless_application_service_provider.

[126] Wikipedia. *Wireless Markup Languate*. http://en.wikipedia.org/wiki/Wireless_Markup_Language.

[127] Wikipedia. *WIZZIT*. http://en.wikipedia.org/wiki/WIZZIT.

[128] Wikipedia. *X.509 certificate*. http://en.wikipedia.org/wiki/X.509.

[129] Wikipedia. *XHTML Mobile Profile*. http://en.wikipedia.org/wiki/XHTML_Mobile_Profile.

[130] World Wide Worx. *Cellphone banking surges*. http://www.worldwideworx.com/2011/02/03/cellphone-banking-surges/, Feb 2011.

[131] www.argospress.com. *Mobile Services Switching Center*. http://www.argospress.com/Resources/gsm/gsmmobilservicyswitccent.htm.

[132] www.cellular.co.za. *Anti Money Laundering (AML)*. http://www.cellular.co.za/wig.htm.

[133] www.wirelessdictionary.com. *GSM A3 algorithm*. http://www.wirelessdictionary.com/Wireless-Dictionary-A3-Algorithm-Definition.html.

[134] www.wirelessdictionary.com. *GSM A5 algorithm*. http://www.wirelessdictionary.com/Wireless-Dictionary-A5-Algorithm-Definition.html.

[135] www.wirelessdictionary.com. *GSM A8 algorithm*. http://www.wirelessdictionary.com/Wireless-Dictionary-A8-Algorithm-Definition.html.