
# ACCESS CHANNELS FOR MOBILE BANKING APPLICATIONS – A COMPARATIVE STUDY BASED ON CHARACTERISTICS

by

**FREDDIE SCHWENKE**

**Thesis submitted in fulfilment of the requirements for the degree**

**Master of Technology:** Information Technology

**in the Faculty of Informatics and Design**

**at the Cape Peninsula University of Technology**

**Supervisor:** Prof M Weideman
**Co-supervisor:** Mr J Janse van Rensburg

**Cape Town**
July 2009

# DECLARATION

I, Freddie Schwenke, declare that the content of this thesis represents my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

**Signed** **Date**

# ABSTRACT

The objective of this research project was to provide an answer to the question: "Which access channel is the most appropriate for mobile banking applications?" This question is posed by providers of mobile banking services and providers of mobile banking applications alike.

In order to provide an answer, a literature survey was conducted to determine

- which access channels are available to mobile banking applications and
- which characteristics should be measured to determine the appropriateness of each of these access channels.

It was determined that there are a number of access channels available to mobile applications. Not all of these are applicable to mobile *banking* applications, due to the nature of the underlying technologies.

In order to measure characteristics of the access channels a selection of the available channels was made. This selection was first based on the applicability of the channel on mobile banking applications, and thereafter on the availability of the channel in a commercial or test environment. Lastly, the list was filtered according to which channels that are available within South Africa. It was however possible to measure one of the characteristics, "ubiquity", in three different countries. Six access channels (IVR, Java/J2ME, SMS, USSD, WAP/XHTML and WIG) were chosen to be measured.

Apart from the selection of access channels, the characteristics that were to be measured were also filtered. This filtering was based on the complexity of the characteristic. Eventually, three characteristics (security, ubiquity and usability) were chosen.

Each of the characteristics was measured in a different way to determine the suitability of each access channel with regard to that specific characteristic. The results were gathered and graphed. A detail description of the results was done on a *per channel* basis. Lastly, the results were analysed. This analysis enabled the author of this research to make recommendations as to the appropriateness of the different access channels for mobile banking applications.

This interpretation of the results showed that WIG (which is representative of all SIM card based channels) is the most secure way to conduct mobile banking transactions. However, IVR and SMS were found to be the most ubiquitous and WAP/XHTML was the most usable. As far as usability is concerned, it was found that there is very little difference in the usability of the different access channels. It was also confirmed that the user's previous experience might have influenced his/her perspective of usability.

In conclusion it is recommended that no single characteristic should be regarded in isolation when decisions are made about which access channels to support. Instead, decision makers should consider several characteristics which may influence the target marketplace as well as prospective clients. The nature of the mobile banking application provider might play a significant role in the decisions. For example if the mobile operator is the service provider, they may consider access channels that are mobile operator dependent, but if a bank is the service provider, they might find it more useful to consider more ubiquitous access channels that are not mobile operator specific.

# ACKNOWLEDGEMENTS

**I wish to thank:**

For the development of this research thesis, the author would like to thank the following individuals/organizations, without whose help, this project would not have been possible.

- Prof Melius Weideman, my supervisor.
- Mr Hannes Janse van Rensburg, my co-supervisor and CEO.
- My employer, Fundamo. They assisted me in many ways, providing financial support, for study leave, knowledge retrieval and testing.

The financial assistance of the National Research Foundation towards this research is acknowledged. Opinions expressed in this thesis and the conclusions arrived at, are those of the author, and are not necessarily to be attributed to the National Research Foundation.

# RESEARCH OUTPUTS

Other research outputs produced by this author during and before the study are listed below.

## JOURNAL ARTICLES

| Authors | Title | Journal | Status |
|---|---|---|---|
| Weideman, M. & Schwenke, F. | The influence that JavaScript™ has on the visibility of a Website to search engines – a pilot study | Information Research – an international electronic journal | Published in July, 2006. |
| Schwenke, F., Weideman, M. & Janse van Rensburg, J. | A comparison of Mobile Access channels characteristics | Journal of banking and finance | To be submitted in April 2010 |

## CONFERENCE PAPERS

| Authors | Title | Institution/Event | Status |
|---|---|---|---|
| Schwenke, F. & Weideman, M. | Mobile application access channels – technologies, attributes and awareness. | 9th Annual Conference on WWW Applications (WWW2007) | Published in September 2007. www.zaw3.co.za |
| Schwenke, F., Weideman, M & Janse van Rensburg, J. | Mobile access channel characteristics – a comparison of security dimensions | 10th Annual Conference on WWW Applications (WWW2008) | Published in September 2008. www.zaw3.co.za |
| Schwenke, F., Weideman, M & Janse van Rensburg, J. | Measuring the ubiquity characteristics of mobile access channels – Africa and the United Kingdom | 11th Annual Conference on WWW Applications (WWW2009) | Published in September 2009. www.zaw3.co.za |

**SUPERVISOR:**

Signature: _____ Date: _____

Prof. M. Weideman

**CO-SUPERVISOR:**

Signature: _____ Date: _____

Mr J. Janse van Rensburg

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER 1

## INTRODUCTION

### 1.1 Overview

The purpose of this research was to determine which mobile access channels are most appropriate for mobile banking applications. It was clear that application providers in the mobile applications industry all had the same problem when they need to decide which access channels to support. It was found that there was little or no academic evidence to support claims of role players that specific channels are more appropriate than others.

This research was therefore aimed at providing evidence to support such claims and to guide decision makers towards making the correct decisions regarding access channels for their applications.

### 1.2 Research Problem

#### 1.2.1 Background

The author of this research learned that one of the most pressing questions in the mobile applications industry is that of access channel support. More specifically: "Which access channel should be supported by mobile applications?" Since this research was aimed specifically at mobile banking applications, the question was refined to: "Which access channel is the most appropriate for mobile banking applications?"

According to Janse van Rensburg (2007a), this is not a problem only for application providers, but also for role players such as mobile network operators (MNOs) and other cellular solution providers.

#### 1.2.2 Importance of mobile banking

According to Cho & Jung (2005) mobile banking is one of the banking channels that are being implemented by financial institutions in order to supply better services to their customers. They state that the advantages of mobile banking make it more advanced than

Internet banking. They further claim that mobile devices have the most advanced technology and that that is exactly what customers need. This seems to indicate that mobile financial services (mobile banking) is an important extension to existing banking services.

### 1.2.3 Statement of the problem

No academic evidence could be found that proves the claims made by some solution providers about relevancy of access channels to mobile banking applications. It seems that most claims are based on hunches or personal preferences. A comparison of the channels and measurement of the characteristics would enable solution providers to make claims based on academic research. Therefore, the research problem stems from the fact that there is no academic evidence for the claims about the suitability of access channels for specific mobile banking applications.

### 1.2.4 Research Objectives

The main objective of this research is to answer the question: "Which mobile access channels should be used in mobile banking applications?" In order to answer the question, a number of access channels were identified, as well as a number of characteristics. These could be used to measure each access channel. The data was collected to determine which access channel should be supported by mobile banking applications.

The answer to the question above will enable decision makers to base their claims about the appropriateness of access channels on academic evidence and data.

### 1.2.5 Research hypotheses

Four hypotheses were formulated for this research study. They are as follows:

$H_0$: No single channel can be regarded as the most appropriate for mobile banking applications.

$H_1$: SIM card applications (WIG & SAT) provide the most secure mobile access channels.

$H_2$: SMS is the most ubiquitous mobile access channel available.

$H_3$: Java/J2ME is the most usable mobile access channel.

In a pilot study done by Schwenke & Weideman (2007), it was confirmed that role players in the industry make claims that cannot be supported by academic evidence. The author of this research could not find any academic evidence that supports any of the opinions of the respondents to the questionnaire used by these authors.

## 1.3 Methodology

### 1.3.1 Literature Survey

A literature survey was conducted to determine the current state of mobile access channels and their characteristics. The main aim of the survey was to identify the access channels as well as the characteristics that may influence decisions about whether or not applications should support them.

The literature survey revealed a number of access channels that are available to mobile banking software. The characteristics that are important for mobile banking software also needed to be researched. The combination of the access channels together with the characteristics formed the basis of the research project.

A number of access channels were found, of which some are more applicable to mobile banking than others. At least one access channel was found to be a purely theoretical technology that does not seem to have been implemented in any production system. The following access channels were identified:

- BREW (Binary Runtime Environment for Wireless),
- Cell Broadcast,

- I-Mode,
- IVR (Interactive Voice Response),
- Java (J2ME – Java 2 Micro Edition),
- MExE (Mobile Execution Environment),
- SAT (SIM Application Toolkit),
- SMS (Short Message Service),
- USSD (Unstructured Supplementary Service Data),
- WAP (Wireless Application Protocol) & XHTML MP (Mobile Profile),
- WEB Clipping and
- WIG (Wireless Internet Gateway).

A number of characteristics have to be considered in mobile banking applications. This research measured some of these characteristics for the access channels. Measurements were done on each of the characteristics for each of the channels that were chosen. A number of characteristics were identified as being important.

Kreyer *et al* (2002) indicate that many people viewed their mobile phone as a payment device. Kreyer's research also indicates that respondents were more likely to use mobile payments rather than cash for payments in excess of €12.50 but less than €50. Below €12.50 cash was preferred. For amounts above €50, credit or debit cards were preferred (Kreyer *et al*, 2002).

Kreyer *et* al (2002) also lists three characteristics that need to be taken into account when assessing the acceptability of mobile payment applications. These are cost, security and convenience. As far as convenience is concerned, it is important to be able to use the application within different payment scenarios, e.g. m-commerce, e-commerce, stationary merchants and consumer-consumer. The list of characteristics was refined by the author of this research to include the following:

- cost,
- security,

- ubiquity and
- usability.

### 1.3.2 Research design

This research was designed in three distinct sections. The reason was that there were three different factors that needed to be measured individually to determine the applicability of the identified access channels. Each of the three factors was measured in a different way, based on the nature of the specific characteristic. However, all measurements were taken quantitatively. Three characteristics were selected to be measured, even though Schwenke & Weideman (2007) determined that there are four characteristics that should be measured.

The "cost" characteristic was excluded from this research due to its complex nature. The author of this research did consider measuring the "cost" characteristic, but found at least four aspects of cost that would need to be measured individually to reveal a complete cost measurement. Such measurements are heavily dependent on economic factors and would require considerable time to measure completely.

Therefore, the three characteristics that were measured were:

- security,
- ubiquity and
- usability.

Each of these characteristics were further investigated and divided into a number of dimensions or subsections that could be measured individually.

Six different access channels were selected based on availability within South Africa. These were:

- IVR,
- J2ME/Java,
- SMS,
- USSD,

- WAP and
- WIG.

Security measurements were taken based on literature and personal interviews. The characteristic was divided into three different dimensions that were measured individually and then summed to determine a total security measurement. The three different dimensions are:

- authentication,
- authorization and
- confidentiality.

Confidentiality was measured in terms of the how easy it would be for a fraudulent party to obtain transactional information during the execution thereof by the user. The measurement was therefore based on the level of encryption that was available for each access channel.

Even though it was found that, in the context of security, a number of other dimensions could be included, these chosen three were regarded as being influenced by the underlying technology of the access channel, as opposed to application design and other factors. Since the project was aimed at measuring the differences between the access channels, the other dimensions were excluded from measurement.

Each of these dimensions was found to have distinct levels and seven different levels were determined for each. Based on information available in the literature, each access channel was assigned a level for each of the dimensions.

Ubiquity measurements were taken to relate to the percentage of users that could be reached through a specific access channel. These percentages were of current mobile phone users. In order to measure ubiquity, it was therefore necessary to determine the market share of each of the MNOs (Mobile Network Operators) in a specific region. Furthermore, the ubiquity measurements were done in three different countries to make

the measurements more universally applicable. Different dimensions of ubiquity were identified that needed to be measured individually. These were:

- technology support,
- MNO support,
- handset support and
- SIM card support.

Market research was conducted to determine percentages needed for the ubiquity measurements.

Usability measurements were taken by means of a focus group and a set of heuristics. The heuristics were compiled from various sources that contained lists of heuristics for the measurement of usability. A new list of heuristics was compiled to measure only factors that were influenced by the underlying technology of each access channel. Application design was specifically not taken into account during these measurements. The measurements were conducted on all available access channels. These were:

- SMS,
- USSD (limited),
- WAP/XHTML and
- WIG (which is regarded to be similar to SAT).

Due to a technical problem, WIG could not be tested during the usability measurement.

### 1.4 Research data and analysis

The research data were gathered and graphed. Each of the characteristics was considered in isolation for the measurements.

## 1.5 Limitations

Some limitations were experienced during the course of this research project. Some existed at the start of the project, and others only came to light later on.

*Ubiquity* was measured in three different countries. These were:

- South Africa,
- Kenya and
- The United Kingdom.

The intent of the research was to measure the ubiquity characteristic by means of market research. A number of avenues were explored to gather the necessary data. These included email requests to specific network operators, to various Internet web sites and to personal contacts. Unfortunately there were still some data that could not be obtained. This research could not obtain data for the *handset dependency* and *SIM card dependency*. The results included *assumed* values for these aspects of ubiquity in order to show the influence that it would have if data could be obtained. The assumptions for these values were based on information available in the literature which indicated relationships between these dimensions and the others.

Initially the intent of the research was to do usability measurements on all six chosen access channels. However, at the time when the measurements were being done, one of the chosen access channels (WIG) was not available, while another one (USSD) was only available in a limited environment. Usability was therefore further limited by these constraints.

## 1.6 Chapter Layout

The rest of this research is laid out as follows:

- Chapter two contains a literature study that was conducted to identify the different available access channels and their characteristics.
- Chapter 3 describes the research methods that were used to collect the data.

- Chapter 4 contains the data that was collected as well as an analysis thereof.
- Chapter 5 concludes the research and provide suggestions about which access channels should be supported in mobile banking applications.

## 1.7 Summary

The purpose of this research was to determine the most appropriate access channel for mobile banking applications. In order to answer the research question in section 1.2.1, the access channels were identified and a selection was made based on availability of the channels within South Africa. Furthermore, measurable characteristics were identified in order to answer the question, based on scientific results. The characteristics were then divided into dimensions that could easily be measured individually. Combined results for each characteristic were obtained and conclusions were drawn.

It is important to note that the neither a dimension of any characteristic, nor a single characteristic should be considered in isolation. It is also important to ensure that a final decision on whether or not an access channel should be supported is not influenced purely by the measurements obtained in this research (or for that matter any claims related to these measurements). Instead the final decision should, by and large, be influenced by the specific needs of a current mobile payment/banking system. For example some systems may have higher security requirements than others, or, on the other hand, a specific implementation may be required to reach large numbers of subscribers and security may not be as important as in other applications.

Finally, the author of this research makes certain recommendations about the applicability of access channels. These recommendations are based on the results that were obtained during the project.

# CHAPTER 2

## LITERATURE SURVEY

### 2.1 Introduction

This literature survey was conducted around mobile applications in general and on mobile banking specifically. It was used to identify different access channels as well as the measurable characteristics. Furthermore useful information was found that assisted during this research project.

Section 2.2 describes E-banking (Electronic Banking) and shows that it can be seen as a grouping of a range of services. One of these is m-banking (mobile banking) (Karem, 2003:9). Others include: telephone banking, credit cards, debit cards and ATM's. The advantages of e-banking for both customers and financial institutions are listed by a number of authors. Even though there are no guarantees for the success of e-banking, there is little disagreement among authors that e-banking is an important banking option of modern times and and will become even more so in the future (Karem, 2003; Taddesse & Kiddan, 2005).

In section 2.3, the use of mobile phones is shown to have increased dramatically in the 1990's (Castells *et al*, 2004) and has continued to grow since. Mobile phones and other mobile devices are currently used for much more than just making phone calls. Younger people tend to make more use of the short messaging services. Male students are reported to use mobile devices for Internet access - mainly for weather and sports updates. Barkhuus (2003) adds calendar and mail functionalities to the list of common uses for modern mobile phones. A number of authors indicate that cultural differences may influence the way mobile devices are used, but there is general agreement that the use of mobile devices is still on the increase. Some authors even report that the design of websites is changing to allow them to be accessed by mobile devices more easily.

The adoption of mobile devices amongst users makes them ideal devices with which to conduct financial transactions. The “unbanked” masses of the developing world will be a

good marketplace for such m-banking services, since traditional banks are less available to these people. M-banking (see section 2.4) services experienced a slow start, because of a lack of interest from users (Riivari, 2005). It is, however, reported that once users got to know the m-banking services, they understood the value of the service better. One of the advantages of m-banking is the convenience of being able to access the banking services anywhere. A drawback of m-banking, however, is the perceived lack of security that is available when such services are used.

In order to find the most applicable way to access m-banking services, it is important that the possible technologies (channels) are identified. A number of these access channels exist and are described in detail in section 2.5. They are available to mobile applications in general and not specifically to m-banking services. The access channels are built on a variety underlying technologies.

Krugel (2007) categorizes the different access technologies as either *client-side* or *server-side* technologies. Consequently, characteristics needed to be identified against which to measure the access channels. These would enable the applicability of a specific m-banking application access channel to be measured. The different characteristics are described in section 2.6.

## 2.2 E-Banking

According to Doern & Fey (Undated:13), e-banking services are generally either replicating existing services electronically, or creating new ones. They name convenience, reduction of fees and better interest rates as possible ways in which e-banking could add value to existing services. Furthermore, they indicate that Internet penetration is important for e-banking services to be successful. These authors also state that a perceived lack of demand, high cost and security are the greatest deterrents for e-banking (Doern & Fey, Undated).

Anderson *et al* (1996) reported that one of the first possible applications for e-banking was the on-demand purchase of journal papers, as opposed to an annual subscription. These

authors reported that earlier e-payment (electronic payment) systems consisted of the buying of electronic coins or tokens. These tokens were then spent at merchants who in turn exchanged them for cash at banks. This process normally involved at least one form of digital signature.

Chau (2003:55) reported that e-banking was one of the first types of e-commerce (electronic commerce) to be used by SMEs (Small to Medium Enterprises). One way in which SMEs use e-banking, is for the relatively secure transfer of funds to other businesses. EFTPOS devices provide another way for SMEs to use e-banking for credit card payments. Learning how to use e-banking is characterised by a relatively flat learning curve. Technologies that require maintenance and support are usually installed and supported by the financial institutions.

Arunachalam & Sivasubramanian (2007) report that the recent growth of Internet based banking transactions is no guarantee that applications in this marketplace will be successful. Customer satisfaction is a key factor that will dictate the success of such applications. They list the factors that will influence user satisfaction. These are security, transaction accuracy, user friendliness and network speed.

These authors also define four forms of e-banking:

- PC (Personal Computer) Banking is a system where the user installs proprietary banking software on a PC. This software allows the user to access his/her account information.
- Internet banking is a system where the user accesses his/her account information via a web browser – either from a PC or a mobile phone.
- TV-based banking is a system where satellite or cable TV is used to deliver account information to a user.
- Telephone-based banking is a system where ordinary telephone and SMS messages are used to access account information. Ordinary telephones are generally used in conjunction with IVR (interactive voice recognition) systems.

These authors specifically note that electronic banking should be regarded as more than just banking via the Internet. However, the Internet is claimed to be currently the most widely used mechanism for electronic banking (Arunachalam & Sivasubramanian, 2007).

It seems that customers often use different e-banking channels simultaneously, and the challenge for banks is to deliver the right services through the right channels at the right time and in the right way. It is important that customers have the freedom to choose whichever channel that they feel most comfortable with. This choice of channel may be related to the type of business that needs to be conducted, cultural differences and legislation (Arunachalam & Sivasubramanian, 2007).

Internet banking offers great value to customers through the use of modern Internet technologies. These include the customization and personalization of services, more control over financial services, ease of use, convenience, speed and security. From a bank's perspective the main benefits are cost savings, the reaching of new market segments, efficiency, cross selling, third-party integration and customer satisfaction. The success of Internet-based banking services depends on the ability of a bank to attract and keep new customers (Arunachalam & Sivasubramanian, 2007).

Most e-payment systems are inadequate for micro payments. This is due to computational or communication burdens. Special systems are therefore needed to enable micro payments. It is fairly easy to ensure that digital currency is valid through the use of digital signatures: However, it is more difficult to ensure that the same digital currency is not used more than once. It is also difficult to ensure that such digital currency cannot be duplicated or reproduced with different values. (Jarecki & Odlyzko, 1997).

Micro payments normally involve very small amounts, often less than a cent. Communication, a computational overhead to ensure the validity of a transaction, is therefore very large in comparison with the value of the transaction. This makes it undesirable to validate each transaction with the issuer of the digital currency (Jarecki & Odlyzko, 1997).

Karem (2003:9) reiterates that e-banking is much more than just Internet Banking. This author claims that Internet Banking is probably the most widespread version of e-banking, but also lists the following types of e-banking:

- telephone banking,
- credit cards,
- debit cards,
- ATM's,
- mobile banking and
- digital TV banking.

Karem (2003:9) suggests that the last two are the most recent additions to the wider e-banking concept.

Siam (2006:1999) states that banking services need to be of high quality to satisfy sophisticated users that will not accept anything less than above average service. This author also indicates that, even though banks may suffer in terms of profitability or even suffer short term losses due to the introduction of e-banking, the long term results should all be positive. As a reason the author states the fact that technology is something that is here to stay (Siam, 2006:1999, 2003).

The above indicates to the author of this research that electronic banking is a very important part of the banking marketplace. Furthermore, it is likely that the importance of e-banking will increase in future. For banks to stay competitive in the marketplace, they will need to have some sort of electronic service available to their clients.

Many authors seem to agree on the importance of e-banking in the modern banking environment. They also agree that e-banking is more than just Internet banking. There are many advantages of e-banking to both the consumers as well as the financial

institutions that supply the services, but there are also limitations that need to be considered.

## 2.3 Mobile device usage

Mobile telephony services took off in the mid 1990s. At the beginning of the previous decade (around 1990), the ratio of mobile telephones to land line phones was about 1:34, with about 1:8 in 1995 and less than 1:2 in 2000. In 2003 the number of mobile phones overtook the number of land line phones. The usage of both technologies kept increasing, which indicates that mobile phones are not taking the place of land lines, but rather act as a complement (Castells *et al*, 2004).

As technology advances, mobile devices are decreasing in size and increasing their mobility and power. Pervasive computing is about convenient access to relevant information and applications. This should be supplied through ubiquitous, intelligent appliances with the ability to easily function when and where needed. Parallel to this is ubiquitous access to e-business services. These ubiquitous devices include mobile devices that use cellular networks and the services include financial services (Agoston *et al*, 2000).

The same authors reported in 2000 that there were 50 million mobile phone subscribers in Japan and 75 million in the USA. The growth of the Japanese service I-Mode reported by the same authors is an indication of the popularity of mobile devices and their usage. These authors also predict that in future Internet services will become more and more suitable for mobile devices (Agoston *et al*, 2000:8).

According to Chakraborty (2006:1), around 31% of the global population have access to mobile phones. This author distinguishes between India (as a typical developing market) and the USA (as a typical mature market). It is stated that in India, only 8% of the population but in the USA 69.8% of the population are using mobile devices. The same author implies that cultural differences have an influence on the way mobile devices are used.

Bachen (2001) reported that 43% of Americans have access to cellular phones while Barkhuus & Dey (2003) stated that mobile phones are the most widely employed ubiquitous computing devices. The fastest growing technology acceptance is that of mobile phones. Mobile phones are becoming more than just a communication tool, but are evolving into a tool for local social interaction. Initially mobile phones were used for business or security reasons. Almost all users did however report that their social use of the devices has grown rapidly (Chakraborty, 2006:3-10). Castells *et al* (2004) agree with Chakraborty (2006), but limit the technology growth to that of communication technologies. They further state that wireless communication technologies have profound social effects.

It is also reported that younger users (those under the age of 30) use text messaging for social communications. Indications are that text messaging is more prevalent among younger users, regardless of their cultural differences (Chakraborty, 2006:3-10). This is supported by Potts (2004:4) and this author further reports that as teenagers become adults (around the age of 20), the usage shifts from text messaging to voice calls.

Similarly, Bachen (2001) reports that American teenagers are increasingly using cellular phones to deepen relationships with their peers. It offers a great deal of freedom in building friendships. These devices also give parents a shorter leash on a child, since they can monitor the child's whereabouts. Some teens are reported to even turn in their cellular phones, because of this constraint.

Five distinct groups of younger users are defined. They are users who are:

- cost-conscious,
- safety/security conscious,
- dependent (reliant on his/her phone and feels disconnected without it),
- sophisticated and
- practical.

It is reported that differences in mobile device usage is mostly related to cultural factors. This also accounts for differences in adoption rates of mobile devices. In some parts of the world, e.g. Japan, the mobile device becomes an extension of the user's personal identity (Chakraborty, 2006:3-10).

According to Lipscomb *et al* (2007:47), mobile phones are becoming so popular that Americans are replacing their traditional land lines with mobile phones. They do suggest that one of the drawbacks of mobile phones is that their subscription is relatively costly.

While fixed line usage has been fairly stable (in 2002), mobile phone and SMS usage have increased rapidly. The number of subscribers in the USA increased from 0.7 million in 1986 to 115 million in 2001. Users are rating the mobility of their mobile devices higher than the speed of their fixed broadband lines (Odlyzko, 2002).

Potts (2004:8) reports that male students use mobile devices to access the Internet in order to get weather reports and sports updates. Cost, ease of use and availability are named as three factors that influence students in their use of mobile phones. This author further suggests that mobile phones will become even more common in the future.

Mobile devices are the most common mobile communication tools, but are becoming much more that just voice communication tools – they have evolved into information and data access terminals with multiple functions. Internet access, calendar, email and text messaging are examples of how modern day mobile devices are used. Mobile phones are described as "ultra mobile", because it is mobile enough to walk with while using it. The mobile phone makes it possible to maintain social relationships without being in face-to-face contact (Barkhuus, 2003).

It is clear to the author of this research that mobile device usage is expanding rapidly throughout the world. Because of the much more personal nature of mobile devices as opposed to desktop computers, it would make sense to utilize them for banking services. Younger users mainly use text messages while their older counterparts prefer voice

communications. One of the drawbacks of mobile devices is reported to be the fact that their usage is still relatively expensive when compared to traditional land lines.

## 2.4 Mobile banking

Anonymous (2007) reports that there is a market for mobile banking among the unbanked masses of the developing world. The biggest problem with mobile banking among the unbanked is the fact that many are still uninformed about the existence of the service. Another obstacle is the fact that they must still learn how to use the technology. They would also need to see the value for using mobile banking. The same author does however report that users are enthusiastic about m-banking once they start using it.

With the number of mobile phones at three times that of on-line PCs, the opportunity for mobile services is more evident than that for Internet based services. M-banking had a slow start in the marketplace, due to the fact that consumers were not interested. This was mainly because of the limitations of the devices and the high costs and slow speeds of transmission. The m-banking technologies have matured since and have become a fast, user-friendly and affordable service. With consumers becoming more used to mobile applications on their devices, m-banking is also accepted more easily by the consumers (Riivari, 2005). Krugel (2007) indicates that the early mobile payment systems are around 10 years old.

Traditional banking services come at a significant cost to the financial institution. They are best suited for developed markets where consumers and infrastructure are readily available. In developing markets, consumers have to pay the price in the form of banking fees. The fact that mobile solutions are much cheaper to set up, should encourage the bank to charge less for such transactions and this should ultimately lead to more transactions more often (Krugel, 2007).

Agoston *et al* (2000:3) describe wireless financial services as one of the *real* solutions that can be provided with the concept of pervasive computing, while Lipscomb *et al* (2007:46) suggest that mobile phones may be used as credit cards in the near future. Krugel (2007)

agrees that mobile banking is a good solution since the market penetration of mobile devices is far higher than any of the other self-help banking channels such as ATM's, POS and the Internet. Mobile banking (m-banking) is attractive since it is a convenient method for remote banking. However, security is one of the drawbacks that make this less attractive (Chikomo *et al*, 2006).

Mobile financial services are one of the most promising electronic services that are available. One of the reasons for this is the wide penetration of mobile devices (cellular phones). M-banking applications are suitable for a wide variety of financial services. Limited m-banking services are generally available, which cause m-banking to be mainly used for content payments. Since security has been an issue in m-banking, it is widely preferred for micro payments but not so much for macro payments. However, new security models have recently been developed, which makes it more acceptable for macro payments (Mallat *et al*, 2004:42).

M-banking is expected to become one of the most important types of m-commerce applications. Four categories of mobile payments are named in the literature. They are:

- micro payments,
- macro payments,
- remote payments and
- proximity payments.

These authors (Mallat *et al*, 2004:42) reduced these to two levels, which are:

- micro- and macro payments and
- remote and proximity payments.

A common way to charge mobile payments is to debit them against the user's monthly phone bill. There are advantages for the customers with this solution, which include the fact that no additional enrolment is necessary and it is widely available. Vodafone in the UK has such a service. Another solution is to charge the mobile payments to the user's credit card, and a third option is to provide a special *mobile* bank account from which

payments are made. A fourth solution is to charge m-payments as direct debits to existing bank accounts. The Dutch company Moxmo offered such a solution and verify the user PIN via an IVR call (Mallat *et al*, 2004:43-44).

In its simplest form, mobile banking allows users to receive SMS notifications of balances and in more advanced options, Java and WAP are used to provide a wider range of services (Mallat *et al*, 2004:44).

As reported by Pau (2004), the roles of mobile operators as money flow handlers increase in importance. They seem to be as efficient at collecting money as banks, which means that one of three scenarios is emerging:

- mobile operators play an increasing role in the m-banking industry,
- banks tie the banking operations tighter to themselves to protect their profits and
- partnerships between banks and mobile operators are established to supply the m-banking services.

Mobile devices as m-banking terminals are very attractive to users because of their convenience. Limiting factors are, however, *ease of use* and *technology*. Another problem facing providers of m-banking services is the ever growing number of mobile operators that need to be involved in the provision of the services (Pau, 2004).

The same author also lists a number of m-banking technologies currently in use, including:

- The use of SIM Toolkit (STK) technologies to support payments.
- Mobile operators that enable SIM cards as Visa payment cards.
- The use of credit cards as prepayment cards for mobiles.
- Payment clearing houses that allow mobile prepaid service reloads from mobile terminals with debit to bank accounts.
- Mobile phones and PDAs with card readers.

- The addition of a chip inside the terminal (device) which would carry debit, credit and loyalty cards and access codes. This would require a device capable of handling such a chip.
- The ability to transmit payment instructions from mobile devices to POS devices via Bluetooth.

Wireless technologies are fast changing the way financial services are designed and delivered. Banks introduce mobile banking systems in order to improve operations and to reduce costs. However, with less than 1.5% of banking transactions being conducted via mobile banking services, it seems as if consumers are slow to adopt. These figures were determined by the Bank of Korea in research that was conducted through their mobile channels in 2004. This is despite the fact that there were 7.3 million mobile subscribers (Lee *et al*, 2007). Janse van Rensburg (2007b) indicated that these figures dramatically increased during 2005 and 2006.

The author of this research is of the opinion that m-banking services will become more important in the near to medium future. The reason is that the m-banking marketplace has become more active in the past months. It is therefore important to investigate the possibilities that are available to m-banking services in order to support application providers with useful information.

Many authors seem to agree about the importance of m-banking and the fact that it is growing. There are some concerns about using m-banking such as security and cost, but solutions to these concerns are evident. At least one of the authors indicates that users become enthusiastic about m-banking once they start using it actively.

## 2.5 Access channels

There are a number of design and development constraints to consider during the development process of mobile applications (Mahmoud, 2004). Some of them are:

- devices generally have a small memory capacity,

- they have low powered CPUs,
- they have other kinds of input devices,
- they have small displays and
- network problems should be expected, since the networks are generally unreliable and the very nature of a mobile device increases the risk of a connection failure.

Mahmoud (2004) identified a number of technologies that are available for mobile applications and classifies them in two categories:

- browser-based applications – applications that use some kind of mark-up language and
- native applications – applications that are compiled and executed using some sort of runtime environment on the mobile device.

The same author also suggests that WAP and J2ME may be used together to provide solutions which benefit from both technologies.

Schwenke & Weideman (2007) identified a number of mobile access channels. They also show that not all access channels are necessarily applicable to m-banking applications, but that providers need to consider the different attributes in order to decide whether or not a specific channel needs to be supported.

A number of access channels have been identified from the literature, and are discussed below.

### 2.5.1 BREW (Binary Runtime Environment for Wireless)

The BREW technology, provided by Qualcomm, is a software layer between the device chip set and the applications. It is similar to the Java VM for J2ME. BREW is currently only available on devices with the Qualcomm CDMA (Code-Division Multiplexing Access) chip sets on CDMA networks. BREW provides APIs to embedded chip set functions

(Mahmoud, 2004). Mehrotra (2007) continues to describe BREW as the preferred environment on CDMA networks. The same author also indicates that BREW is gaining acceptance among developers in India.

BREW allows code written in a variety of programming languages to be executed on the device. It can also act as an extended platform for other environments like the Java VM. In addition it allows any type of browser to run on the device, e.g. HTML, WAP and cHTML. The VM extensions can be downloaded OTA (Over The Air) without any problems, and immediately allow the BREW client device to execute the applications that require them (Qualcomm, 2003).

The distribution system for BREW applications is controlled by the MNOs. They also control the billing system for these applications. BREW is also optimized to make use of the wireless communication system for communications between the client- and server-side applications. This allows subscribers to find applications that they want to install easily, since there is a single point of access to all applications – the MNO. This arrangement, however, also allow MNOs to choose which applications they are willing to distribute to their clients, which in turn requires application providers to negotiate with the MNO before they can distribute their applications (Qualcomm, 2003).

The download process for a BREW application requires a handshake between the device and the MNO server. This handshake enables the device to communicate to the server what it needs to run the selected application, e.g. the Java VM. The server will then send the required Java VM (if not already resident on the device) with the first application download. Subsequent applications that needs the same VM, will not receive the VM again. This technology allows the user to choose any application without ever needing to make "technology" decisions, like which VM to install in order to run the application (Qualcomm, 2003).

Even though BREW has many advantages, the author of this research is of the opinion that it may not play a major role in m-banking services. The reason for this is the fact that

BREW is not widely used and is exclusively bound to CDMA networks. Furthermore, it is an expensive process to develop and deploy BREW applications. Definite advantages to this technology include the ability to access low-level device attributes, which in turn gives higher security possibilities than on many other platforms. This does, however, also open up the possibilities of malicious attacks on the device. Based on Krugel's (2007) categorization, this technology is a *client-side* technology.

### 2.5.2 Cell Broadcast

Cell broadcast is a one-to-many SMS type service provided by the MNO. As opposed to the one-to-one SMS service which is the normal text messaging system provided on all GSM networks, this service sends the same message to all subscribers within range (Schwenke & Weideman, 2007).

This service is especially useful for location-based marketing services. Subscribers within range may then receive information about specials in a specific store. Other functionalities for this service include news services and traffic update services (Schwenke & Weideman, 2007).

Goel *et al* (2003) used cell broadcast technology for their proposed framework. It entailed the use of cell broadcast messages to inform vehicles of traffic conditions. They report that the technology to send cell broadcast messages is available, but that usually MNOs do not allow subscribers to access it.

Since this technology is limited to a one-way communication to the subscriber, the subscriber has no way to communicate back to the server via this technology. It is therefore not suitable for m-banking services. The author of this research can see the value of this technology in marketing applications where subscribers are informed about services and products. Based on Krugel's (2007) categorization, cell broadcast will fall within the boundaries of a *server-side* technology.

### 2.5.3 I-Mode

I-Mode is described as a very popular service which, amongst others, includes banking options. It is reported that this service grew from zero in early 1999 to about five million subscribers in March 2000. It is also described as a precursor to 3G services. Available I-Mode services can be divided into two major categories. They are:

- *practicality and convenience* services and
- *fashion statement and entertainment* services (Agoston *et al*, 2000:8).

Four major practicality and convenience services were supplied by the I-Mode technology in 2000:

- banking,
- travel,
- ticketing and
- e-mail

Other services emerged but were not as popular at that stage (Agoston *et al*, 2000:9).

The same authors identified six fashion statement and entertainment services:

- chakumero – a service that sells melodies for ring tones,
- music download,
- screen savers,
- animated characters,
- greeting cards and
- horoscopes.

Similar to an SMS service, I-Mode offers I-Mail, which pushes email messages straight to the mobile device. It allows users to write response email messages which are not limited to the 160 character maximum of an SMS message (Hellmund, 2003).

I-Mode seems to be failing and loosing ground at the moment. One of the reasons is the lack of content based on this technology. The problem around content is that content that is customized for I-Mode is not compatible with WAP browsers. Apart from this, specialized devices are needed to use this service. It does seem that I-Mode would still be dominant in Japan in the near future (Yoga, 2007).

I-Mode was developed as a domestic Japanese service. Since it was never really marketed outside of Japan, it was easily out-marketed by WAP over GPRS. The same author believes that I-Mode will remain the market leader in Japan for the near future (Yoga, 2007).

This technology is useful, but it has ubiquity limitations. It is available in Japan and websites need to be specifically adapted to enable devices to access it via this technology. The author of this research is of the opinion that m-banking services could be implemented successfully using I-Mode, but the limitation of the single country makes it unlikely to be a global player. It is however possible that existing services will be extended in a Japanese marketplace and specifically adapted to enable this technology as well. Krugel's (2007) categorization will place this technology in the *server-side* group.

### 2.5.4 IVR (Interactive Voice Response)

This system involves the replacement of a human speaker by a high-quality recorded interactive script. The respondent provides answers by pressing the keys of a touch telephone. It differs from traditional electronic systems in that the user does not read information but rather listens to it. Cellular phones can be used in IVR systems, therefore enabling it as a mobile access channel (Corkrey & Parkinson, 2002). The same authors reported that IVR applications were present mostly in health areas. They further stated that there was an increase in the use of this functionality in financial management systems.

Couper *et al* (2004) indicated that the type and gender of the voice used may have an impact on the responsiveness of the respondents. They even suggest that these two attributes may be one of the most important design decisions for the IVR channel. They further suggest that the specific voice may have an influence on the way the user reacts. This suggests that the usability of this channel may be influenced by the specific voice used. These authors found in their study that laboratory results on these issues differ from field research results. They do not suggest any reasons for these differences.

IVR is not limited to mobile phones. It is one of the oldest forms of mobile-banking technologies and is still in use today. The caller's phone (as forwarded by the telephone company) is often used as identification as well as a level of authentication. A requirement for this technology is that the service provider needs to have an IVR system in place (Krugel, 2007).

This is a useful technology that is easily adapted for m-banking services. The technology does have some usability limitations, though. The user is unable to see the results of his/her query. The user will therefore be forced be highly attentive when this technology is used by itself. This channel may however be useful as an add-on for another channel. Krugel (2007) categorized this technology as a *server-side* technology.

### 2.5.5 Java (J2ME – Java 2 Micro Edition)

J2ME is a subset of SUN Microsystems's Java environment with some additional APIs. It is specifically aimed at the consumer and embedded device market. An ever growing number of mobile devices already support J2ME. Two sets of configurations are usually found at implementation level. Those are:

- CLDC (Connected Limited Device Configuration) which dictated the Java VM (Virtual Machine) features and
- APIs that are supported and the MIDP (Mobile Information Device Profile) which provides domain specific APIs for user interface, networking, database and timers.

Special Java VMs (such as the KVM or Kilo Virtual Machine) are running on the devices to execute the J2ME applications (Mahmoud, 2004).

Setiawan (2001) supplies four reasons for the J2ME technology's success.

- The fact that applications can be dynamically delivered to users, regardless of the user's location.
- The fact that J2ME applications can be developed to be device independent provided that the developers do no make use of device specific libraries.
- J2ME provides a solid underlying technology for complex applications.
- J2ME applications can keep running on the device, even when the network is disconnected.

The same author indicated that security in J2ME applications is automatically built in for Internet oriented protocols like TCP/IP and SSL.

Even though the J2ME technology at its base is cross-platform, device manufacturers are often supplying their own proprietary APIs to enable device specific functions. This makes implementations more difficult and expensive, since different code bases need to be maintained (Hellmund, 2003).

Mehrotra (2007) indicates that Java is the leading technology in India with the greatest market penetration. The greatest advantage of Java over BREW is that it is much cheaper to develop an application in Java than in BREW. In addition to that, Java applications can run on GSM devices while BREW is limited to CDMA networks.

This technology is a rather useful one for complex applications. The author of this research predicts that m-banking services will be based on this technology in future. The technology has a high level of usability (as also indicated by Schwenke & Weideman (2007)) and adaptability. There seem to be some security concerns around a channel built on this technology, though. Currently there are a limited number of devices that support

Java, but that number is growing with each new model that becomes available. Java is promoted as a cross-platform language, which gives developers the opportunity to develop applications once and run them on multiple devices. However, device-specific libraries provided by device manufacturers may limit this advantage unless specific care is taken by developers. Krugel (2007) placed this technology in the category of *client-side* technologies.

### 2.5.6 MExE (Mobile Execution Environment)

MExE is an execution environment that enables multiple environments like WAP and Java. It is more than just a single environment, since it also incorporates location services, sophisticated menus and other interfaces. A variety of configurations is available. One requirement for this technology is the fact that it has to be configurable by the user (Schwenke & Weideman, 2007).

MExE enables full application programming. It also integrates location services, sophisticated customer menus and other interfaces, including voice recognition. It is likely that MExE will be built into 3rd generation UMTS phones (Thompson, 2000).

In addition to applications that execute on the handset, MExE allows the user to manipulate network services in a user-friendly manner. The security model of this technology allows the user full control over which services are allowed to be executed as well as the extent of permissions granted to the services. Four scenarios for the execution of services are presented:

- services that execute on remote services,
- application download to the MExE client,
- services downloaded to the MExE handset and
- MExE handset to MExE handset services.

In the first scenario the MExE client accesses the services executing on a remote server, which presents the content to the user. In the second scenario an application is downloaded to the MExE client and it then acts as a local browser through which the user can access the services on a remote server. The third scenario is when a user downloads and configures a service to the handset. This service may not require servers to execute it successfully. The last scenario is when two or more MExE handsets interact with one another without the necessity of servers that support the services (M-Indya, 2005).

The MExE server provides a means to negotiate terminal and network capabilities. Unfortunately, it is MNO dependent. The server provides a means to exchange capability and content. Capabilities include hardware changes such as an external keyboard or screen. The execution environment also forms part of this, e.g. some content can either use Java Applets or WAP. Content negotiation is about the best way to represent the content to the user. This may include conversions from standard protocols to their wireless equivalents. Personalisation information forms part of the content negotiations (Salmenjoki & Jantti, 2002).

MExE allows services in which two mobile devices can communicate without the use of MNOs or other third party MExE servers. It also enables the authentication of services and content that is downloaded. Furthermore the user can control which functions can be executed by that service or content (Salmenjoki & Jantti, 2002).

Salmenjoki & Jantti (2002) also define three class marks (which control the execution environment of the terminal).

- Class mark 1: WAP Environment – this is intended for devices with limited screens and keypads.
- Class mark 2: PersonalJava Environment – this is intended for more sophisticated devices that have colour screens and better input devices. This includes a MExE library for PersonalJava that allows support for networking protocols.
- Class mark 3: J2ME CLDC Environment – this is intended to resource constraint devices. It utilizes the J2ME environment.

It seems that this technology may be a good candidate for m-banking services. The adaptability in a device enables users to choose how they want the services to be delivered to them. The literature is unclear as to the ubiquity of MExE, but there seem to be security advantages.

Mitchell (2004) indicates that this technology is not yet available in any commercial products. The same author indicates that many of its principles are implemented by other technologies such as MIDP which is one of the components of the J2ME technology. Based on Krugel's (2007) categorization, this technology can be categorized as *server-side*.

### 2.5.7 SAT (SIM Application Toolkit)

This technology is based on a tool kit that is built into the GSM SIM cards. It is an ETSI/SMG standard for GSM services. It provides the SIM card with a proactive role in the handset and enables an interactive exchange of information between the mobile device and the network. Applications based on this technology are loaded onto the SIM card which can be notified of events and it can issue commands (Schwenke & Weideman, 2007).

The technology provides functionality for the SIM card. Applications are loaded onto the SIM card. It provides mechanisms which allow applications to interact and operate with compliant devices. These mechanisms include displaying text, sending and receiving SMS messages and initiating dialogue with the user (Claessens *et al*, 2001). These SAT applications use the mobile handset as an IO device (Hampe *et al*, 2000). Due to the fact that this technology was developed in 1994, it was suggested in 2005 that it has limited capabilities. More recent devices, however, are capable of a much richer instruction set than that available in SAT. It was also suggested that the Java technology overcomes these limitations (Schwenke & Weideman, 2007).

SAT provides security factors as follows: communication security is provided by standard GSM security and on the application layer, the SAT technology provides the security (Claessens *et al*, 2001). SAT applications use the MNO SMSC server as an intermediate server (Hampe *et al*, 2000).

This technology seems to be a subset of the WIG technology. It therefore has a more limited capability and possibly a more limited usability. It does seem to be more available than WIG, which would be an advantage when m-banking applications need to be deployed. Security is likely to be high in this technology, since it has access to the SIM card and other applications that are stored on it. Krugel (2007) categorised it as a *client-side* technology.

### 2.5.8 SMS (Short Message Service)

SMS was originally intended for signalling users of new messages in their voice mailboxes. It has evolved to a widely used communication channel among users (Hellmund, 2003).

This technology was developed for GSM networks. It is a store-and-forward service, which means that, if the receiving party is not available, the message is stored and sent to the receiver when he/she becomes available. This service can be used to trigger the delivery ring tones, graphics and other types of content to the user. Text messages can contain any type of information that needs to be delivered. The same author reported that SMS is growing as a payment medium, mostly through reverse billing and premium numbers (McKitterick, 2003).

SMS messaging is often seen as most popular among the 15-30 year age group. However, marketers and entrepreneurs are becoming more aware of its business capabilities. SMS short codes (five or six digit numbers) are becoming very popular. These codes are used by subscribers to request specific services, like weather updates or competition entries. One major advantage of these services is that the user initiates the request, without being spammed with information on his/her phone (O'Meara, 2007).

Kiyingi (2007) reports that SMS services can be quickly and cheaply deployed in rural areas for payment applications. The main reason for this is that the infrastructure is already in place. The ubiquitousness of the SMS service is one of the major advantages of this system.

In order to make the SMS technology work for mobile banking, the user sends an SMS to a specific number called a short code. These short codes are usually a shortened version of a phone number. The message needs to be structured specifically for the different kinds of transactions. The banking system will identify the user by the mobile number that is provided when the SMS arrives at the server. The result is then sent back to the user in the form of a normal SMS (Krugel, 2007).

The ubiquity of SMS (on all networks) will be advantageous when SMS is considered as an m-banking access channel. However, there are limitations in the security when using this technology. Another limitation is the limit on the number of characters that can be sent in one message, which could make SMS very expensive for the user. This concern may cause application providers to consider SMS not to be an option. However, in combination with another channel (like IVR or USSD), this technology may gain popularity for m-banking applications. Usability is likely to be limited, since the user may need to remember a complex set of text instructions in order to do m-banking transactions. Krugel (2007) categorized this technology as being *server-side*.

### 2.5.9 WAP (Wireless Application Protocol) & XHTML MP (Mobile Profile)

The WAP technology started out as a HDML (Hand held Device Mark-up Language) as proprietary solutions. The WAP work started in 1997. WAP applications are independent of device, user interface and network provider. As opposed to SAT which is GSM specific, WAP is more universal. WAP v.1.x is based on the WML (Wireless Mark-up Language), which also includes limited scripting functionality (Hampe *et al*, 2000).

In 2001, WAP was reported as the *de facto* standard for Internet content on mobile devices. Internet content is generally not designed for mobile devices, since it has not been designed with small displays and limited bandwidth in mind. WAP was designed to overcome these constraints. The WAP proxy translates the HTML content to WML content which is suitable for the mobile devices. Different bearer services can be used for WAP communications (Andreadis *et al*, 2001).

WAP applications are similar to desktop browser applications in the sense that they also use a mark-up language. Normal HTML is not appropriate for mobile devices, since it is too content rich, and the small devices do not have the ability to display all the content. Two existing technologies have been adapted for mobile devices: HTML was adapted and WML (Wireless Mark-up Language) was designed; and JavaScript™ was adapted and WMLScript was designed (Mahmoud, 2004).

WAP 2.0 is mostly XHTML MP based with cascading style sheets. XHTML MP offers better content presentation, but also borrows scripting and push capabilities from earlier WAP versions (Forum Nokia, 2007).

Although the WAP technology (categorised by Krugel, (2007) as server-side) by itself will probably not be a very good choice where m-banking is concerned, the newer version which includes XHTML MP may be a better option. There are concerns about the security, but generally speaking, it is not worse than that of a normal Internet banking channel. The author of this research is of the opinion that this technology will become one of the most popular m-banking access channels.

### 2.5.10 WEB Clipping

As described by Schwenke & Weideman (2007) this is a Palm (a specific hand held PDA device) proprietary technology. Similar to WAP, it involves a proxy that translates ("clips") normal Internet content and delivers low-bandwidth results to mobile devices.

The technology makes use of a browser *proxy* that delivers *clipped* content to the mobile device. The proxy browser *clips* the content by summarizing it and therefore reducing the size dramatically. Typically only text will be delivered to the mobile device. Images, text colour and other visual effects are usually ignored, because the device has a low resolution, monochrome display (Buyukkokten *et al*, 2000).

Gomes *et al* (2001) indicates that this technology is similar to a solution by AvantGo in that it requires special preparation of the web content beforehand. This limitation puts extra pressure on developers of web content and also adds to the maintenance cost of such content. They developed a hypothesis that web content become too cumbersome to read with these solutions. They confirmed it with the results of a questionnaire.

The limited ubiquity of this technology (Palm devices only) as well as the complexity of the proxy device (needed to *clip* the information), is likely to limit the popularity of this technology as an m-banking access channel. Furthermore, the technology does not allow for proper feedback mechanisms to the user, and by design allows for off-line browsing. The author of this research is of the opinion that this technology will probably not be used for m-banking.

Other technologies (such as OperaMini) enable a similar kind of technology on many more devices. The OperaMini browser is a Java (J2ME) program that users download to their devices. It then browses the Internet as if from a desktop and gives the user the ability to enlarge areas of the web page that they wish to see. The author of this research experimented with OperaMini and found that, while it is useful for displaying web content, there seem to be limitations in its ability to correctly handle secure data pages such as is required by banking solutions.

Based on Krugel's (2007) categorization, this technology can be grouped under *server-side* technologies. However, with applications such as Opera-Mini, which need to be downloaded to the mobile device, it becomes a *client-side* technology. This would then make this technology a *hybrid* technology based on Krugel's (2007) categorization.

### 2.5.11 WIG (Wireless Internet Gateway)

The WIG technology is similar to SAT. In both technologies, an application is loaded onto the SIM card and executed there. The WIG application is executed with a special SIM card application – the SmartTrust™ WIB (Wireless Internet Browser). The WIG server receives requests from the WIB and translates them into HTTP requests, which in turn are delivered to the application server. The HTTP response is translated back into a WIB script and sent back to the device. The message protocol is based on the SAT message protocol (Schwenke & Weideman, 2007).

This technology supports a *push* request via the WAP Push Access Protocol (PAP). Not all WAP PAP functions are supported by WIG. For those functions which are supported by WIG, the following steps are normally followed.

- The Push Client sends a push request to the WIG server.
- The server immediately responds to the Push client with an acknowledgement.
- The WIG server translates the request and sends it to the WIB.
- The request may contain a *GO* element which will in turn generate a request via the WIG server to the given URL (SmartTrust, 2003).

This technology is likely to be very useful for m-banking applications. Many m-banking providers are already using it in South Africa. The author of this research is uncertain about the ubiquity of this technology outside of South Africa. Apart from that, the technology needs to be supported by the MNO to be used. This may cause this technology to lose popularity in the m-banking world, but the available security is a definite advantage.

With the similarity between this technology and SAT, this would also be categorized under *client-side* technologies, based on Krugel's (2007) categorization.

### 2.5.12 USSD (Unstructured Supplementary Service Data)

McKitterick (2003) describes the USSD service as being used mainly for financial services like shopping and payments. The same author also indicates that the service is similar to SMS with the difference that during a session it has a real-time connection.

This technology is unique to GSM networks. The messages are routed through the user's home network, which makes it usable even while roaming internationally. All GSM phones support USSD messages. The dialogue between the mobile device and the network can be initiated from either side. The session continues until one side explicitly releases the dialogue. Since a session is established and kept alive while the dialogue continues, it results in smaller data packets, because the service code does not need to be transmitted with each message. Only one session is possible at a time between the device and the network (Schwenke & Weideman, 2007).

Hellstrom (2003) indicated that the GSM network has eight time slots. USSD used the first of these slots (together with SMS). This technology is available throughout the GSM network population. This makes it a very useful technology. It overcomes some of the usability and security concerns around the SMS technology and may therefore be a more popular choice when m-banking services are to be deployed. Krugel (2007) categorized this technology under *server-side* technologies.

## 2.6 Characteristics for access channels

Convenience, security, reliability and ease of use are essential attributes for the success of e-commerce applications (Chau, 2003:55). Three other factors will influence a user to use a specific application again: utility, usability and pricing. Utility refers to the usefulness of a specific application. Usability refers to a large extent to *ease-of-use* and pricing is important both for initial cost (download and installation) and *usage* cost such as subscription charges and traffic costs (Hellmund, 2003).

Schwenke & Weideman (2007) identified four characteristics for mobile access channels that influence their applicability to specific applications. These coincide with those identified by other authors to a greater or lesser extent. These four are:

- cost – also identified by Hellmund (2003),
- security – also identified by Chau (2003),
- ubiquity – also identified by Chau (2003) as a convenience factor and
- usability – also identified by Hellmund (2003). The utility factor identified by Hellmund (2003) also forms part of this and so does the reliability factor identified by Chau (2003).

Lee *et al* (2007) reported that "trust" (security) has a stronger influence on adoption behaviour than usefulness (usability) when mobile banking is concerned. The same authors report that "trust" (which is related to security) influences the perceived usefulness (usability) of mobile banking applications.

Talbot (2007) agrees with the other authors and also adds complexity to the list of the most critical issues for users of mobile devices. Cost seems to be the most critical, but usability is also high up the list. Security is also a concern, but mostly in terms of device loss, like theft.

### 2.6.1 Cost

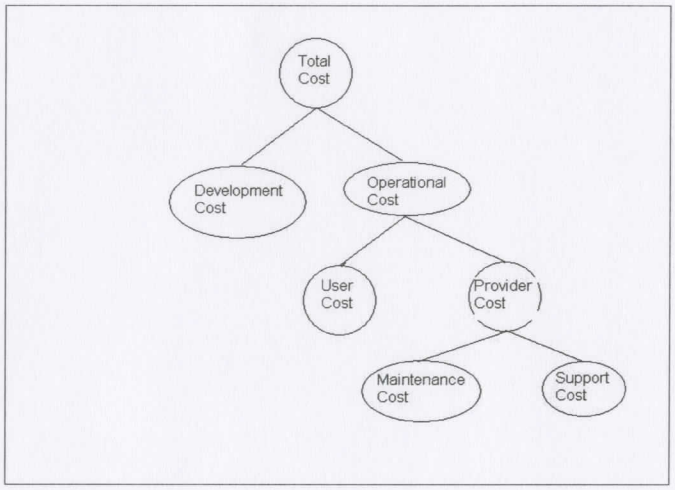
Chmielarz (2002:1580) reported that economic (cost) factors of e-banking are an important part of the success of e-banking applications. As a result of this, experts who use mobile applications, are calling for a value-based pricing structure as opposed to a traffic-based structure (Hellmund, 2003).

Traditionally, mobile network operators charge users on an "airtime" basis for usage. With data services becoming more important, this "airtime-based" model was not appreciated by users. I-Mode was the first packet-switched mobile service that started charging users

for data traffic and not airtime. This is noted as one of the critical success factors for I-Mode. Mobile network operators in Europe seem to have been reluctant to implement similar packet-switched data networks. The introduction of GPRS (General Packet Radio Service) in 2001 as the first volume-based price model, provided a solution to this problem (Hellmund, 2003).

The cost aspect involves a number of items which influence the total cost measurement. These aspects need to be measured individually in order to arrive at a total cost calculation for the channels (Schwenke & Weideman, 2007). Figure 1 shows the breakdown of the cost factor.

**Figure 2.1: Composition of the cost structure. Source: Schwenke & Weideman (2007)**




Even though this characteristic is likely to be one of the most important ones when an application is developed, its complexity is such that it will be nearly impossible to measure accurately. The author of this research is of the opinion that the study of this characteristic is likely to be a complete research project on its own.

### 2.6.2 Security

Claessens *et al* (2001) defines a number of security factors that need to be considered:

- authentication,
- authorization,
- message integrity,
- replay detection,
- sequence integrity,
- proof of receipt,
- proof of execution,
- message confidentiality and
- indications of security mechanisms.

The same author indicates that all GSM communications are secured at the communications layer by means of symmetric keys. Encryption algorithms are integrated into the devices as dedicated hardware.

SIM cards also contain a unique device identification code which uses challenge-response algorithms to authenticate itself against the host system. Trust relationships are also important for the success of m-commerce (Hampe *et al*, 2000).

Chmielarz (2002:1579) supports the fact that security in e-banking is a very important attribute. This author specifies two levels of security: the first is that of identification and the second is that of transmitted data.

Fischmeister *et al* (2001:2) emphasize that e-banking services require a high degree of security. They name the use of PINs (Personal Identification Numbers) and TANs (Transaction Authorisation Numbers) as the most common approach for service providers. They also describe the use of digital signatures as an alternative approach and further

describe the use of smart cards, which are highly tamper proof, as a means to provide security. Problems with smart cards include the fact that they are rather expensive, they are often limited to one application and special hardware is required to use them. A typical application of smart cards is the SIM card used by mobile devices in a GSM network (Fischmeister *et al*, 2001:2-3).

The level of security needed for a specific application will depend on the sensitivity of the data being transmitted (Mahmoud, 2004). This implies that an m-banking application may need lower security for certain kinds of transactions, which further implies that applications which only supply lower sensitivity transactions will need a lower overall security level.

A possible security flaw of the WAP 1.0 protocol is the fact that security data need to be translated at the WAP gateway. A possible solution to this problem can be found with banks (or other providers that need the higher security) providing their own WAP gateway (Hellmund, 2003).

OTA application provisioning is also a security concern. J2ME applications were originally transported over unencrypted HTTP connections. With MIDP 2.0, the more secure HTTPS protocol is used (Hellmund, 2003).

"Perceived risk" does not have a significant impact on the adoption of mobile banking applications, but "trust" does, and "perceived risk" impacts "trust" significantly. "Trust" also has a significant impact on "perceived usefulness", which also impacts the adoption of mobile banking. The "trust" factor is influenced by the user's trust of the bank, MNO and wireless Internet (Lee *et al*, 2007).

Trust will therefore probably be one of the most important factors to consider when m-banking services are deployed. The security concerns are high, especially with news about e-banking fraud that is reported on a regular basis. Measurement of this characteristic will therefore be important to assist providers of m-banking solutions in

decision-making about access channels. Some authors suggest that SIM card technology will be more secure than any of the others.

#### 2.6.2.1 Risks

Bezuidenhoudt (2008) indicate that many risks in m-banking are related to the ubiquity of the channel. E.g. the lower end handsets are more ubiquitous, but have fewer security capabilities as opposed to the higher end handsets with more security capabilities.

Bezuidenhoudt (2008) indicated furthermore that there are two distinct levels or categories of risks that have to be considered. They are:

- individual risk, which defines the risk to an individual using a mobile banking service, and
- business risk, which defines the risk to the financial institution providing the mobile banking service.

It is important to consider the differences between these two levels of risk when an access channel needs to be chosen. The amount of effort needed by a fraudster to exploit these different categories of risks is also substantially different.

Security measures are therefore needed to protect the individual user of the service as well as the business (provider of the service) against risks.

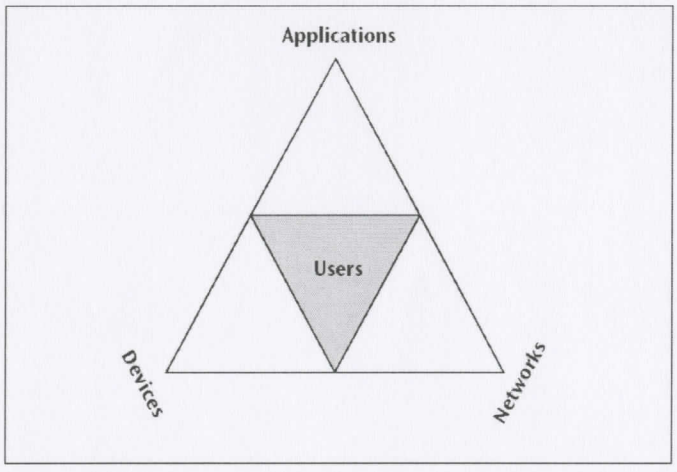
### 2.6.3 Ubiquity

Scholtz & Richter (2001) indicated that ubiquity involves the delivery of service in a physical environment. They mention the *where* and *when* existence of technology as different factors.

Hoffman (2007) indicated that the different access channels have different levels of ubiquity. This is a view that is supported by Ling (2007) that furthermore indicated that ubiquity is one of the most important factors that needs to be taken into account when access channels are chosen. Ling (2007) continued to indicate that this is especially true in developing economies. Ubiquity was also one of the characteristics indicated by Schwenke & Weideman (2007) as one that should be measured and taken into account when access channels are chosen.

Figure 2.2 indicates the four role players in a mobile application. Schwenke & Weideman (2007) define ubiquity as "the availability of a specific access channel, regardless of cellular network or mobile handset". It also shows these two factors, but adds "applications" to the equation. Schwenke & Weideman indicates that "convenience" may also be regarded as a factor in ubiquity measurement. Ling (2007) indicated that a factor of "MNO dependence" is a growing concern for application providers of financial applications. In a measurement of ubiquity, this will also have to be considered.

**Figure 2.2: Factors influencing the ubiquity of a channel. Source: Hellmund (2003)**




Ubiquity of an access channel may not be important to all marketplaces of m-banking applications. However, in countries where m-banking solutions are one of the only options for banking, this may be a great concern. Some of the reasons for m-banking being one of the only options, are as follows:

- in rural areas traditional banks are located far away and

- in some areas more traditional e-banking facilities are limited, e.g. no or limited Internet availability, or few people have access to a computer.

### 2.6.4 Usability

Arunachalam & Sivasubramanian (2007) indicate that usability is not a single dimensional property. They indicate five attributes that define usability, which are learnability, efficiency, memorability, errors and satisfaction. They derived a formal definition from the ISO 9241-11 (1998) standard as such:

*"The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use"* - (Arunachalam & Sivasubramanian, 2007).

Hellmund (2003) adds attributes from the IEEE definition to this to include the ease-of-learning aspect. The author adds that usability in wireless environments is more specific, since it needs to take the user context into account. Users in this environment are often in low-attention situations and the applications should be able to work there as well.

Schwenke & Weideman (2007) refine the definition. They define usability in terms of the quality of a system with respect to ease of learning, ease of use and user satisfaction. They further indicate that the measurement of usability can be done in terms of error rate and user perception while a user performs a specific set of tasks.

Personalization may very well be the difference between a usable and an unusable application (Hellmund, 2003). Fang *et al* (2006) contrasts the effectiveness of visual and auditory presentations. Auditory presentation is acceptable for shorter, simpler messages, while visual presentation should be used for longer, more complex messages.

Similar to ubiquity, the usability characteristic is also not always very important. In places where literacy is high, a limited usability may not be a problem, but lower literacy levels increase the need for higher usability. Users with lower literacy levels are also more likely

to be "unbanked" and therefore they will need an easy to use application in order to be more likely to adopt the technology.

## 2.7 Summary

The literature study revealed the following relevant facts.

- The importance of e-banking to the traditional banking marketplace. It is also clearly indicated by various authors that e-banking is much more than just Internet banking. It is further indicated that mobile banking (also called cell phone banking by some) forms part of this sector of the banking industry.
- The widespread usage of mobile devices, which could make them popular as banking/payment devices. It is further clear from the literature that users are using their mobile phones for more than just voice communications. The author of this research is therefore of the opinion that it would be quite natural for people to use their mobile phones for banking purposes – especially those that already use other forms of electronic banking services.
- The importance of m-banking solutions as a compliment to more traditional e-banking solutions as well as to the traditional banking marketplace in general. The adoption of mobile banking services is hampered by factors like knowledge about the existence and perceived security of the service. The author of this research believes that all these obstacles can be overcome and the industry can grow beyond them.
- The wide variety of access channels that is available to providers of m-banking applications. Of these access channels, 12 were identified and discussed. The suitability for m-banking applications differs from one channel to another. It is also suggested by previous research (Schwenke & Weideman, 2007) that the choice that service providers need to make about supporting these channels, cannot be made lightly. These authors suggest that decision makers need to take a number of factors into account when such decisions are made.
- The importance of the characteristics that will need to be considered when decisions are made about which of the access channels should be supported. Four of these characteristics were identified during the literature survey. These

characteristics will need to be measured for each of the channels in order to assign a proper "applicability" value to an access channel.

Krugel (2007) categorized the access channels in two categories. He named them *server-side* technologies and *client-side* technologies. He categorized six channels (of the 12 mentioned in this research). The author of this research categorized the other six similarly.

The 12 access channels that were identified can therefore be classified based on Krugel's (2007) categorization as follows:

- *Client-side* applications include
  - BREW,
  - Java,
  - MExE,
  - SAT,
  - WEB Clipping (depending on the specific environment) and
  - WIG.
- *Server-side* applications include
  - Cell Broadcast,
  - I-Mode,
  - IVR,
  - SMS,
  - WAP,
  - WEB Clipping (depending on the specific environment) and
  - USSD.

This author also indicated that SIM card applications (which include SAT and WIG) may involve additional cost to the MNO in order to provide the consumer with a SIM card that contains the application.

The author of this research concludes that some of the access channels that were identified will be more suitable to mobile banking applications than others. The characteristics available for each of the access channels are likely to influence its suitability when m-banking applications are developed.

The next chapter contains a discussion of measurement techniques for the various channels as well as the actual measurements that were done on them.

# CHAPTER 3

## METHODOLOGY

### 3.1 Introduction

This chapter describes the methodology used to do the measurements needed for this research. A selection of access channels was made based on their availability within South Africa. Then three different characteristics were selected to be measured for each access channel.

Each of the characteristics was divided into a number of different dimensions that could be measured individually. Different methods were used to measure each of the characteristics. They were:

- weighted parameters to measure security dimensions,
- market research to measure ubiquity and
- a focus group with heuristics to measure usability.

### 3.2 Research Hypotheses

$H_0$: No single channel can be regarded as the most appropriate for mobile banking applications – it depends on installation specific requirements.

$H_1$: SIM card applications (WIG & SAT) provide the most secure mobile access channels.

$H_2$: SMS is the most ubiquitous mobile access channel available.

$H_3$: Java is the most usable mobile access channel.

Role players in the mobile application industry agree mostly on these hypotheses. This was confirmed with a questionnaire that was conducted by Schwenke & Weideman (2007). Apart from that questionnaire, there is little empirical evidence of these hypotheses and, as those authors emphasized, the results of their research were based on opinions of people and not on scientific measurements.

## 3.3 Available Research Methods

Myers (2008) indicated that there are various ways to classify research methods, but that the most common distinction is between quantitative and qualitative methods.

### 3.3.1 Quantitative methods

Myers (2008) indicates that quantitative methods include survey methods, laboratory experiments, formal methods and numerical methods. These methods were developed in the natural sciences arena to study natural phenomena.

### 3.3.2 Qualitative methods

Qualitative methods, as opposed to quantitative methods, were developed to study social and cultural phenomena. Qualitative methods include action research, case study research and ethnography. Qualitative research data is collected through observation and participant observation, interviews and questionnaires, documents and texts and the researcher's impressions and reactions (Myers, 2008).

The same author indicates that there are three distinct underlying epistemologies for qualitative research methods. These are:

- positivist research, which assumes that reality is objective and can be described by measurable properties – independent of the researcher and his/her instruments;
- interpretive research, which attempts to understand phenomena through the meanings that people assign to them; and

- critical research, which is mainly used for social critique by which the restrictive and alienating conditions of the *status quo* are brought to light.

### 3.3.3 Triangulation

Coldwell (2007) defines triangulation as the use of different research methods to provide evidence. Originally triangulation was considered a combination of qualitative and quantitative methods (Myers, 2008), but it can also be a mixture of different methods within a single methodology. Myers (2008) indicates furthermore that most research studies are either quantitative or qualitative.

### 3.3.4 Measurement Methodology

Since this research was conducted by making tangible measurements, a quantitative methodology was chosen. A number of techniques were used to measure the characteristics of each of the access channels. Each of these characteristics was measured using a different measurement technique, the one that suited that specific characteristic the best. The technique used to assess the characteristic (security) was based on information obtained from literature and measurement values were deduced from that information. The technique use to measure the characteristic (ubiquity) was based on market information that was available in the public domain. The technique used to measure the third characteristic (usability) was based on data obtained in a focus group session.

### 3.3.5 Measurement of characteristics

In order to properly measure the applicability of an access channel to a specific type of application, it needs to be measured in terms of the characteristics that have been identified (see section 2.5). This section describes the measurement techniques that have been applied to measure each of the characteristics.

During the measurements, the SAT and WIG channels were regarded as technically equivalent, since both are based on SIM card technologies and the technologies for both are very similar. Therefore, the following conditions were assumed:

- In terms of security, they would have equivalent features and measurements taken for any one of the two, would be the same for the other.
- In terms of ubiquity, they would be similar, since both are heavily dependent on the MNO for support as well as specific features on the SIM card. They are therefore measured as if they are identical.
- In terms of usability, only WIG was measured, but it is assumed that SAT will have a similar measurement.

### 3.3.6 Cost

Schwenke & Weideman (2007) indicated that the cost measurement of a single access channel is rather complex. There are a number of factors to consider. The cost characteristic is considered complex due to the fact that at least four different aspects were identified for a complete cost measurement. These aspects are all dependent on current economic factors and therefore rather volatile. The time that would be required to measure cost would also be considerable. The comparison of the different access channels as far as cost is concerned, therefore, is considered outside the scope of this research.

### 3.3.7 Security

Mobile banking applications have a unique risk profile. This is because there are two unique features of mobile banking that do not exist in traditional e-banking environments. These are the mobile device and the mobile network (Bezuidenhoudt & Porteous, 2008).

Van der Merwe (2003) identified four possible attacks that may be suffered by on a transmitted message. They are

- interruption, which occurs when a message is interrupted and never reaches the intended destination,

- interception, which occurs when a message is intercepted and the content is therefore diverted and available to an unintended third party,
- modification, which occurs when the message is intercepted and modified before it is transmitted further to the intended destination, and
- fabrication, which occurs when a message is fabricated, based on messages that were transmitted earlier, and sent to the destination. This effectively means that the message did not originate from the source that the destination believes it to be from.

The main purpose of the security mechanism is to protect the messages from these attacks. Bezuidenhoudt & Porteous (2008) confirmed the existence of these potential attacks.

In order to measure the security capability of a specific access channel, one would need to understand what kind of security is required to make a banking transaction safe. Mobile communications are generally regarded as *in-the-clear* (not encrypted) because the data literally travels through the air. It is therefore supposedly easy to tap in and "listen" to the communications and even copy the data. This is however, not the case. GSM networks have strong security on their communication protocols and it would therefore take considerable effort to "listen" in on mobile communications (Krugel, 2007).

This author furthermore indicates that in order to "listen" in on mobile communications, a person would need to firstly know exactly where the consumer would be at the time of the call. The defrauder would also need to know the number of the consumer. He would then need to keep up with the consumer while the call travels from one base station to the next. After this, the defrauder would need to decipher the GSM encryption and identify the consumer, since the consumer data is hidden for privacy reasons.

The same author also indicated that even if a defrauder were able to "listen" in on the communications and identify the original user, in the mobile banking environment he/she would then be faced with normal velocity checks and transaction limits levied by the bank. It seems therefore not feasible for a third party to try and "listen" in on mobile communications.

Traditional fixed line communication data is generally not transmitted in an encrypted manner, while mobile communications data are always transmitted in an encrypted manner. This may not be sufficient for banking as it is still unencrypted data through an encrypted channel (Krugel, 2007).

The security characteristic of access channels can be further divided into sub components. These are explained below.

#### 3.3.7.1 Authentication

SearchSecurity.com (2008a) defined authentication as follows: "The process of determining whether someone or something is, in fact, who or what it is declared to be. (sic)" The author of this research refined this definition for banking transactions to: "Authentication is the process by which the financial institutions verify that the originator of a transaction is who he/she claims to be." The measurement of an authentication dimension would therefore measure the ability of a specific access channel to enable the bank to authenticate a consumer.

Wikipedia (2008a) identifies three types of authentication:

- something the consumer **has** (some form of token, e.g. a credit card or security token),
- something the consumer **knows** (e.g. password, pass phrase or PIN number) and
- something the consumer **is** or **does** (biometric identifiers like fingerprints or voice prints).

Often two of these classes are used together for authentication, e.g. a bank card together with a PIN authenticates an ATM transaction. Wikipedia (2008a) furthermore indicates that the U.S. Government's National Information Assurance Glossary defines *strong authentication* as follows: "Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information." This corresponds to the principle of "Dual-bearer" authentication as described in *section*

*3.5.2.5.* This is further supported by Arumuga (2006) that indicates that a multi-factor authentication increases the strength of the authentication mechanism.

Most mobile banking applications use a combination of MSISDN and a customer selected PIN to authenticate transactions. The MSISDN is usually provided by the SIM card in a mobile device and the user then supplies the PIN to verify that he/she is the owner of the SIM card. Furthermore the PIN should not be stored as a PIN but rather as a PIN Offset to minimize the risk of it being decrypted by fraudulent people. The same author recommends that the customer should be asked for certain elements of his/her PIN and not the complete PIN (Krugel, 2007).

A measurement of *authentication* would therefore need to be based on which authenticators (knows something, has something or is something) are used during the authentication process.

#### 3.3.7.1.1 Perceived rankings of authenticators

Adams & Sasse (1999) indicate that users often choose insecure passwords. This would indicate that a password is a rather insecure method of authentication. AuthenticationWorld.com (2006) seems to agree with this and adds that there are ways to make a password more secure, like: password length, type of characters and expiry of passwords. These authors also indicate that security tokens and biometrics have higher security levels than passwords.

Ratha *et al* (2001) indicate that biometrics offer the most secure form of authentication. These authors further indicate that exact matching of biometrics is nearly impossible. This is because pattern matching is used and different samples of the same biometric are seldom identical. In order to keep the FAR (False Accept Rate) and FRR (False Reject Rate) at acceptable levels, the system would need to be tuned. It should accept marginally non-identical patterns without being too lenient. Different applications may have different acceptable levels of the FAR and FRR. Since exact matching is almost

never used, it implies that a biometric may be supplied that is not coming from the actual owner and therefore even biometrics are not completely secure.

In order to enhance the security, multiple authenticators can be used, as mentioned before. As indicated by AuthenticationWorld.com (2006) the different authenticators may be used to gain access to different levels of data in an organization.

#### 3.3.7.1.2 Authentication Rankings

According to Schwenke *et al* (2008) there are three basic rankings of authenticators. As mentioned in 3.3.7.1.1, they are:

- something the user *knows* like a password;
- something the user *has* like a security token; and
- something the user *is* or *does* like a fingerprint or a voice print.

In casual discussions with various people in the mobile application industry, this basic ranking was confirmed. It was then suggested that any two authenticators would be stronger than any one authenticator by itself. Since different combinations of authenticators are possible, the relative strength of the combinations depends on the strength of the individual components. The relative strength of an authentication system can therefore be measured by knowing which one or which combination of authenticators are used during authentication.

Schwenke *et al* (2008) compiled a list of seven different ranks for authentication. O'Gorman (2003) indicated that biometric authenticators may not always be as safe as one might think. That author compiled a table that indicated the FMR (False Match Rate) and the FNMR (False Non Match Rate) for different authenticators. It shows clearly that some biometric (what the user *is/does*) are far less secure than others. The author of this research therefore divided the third authenticator into two subsections:

- strong (unlikely to be replicated) and

- weak (likely to be replicated) biometric authenticators.

The list of Schwenke *et al* (2008) was therefore refined with this in mind and Table 3.1 shows the results of this refinement. In a mobile application something a user *knows* will constitute a *password*, something he *has* will be a *SIM card* and something he *is/does* will be a voice print.

**Table 3.1: Summary of authentication values**

| Authentication Characteristics | | | | Authentication Value |
|---|---|---|---|---|
| User Knows | User Has | User Is/Does | | |
| | | Weak | Strong | |
| X | | | | 1 |
| | X | | | 2 |
| | | X | | 2.5 |
| | | | X | 3 |
| X | | X | | 3.5 |
| | X | X | | 4 |
| X | X | | | 5 |
| X | | | X | 5.5 |
| | X | | X | 6 |
| X | X | X | | 6.5 |
| X | X | | X | 7 |

The authentication value is determined by the position (top to bottom) in the table and is assigned based on the relative strength of the different combinations of authenticators. This table therefore implies that for single authenticators the following will be true in order of authenticator strength:

- User Knows < User Has < User is/does (weak) < User is/does (strong)
- Combinations of authenticators are always stronger than single authenticators
- (User knows) + (User is/does (weak)) < (User Has) + (User is/does (weak))

- (User has) + (User is/does (weak)) < (User knows) + (User has)
- (User knows) + (User has) < (User knows) + (User is/does (strong))
- (User knows) + (User is/does (strong)) < (User Has) + (User is/does (strong))
- (User Has) + (User is/does (strong)) < (User Knows) + (User Has) + (User is/does (weak))
- (User Knows) + (User Has) + (User is/does (weak)) < (User Knows) + (User Has) + (User is/does (strong))

#### 3.3.7.2 Authorization

SearchSecurity (2008b) defines authorization as follows: "the process of giving someone permission to do or have something." The author of this research refined this definition as follows: "Authorization is the process by which the consumer gives the financial institution permission to perform a specific transaction on his/her account." SearchSecurity (2008b) further indicates that authorization is logically preceded by authentication. This implies that a user is first authenticated and then he/she authorizes the institution to perform a transaction. However, in mobile banking applications, these processes are often happening in a single message from the consumer to the institution (Janse van Rensburg, 2008).

In order to measure authorization, one would need to measure the possibility of a user being correctly authenticated but a fraudulent authorization being received by the institution. This would typically happen in a case where a user is authenticated at the beginning of a session and a fraudulent agent then intercepts the transmission of valid messages and change it to benefit itself as opposed to the original, intended beneficiary. It may be possible to increase the authorization value of an access channel by changing the design of the back-end system.

Janse van Rensburg (2008) indicated that authorization is very important from the point of view of the financial institution. The institution needs to prove that the transaction executed was authorized by the real client and not someone that pretended to be the

client. From that perspective, it is therefore important to distinguish between authentication and authorization. Although authentication needs to happen logically before authorization, the closer the two can be together, the less likely is the chance of a fraudulent agent intercepting the authorization for its own benefit. Table 3.2 summarizes rankings compiled by Schwenke *et al* (2008) for authorization values that can be assigned to an access channel.

**Table 3.2: Summary of authorization levels**

| Authorization Characteristics | | | | Measurement Value |
|---|---|---|---|---|
| **Authentication** | **Encrypted Authorization** | **One session** | **One message** | |
| | | | | 1 |
| X | | | | 2 |
| X | X | | | 3 |
| X | | X | | 4 |
| X | X | X | | 5 |
| X | | X | X | 6 |
| X | X | X | X | 7 |

The measurement value was assigned by the position in the table (top to bottom). It was based on the relative strength of the authorization level.

#### 3.3.7.3 Confidentiality

Confidentiality of mobile banking transactions is achieved through encryption of transmitted data. Krugel (2007) identified three basic levels of encryption for data transfer.

The figures below indicate the encryption strength of different kinds of communication. The two parallel lines indicate encryption on a line level, while the boxes between the lines indicate encryption on a message level. Base stations, mobile operators and banks are

also shown. Dotted lines indicate unencrypted entities, while solid lines show encrypted entities.

**Figure 3.1: Unencrypted data over an unencrypted line (Krugel, 2007).**

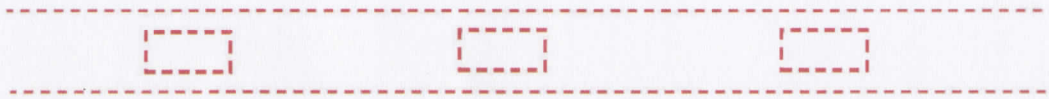


Figure 3.1 indicates the least secure form of data transmission. This is equivalent to a normal fixed line voice call or normal fixed line unencrypted Internet communications.

**Figure 3.2: Unencrypted data over an encrypted line (Krugel, 2007).**

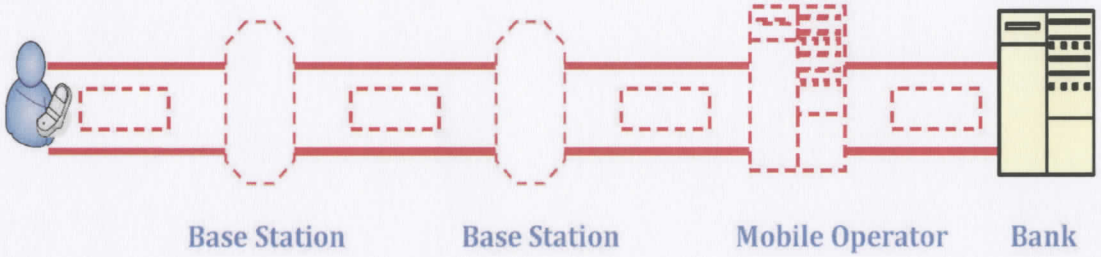
Figure 3.2 shows the form of data encryption that is generally available in Internet banking transactions. Clear data is transmitted over a line that is encrypted. Once the outer layer is bridged, the clear data is at risk.

**Figure 3.3: Encrypted data over an encrypted line (Krugel, 2007).**

In Figure 3.3 the most secure form of data transmission is depicted. The data needs to be encrypted at the start terminal and is then sent over an encrypted line. This is normally how banks transmit data via their traditional channels (ATM or POS).

The same author extended Figure 3.2 and Figure 3.3 to explain the encryption levels available for mobile access channels.

**Figure 3.4: Unencrypted mobile data over an encrypted mobile line with unencrypted hops (Krugel, 2007).**




Typical mobile data encryption, where the data is available at the base stations and the mobile operator in an unencrypted manner is shown in Figure 3.4. While travelling through the air, the data is protected by line encryption.

**Figure 3.5: Unencrypted mobile data over an encrypted mobile line with encrypted hops or storage (Krugel, 2007).**

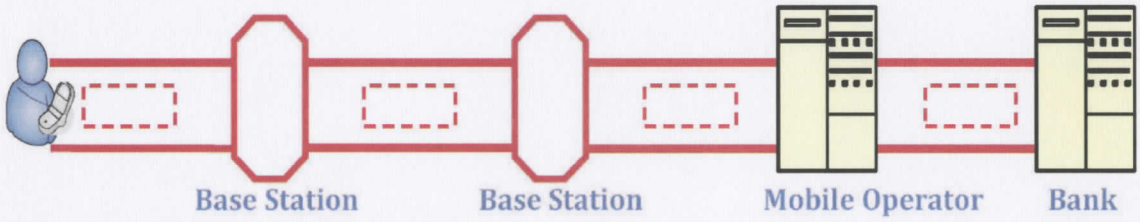
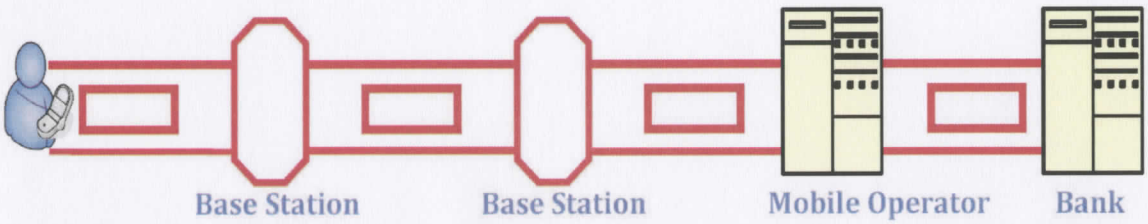



Figure 3.5 indicates unencrypted mobile data travelling through an encrypted mobile network. Note the fact that the data is never available without an external encryption layer. In this scenario it is usual not to store the data at the base stations or at the mobile operator, but if it is stored at those points it will be encrypted in some way.

**Figure 3.6: Encrypted mobile data over an encrypted mobile line with encrypted hops or storages (Krugel, 2007).**




The most secure form of encryption available to mobile data can be seen in Figure 3.6. It shows the flow of encrypted data over an encrypted line. It also indicates that the data is never available unprotected along the way. While passing through the base stations the data remains encrypted as well as when it passes through the mobile operator. This can only be implemented if the data can be encrypted at the handset before it is transmitted.

Furthermore the confidentiality of mobile data is protected by the GSM *protection of identity* protocols. This is implemented by the fact that the user identification is never transmitted over a GSM network. A SIM identification number is transmitted and a lookup at the MNO identifies the user. User data is added to the data at that stage before it is forwarded to the banking application (Krugel, 2007).

For the purpose of this research, a third party hop is defined as a machine or device which lies between the originators through which the message would need to pass in order to reach its destination. This machine or device may or may not store the data, depending on the type of message and protocol used.

A list of six encryption techniques, identified by Krugel (2007), follows:

- unencrypted data over an unencrypted line (Figure 3.1),
- unencrypted data over an encrypted line with no third party hops between the originator and the receiver (Figure 3.2),
- unencrypted data over an encrypted line with unencrypted hops between originator and receiver (Figure 3.4),

- unencrypted data over an encrypted line with encrypted hops between originator and receiver (Figure 3.5),
- encrypted data over an encrypted line with encrypted hops between originator and receiver (Figure 3.6) and
- encrypted data over an encrypted line with no third party hops between originator and receiver (Figure 3.3).

This is in agreement with Schwenke *et al* (2008). Table 3.3 summarizes the rankings assigned by those authors.

**Table 3.3: Summary of encryption values**

| Encryption characteristics | | | | | Measurement Value |
|---|---|---|---|---|---|
| **Line Encrypted** | **Data Encrypted** | **Encrypted Data Storage** | **Tamper proof keys** | **No Data Storage** | |
| *No encryption at all* | | | | | 1 |
| X | | | | | 2 |
| X | | X | | | 3 |
| X | | | | X | 4 |
| X | X | X | | | 5 |
| X | X | X | X | | 6 |
| X | X | | | X | 7 |

The measurement value was assigned based on the type of encryption that is available. The relative strength of encryption was taken into account and the groupings were ordered accordingly.

Transmission methods of data over a line with third party hops, is considered less secure that those without. In cases where these hops are unavoidable, the encryption levels offered by these third parties were taken into account. The reason for this is the fact that at each third party hop there is the possibility of data tampering or modification. Thus at those points fraudsters have an opportunity to break the encryption.

#### 3.3.7.4 Data Storage

Data sufficient to perform transactions should be stored in a central location wherever possible (e.g. server-side channels) and not be sent from the handset (Krugel, 2007). The author of this research is of opinion that this attribute is not relevant to the measurements of the access channels, since all GSM mobile communication is already protected by the GSM *protection of identity* protocol. The data that identifies the consumer is already stored at the MNO only, which in turn implies that identification data is not transmitted over the network.

#### 3.3.7.5 Dual-bearer Channel

Krugel (2007) further suggests that a dual-bearer channel should be used for a single transaction. This kind of authentication occurs when the user initiates a transaction from one channel (e.g. SMS), but is challenged for his/her PIN on another channel (e.g. USSD or IVR). This prevents possible spoofing. This dimension is not influenced by the underlying technology of the access channel, but rather by the applications design. It is therefore not measured. Typically one would prefer a more secure channel as the second authorization channel, but a channel would not be considered more or less secure because it can or cannot be used as a second authorization channel.

#### 3.3.7.6 Non-repudiation

Wikipedia (2008b) defines non-repudiation as "ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract". McCullagh & Caelli (2000) adds a digital element to this definition. They indicate two properties of non-repudiation in digital terms:

- an authentication service that provides proof of integrity and origin or
- authentication with high assurance that can be regarded as genuine.

These properties need to be verifiable by a third party.

Non-repudiation therefore provides a mechanism that prevents an individual from denying having performed a specific action. In a mobile banking environment, this means a consumer will not subsequently be able to deny having performed a specific banking transaction via his/her mobile handset. This dimension is primarily linked to the "authentication" dimension. The author of this research considers that non-repudiation does not to have any additional influence on the security characteristic of an access channel. It was therefore not measured as a separate dimension of security.

### 3.3.8 Ubiquity

Ubiquity measurements were done in three countries. It enabled the author of this research to ensure that the results were universal.

All ubiquity measurements were done as an indication of the subscriber population that can be reached with a specific technology. In order to get proper results, the market share of the different MNOs in each country was taken into account. The three countries selected were: South Africa, Kenya and the UK. Appendix A shows the market shares of the MNOs in these three countries.

As indicated by Schwenke *et al* (2009), the ubiquity aspect of the access channels can be divided into a number of smaller categories. Each of these should be scaled and measured in order to properly measure the ubiquity of any single access channel. Ling (2008) identified four of these dimensions that need to be measured separately. The same author also stated that the dimensions do not all carry the same weight. The relative weights that were assigned to the different dimensions are: *handset availability – 2*, *MNO independence – 1*, *SIM Card support – 1*, *technology support – 1*. The measurements for the dimensions are therefore scaled based on these weights. This is supported by Derballa & Pousttchi (2004) that indicate that ubiquity not only affects the accessibility of mobile services but also the reachability of the users. In addition they indicate that ubiquity affects the reaction time and convenience aspect of services.

#### 3.3.8.1 Handset Availability

This measurement covers the availability of handsets that support a specific technology (access channel). The larger the number of handsets that uses a specific channel, the better the ubiquity of that channel will be. This is supported by Chovanova, (2006) who maintains that a dependency exists between technology and support by handsets. Oliver & Barrett (2004) continue with this argument and add that compatibility issues between different handsets may be a much larger factor than it is with desktop PCs.

#### 3.3.8.2 MNO Independence

This is a measurement of the level of independence from MNOs. An access channel with less MNO dependence is considered more ubiquitous than one with more MNO dependence (Ling 2008). This view is shared by Bezuidenhoudt & Porteous (2008). Schwenke *et al* (2009) reports furthermore that MNOs and banks are often in competition about the ownership of the subscriber. This friction is reported to hinder access by the subscriber and hence the ubiquity of the channel.

#### 3.3.8.3 SIM Card support

SIM card support is important, especially for the access channels that rely on applications being loaded onto the SIM card. These applications are used in SIM card technology channels like WIG and SAT (Schwenke *et al*, 2009). This view is supported by Chovanova (2006) who indicates that users may need to buy special SIM cards to support certain applications.

#### 3.3.8.4 Technology availability

This dimension measures the availability of the underlying technology required to support a specific channel. As indicated by Ling (2008) it is of little use if the MNO supports a specific access channel, but it does not have the underlying technology to use the access channel in a commercial m-banking environment. Schwenke *et al* (2009) provide examples of technology dependencies for some of the access channels. These

technologies do not include the technologies incorporated in the handset, but only third party technologies such as gateways that are needed to enable the communications.

In some cases (e.g. MNO independence) the measurement cannot be done as an indication of which of the available networks support the named technology. In such cases the measurements was translated into a percentage of subscribers with access to this technology, given the restrictions of the dimension. Dimensions to which this translation is applicable are:

- handset availability, where the measurement was done according to the handsets that are currently in use;
- MNO independence, where the measurement was done according to the relative market share of the networks; and
- SIM card availability, where the measurement was done based on the SIM cards that are currently in use by the subscribers.

### 3.3.9 Usability

In 2005 it was reported that the measurement of usability in mobile applications is a difficult task. This is because many of the techniques used to measure usability are better suited to normal desktop computing. The special requirements of mobile computing often make these techniques unsuitable for mobile applications. The same authors report that task-centred simulation techniques are sometimes used in desktop computing, because tasks are well-structured and predictable. In mobile computing, these techniques fall short, because tasks are often unpredictable and unstructured. These authors therefore propose a heuristic approach which requires limited human resources and is effective in detecting usability problems (Bertini *et al*, 2005).

Coursaris & Kim (2006) indicate that a central theme in usability studies is the ease with which users can employ a particular technology in order to achieve a particular goal. These authors identified 11 *usability dimensions* of which three were identified as major dimensions. They are effectiveness, efficiency and satisfaction. These authors also

indicated that there are challenges and limitations to mobile devices that make standard usability studies less applicable. They listed the limitations and challenges which are related to the characteristics of mobile devices, as:

- small screen sizes,
- low resolution displays,
- non-traditional input methods and
- navigational difficulties.

These authors furthermore indicated that the challenges cause usability issues to be particularly important for mobile technologies.

Garzonis & O'Nell (2006) suggest that the reason for low usage of data services on mobile devices is because users are too frustrated with the applications. They indicate that users refuse to use services if the frustration rate is higher than the perceived value for using the services. These authors also maintain that one large difference between using services on a desktop PC and a mobile device is finding out how to access the services. On a PC the software is more than likely familiar, because it has been personally installed by the user, while the variety of ways of accessing services on a mobile device is often confusing to the end user. These authors continue to highlight the *context* within which the service is used as a factor that might influence the usability perception of the application.

#### 3.3.9.1 Evaluation of Usability by means of heuristics

Bertini *et al* (2005) identified the following set of standard heuristics for evaluation of the usability of a system.

- *Visibility of system status* – this rates the way the system keeps the user informed.
- *Match between system and real world* – this rates the extent to which the system speaks the user's language.
- *User control and freedom* – a rating of the ability of a user to "abort" a function that was chosen by mistake.

- *Consistency and standards* – words and phrases should be used in a standard way and different words or phrases should not refer to the same thing.
- *Error prevention* – the design should aim to prevent errors, rather than aim to recover from errors.
- *Recognition rather than recall* – instructions should be clear and easily available; users should not need to remember previous parts of the dialogue to continue.
- *Flexibility and efficiency of use* – expert users should be able to accelerate their actions by means of shortcuts that are "invisible" to novice users.
- *Aesthetic and minimalist design* – irrelevant information should be avoided, since it makes the relevant information "less visible". Additionally, interaction with the mobile device should be comfortable and respectful of social conventions.
- *Help users recognize, diagnose and recover from errors* – error messages should be displayed in plain text (not codes), and suggest solutions.
- *Help and documentation* - even though intuitiveness is preferable, documentation should be easily accessible for those who need it.

The same authors furthermore indicated that mobile applications have their own set of unique challenges, which makes the standard heuristics less applicable to such applications. They refined the standard heuristics to a set of heuristics that are more applicable to mobile applications. The refined set of heuristics follows (Bertini *et al*, 2005).

- *Visibility of system status and lossability / findability of the mobile device* – does the system keep the user informed? Are measures in place to cater for the common occurrence of a device being lost?
- *Match between system and the real world* – are users able to correctly interpret information? Is information presented in a logical and natural order?
- *Consistency and mapping* – is the user's conceptual view of the function consistent with the context?
- *Good ergonomics and minimalist design* – is the screen real estate used with economy, since it is limited?

- *Ease of input, screen readability and glancability* – is the screen content easily readable and the input simple and easy?
- *Flexibility, efficiency of use and personalization* – are users able to personalize frequent actions and configure the system according to their personal needs?
- *Aesthetic, privacy and social conventions* – is user's data kept private and safe?
- *Realistic error management* – are users shielded from errors and helped to recognize, diagnose and recover from errors? Are messages plain and precise?

#### 3.3.9.2 Heuristics for access channel usability

The author of this research is of the opinion that the available heuristics that can measure usability are based mostly on application design. Since this research was focussed on the underlying technology provided by the access channel, the heuristics had to be refined to fit in with the desired constraints. Therefore, the following set of heuristics was compiled to measure usability:

- *Number of screen changes to start* – this measures the number of screen changes the user has to execute to get to the first screen of the application.
- *Number of screen changes to execute a transaction* – similar to the previous heuristic, but this measures the number of screen changes from the first screen of the application up to a specific transaction.
- *Ease of executing menu options* – this measures the ease with which menu options can be selected.
- *Ability to use different media* – this includes the ability to use colour, pictures etc. on a specific access channel.
- *Default keypad selection* – this measures whether or not the technology allows settings that enable the keypad selection to be automatically correct, e.g. for numeric fields.
- *Format validation* – this is measured to determine whether or not field values be validated on the handset.

- *Intuitiveness* – this measurement determines if the technology allows for intuitiveness to lead the user to the correct input.
- *Editability of previously entered fields* – this includes the ability of the user to return to previously entered fields for the purpose of changing entered values.

#### 3.3.9.3 Questionnaire

The measurement tool that was selected to measure usability was a *focus group*. A group of people were selected and instructions were given to them to execute three different transactions. Each time they had to judge the experience based on the questionnaire (Appendix B), which included the heuristics explained above.

In addition, the facilitators at the focus group were asked to complete a table (Appendix C) that indicated the number of queries received during the testing of every individual access channel. This served as an indication (in addition to the experience of the user) of the intuitiveness of the specific channel.

#### 3.3.9.4 Selection of focus group

Bertini *et al* (2005) indicated that heuristics are normally evaluated by a panel of experts. During this research project the services of such a panel of experts were not available. The design was therefore adjusted to use a panel of non-experts. These people were individuals that volunteered for this project. A total of 12 people were used in two different groups.

Ideally, 12 identical handsets should have been used, but due to financial constraints, it was not possible to obtain identical handsets that had the capabilities required for the experiment. Since only one of the channels (WAP/XHTML) required a high-end (*advanced* as indicated by Bezuidenhoudt & Porteous (2008)) handset, six of these high-end handsets and six low-end handsets were used.

#### 3.3.9.5 Structure of the tests

The tests were run in four different stages. The procedure below was followed for each stage of the tests.

- Each group was given a set of identical handsets.
- Each group was instructed to test a specific access channel. During each stage, the two groups tested different access channels. This meant that the order of access channels was different for the two groups, thereby minimizing the influence of previous experience on the current stage.
- A brief explanation of the access channel was given to each group.
- The group was instructed to execute a number of distinct transactions. The group was then required to rate their experience (based on the questionnaire) for each of the access channels.
- Once the tests on a specific access channel were completed, the set of handsets were exchanged with the other group and the process was repeated for another access channel.

This process was repeated for each of the four selected access channels. Therefore, all four access channels were tested by both the groups but with different handsets.

## 3.4 Summary

Six different access channels were selected to be measured. Furthermore, three different characteristics were selected. The six access channels were:

- IVR,
- Java/J2ME,
- SMS,
- USSD,
- WAP and
- WIG.

WIG was considered to be similar to SAT because of the considerable similarities in the technologies. The three characteristics that were selected, are:

- security,
- ubiquity and
- usability.

Each of the characteristics was measured differently. The measurements were done as follows.

- Security was measured with weighted parameters, based on information available in the literature.
- Ubiquity was measured by means of market research which determined the percentage of users that can be reached with each of the selected access channels.
- Usability was measured by means of a focus group and a set of heuristics. The heuristics were determined by means of the literature. The heuristics were then refined to include a list that is purely based on the underlying technology and to exclude any other factors such as application design.

The next chapter describes the data captured for the different measurements as well as an analysis of the data.

# CHAPTER 4

## RESEARCH DATA AND ANALYSIS

### 4.1 Introduction

This chapter presents the results (section 4.2) that were formulated from the collected data. The data was analysed (section 4.3) to test the hypotheses presented earlier.

The data for the different characteristics was gathered in three different ways. Security information was gathered from literature and measurement values were assigned based on that information. Ubiquity data was gathered from market research. Usability data was gathered by means of a focus group.

There were certain limitations when the data was gathered. The following are of special interest.

- The ubiquity characteristic could not be measured accurately, due to a lack of available data. In such cases "assumed" values were assigned in order to do the analysis.
- The usability measurements were delayed as long as possible to allow the access channels to be available for measurement. Nevertheless, at the time the measurements were taken, only four of the channels were available, and some only in a limited fashion.

No limitations were experienced during the security measurements.

### 4.2 Results

This section describes the data that was gathered for each of the characteristics. Each characteristic is summarized and then each value is motivated on a per-channel basis.

### 4.2.1 Security

Below follows the motivation for the assigned security values.

### 4.2.2 IVR

It is possible to use all three authentication levels for IVR. The token (handset) can be identified by means of the caller identification, the user can be required to enter a pin that he knows and he may be required to pass through a voice recognition system. However, based on O'Gorman (2003), voice prints can be considered "weak" authenticators, and therefore a value of *6.5* is assigned for IVR authentication based on Table 3.1.

Since the complete message is compiled on the IVR server before it is submitted to the back-end application, the system can be designed to send the authentication information and the authorization information to the application server in the same message. However, the data will flow in different messages between the handset and the IVR server, but it is guaranteed to be in one session. If the call is terminated the data will be lost and recompiled. Based on Table 3.2, a value of *4* can therefore be assigned for the authorization dimension.

IVR is considered more secure than SMS. Figure 3.5 indicates the encryption available for the IVR access channel. The data is only stored at the IVR server, which in the case of banking transactions, should be secured by the bank (Krugel, 2007).

As far as confidentiality (encryption) is concerned, IVR is as secure as a voice call. It is therefore unencrypted data over an encrypted GSM line as long as a GSM network is used. Since voice calls are not stored at any of the nodes, it is considered to be encrypted hops. However, the author of this research is of the opinion that voice calls are likely to travel through a public voice network, which is generally not protected. This means that the GSM encryption is effectively nullified. IVR therefore needs to be measured as unencrypted data over an unencrypted line, which allows a value of *1* to be assigned for the confidentiality dimension, as indicated by Table 3.3.

#### 4.2.2.1 J2ME / Java

J2ME can only use one authenticator, since generally a Java application does not have access to SIM card information. Therefore, user-provided credentials are needed (e.g. user name & password). Table 3.1 shows that a value of *1* could be assigned for the authentication dimension.

As long as the Java application is designed to use the GPRS bearer, the channel can provide its own authorization. It is also possible to design the application in such a way that the authentication information and authorization information is sent in one message. This enables a value of *7* for the authorization dimension as indicated by Table 3.2.

As far as the confidentiality dimension (encryption) is concerned, Java allows for two options. It is possible to encrypt the data on the handset before transmission or, alternatively, a secure HTTPS connection can be used (see Figure 3.6). A risk for this channel is the fact that the consumer needs to establish that the application was downloaded from the correct (trusted) source and is not malicious in nature (Krugel, 2007). GSM communications are normally encrypted, which qualifies them as encrypted as well as an encrypted line. Therefore, the Java access channel can be considered to transfer encrypted data over an encrypted line. With the use of the GPRS bearer, the data will not be stored at any of the nodes, which is equivalent to encrypted hops. Based on Table 3.3, this allows a value of *5* to be assigned for confidentiality.

#### 4.2.2.2 SMS

In terms of authorization, the SMS channel provides 1 authentication level. The user *has* his/her SIM card which can be identified by means of the caller identification. Since SMS messages are stored unencrypted at different places, it is considered unsafe to require the user to enter authorization information that he/she might *know*, even though it is possible to send such information unencrypted. According to Table 3.1 a value of *5* can be assigned for the authentication dimension.

Since it is considered unsafe to enter PINs or passwords, the SMS channel is considered NOT to provide its own means of authorization. A second channel is needed. It is, however, possible to send unencrypted authorization data in conjunction with the authentication instruction. Table 3.2 indicates that a value of *2* can be assigned to the authorization dimension.

SMS data is encrypted only at the protocol layer by the GSM security protocols (see Figure 3.4). A further risk to SMS data is the fact that many handsets automatically stores sent SMS messages on the handset, which means that once the handset is compromised (e.g. stolen) the data that was transmitted in this way is available to the person that obtained the handset. SMS data is habitually stored at the mobile operator, where it is generally also not encrypted (Krugel, 2007). A value of *2* can be assigned for the confidentiality (encryption) dimension, based on Table 3.3.

#### 4.2.2.3 USSD

The USSD channel is capable of using two of the authentication layers. It is possible to identify the SIM card that the user *has* through the caller identification. The user can also safely enter a password that he/she *knows* since the data is not stored anywhere before the back-end application. It is shown in Table 3.1 that a value of *5* could be assigned for the authenticate dimension.

The USSD technology by definition is session-based. Even though the data is sent to the application in different USSD messages, it is guaranteed to be within one session. The dialogue cannot be terminated and continued later. Based on Table 3.2, this means that a value of *4* can be assigned for the authorization dimension.

As far as encryption and data storage is concerned, this is similar to IVR (see Figure 3.5). Since the transaction is completed within a single session, there is no data storage anywhere except at the termination point where the USSD messages are received and the

interpretation is handled. This means that the data can only be compromised if the GSM encryption protocols are compromised (Krugel 2007). A value of *3* can be assigned for the confidentiality (encryption) dimension as shown by Table 3.3.

#### 4.2.2.4 WAP / XHTML-MP

The WAP channel will not have access to SIM card information. The user will therefore be required to enter authentication information that he/she *knows*. This means that only one of the authentication levels is available to the WAP channel. Krugel (2007) indicated, however, that it is possible for the bank to trace the origin of the transaction to the SIM card that the user has. This seems to be dependent on the MNO, however, since they are responsible for adding the mobile number to the request header at the gateway (Various, 2007). A value of *5* is assigned to the authentication dimension.

In terms of authorization, the WAP channel is capable of providing its own authorization information. Care should be taken by the application designers to send the authentication information and authorization information in one message. However, WAP is generally used in a similar fashion to an Internet session, which means that the user will login at the start of the session and the authentication information will not be sent with each transaction. With the use of HTTPS a single session can be guaranteed, which allows a value of *5* for the authorization dimension. This value is based on Table 3.2.

WAP enables a GPRS session to be opened between the handset and the bank. The session is firstly protected by the GSM security protocols and further protected by the encryption of the banking site (HTTPS). This opens WAP up to threats similar to those posed to Internet banking, but with the added security of the bank being able to establish that the session was initiated from the user's SIM card. The GSM communication security protocol also adds more security (Krugel, 2007). This enables encrypted data (HTTPS) over an encrypted (GSM protocol) mobile line. GPRS data is not stored at any of the interim nodes. With reference to Table 3.3, this allows a value of *5* for the confidentiality (encryption) dimension.

#### 4.2.2.5 WIG (Similar to SAT as far as security is concerned)

Krugel (2007) indicates SAT as the most secure mobile banking channel. Since WIG uses technology that is similar to SAT, the author of this research considers the information regarding security to be equally applicable to both access channels.

The WIG channel allows two of the authentication levels. The user may be required to enter authentication information (password) that he/she *knows*. It is also possible to identify the origin of messages and trace them to the SIM card that the user *has*. Table 3.1 shows that a value of *5* can therefore be assigned to the authentication dimension.

Generally speaking, the WIG application can compile all necessary data on the handset before the data is transmitted to the back-end application. This means that it can easily guarantee that the authentication and authorization information is transmitted in a single message. As indicated by Table 3.2, this allows a value of *7* to be assigned to the authorization dimension.

The technology allows the bank to load its own encryption keys together with its own application onto the SIM card. This allows the consumer data to be stored on the SIM card and the user can be authenticated on the handset before the data is transmitted to the bank. The data can further be encrypted before it is transmitted over the mobile network and it will only be decrypted at the bank. The encryption of the data is therefore similar to WAP and J2ME as shown in Figure 3.6. With secure tamper proof keys available, a value of *6* was assigned to the confidentiality (encryption) dimension.

It is also possible to restrict access to the menus of the SIM card application with a so-called BPUK (PUK for Banking) and BPIN (PIN for Banking). This is similar to the normal PIN and PUK code of the SIM card. The user is required to enter the BPIN each time the menu is accessed and the BPUK can help recovery in the case where the BPIN has been entered incorrectly three times (Chovonova, 2006).

The security measurement values were assigned as follows:

**Table 4.1: Summary of security values**

| | IVR | J2ME | SMS | USSD | WAP | WIG |
|---|---|---|---|---|---|---|
| Authentication | 6.5 | 1 | 5 | 5 | 5 | 5 |
| Authorization | 4 | 7 | 2 | 4 | 5 | 7 |
| Confidentiality | 1 | 5 | 2 | 3 | 5 | 6 |
| **Total** | **11.5** | **13** | **9** | **12** | **15** | **18** |
| **Percentage** | **54.76** | **61.9** | **42.86** | **57.14** | **71.43** | **85.71** |

Since a maximum measurement of 7 could be assigned for each of the dimensions, a maximum total value of *21* is possible for a specific channel. Hence, the percentage is the total compared with 21.

### 4.2.3 Ubiquity

Ubiquity values were assigned as percentages that describe the availability of a specific channel for that specific dimension. Therefore a maximum value of 100 could be assigned for each of the channels for each dimension. The total is calculated by adding all the percentages not forgetting that the percentage for the *handset availability* must be multiplied by two - since it carries double the weight of the other dimensions.

The values assigned were gathered from various sources. They were:

- Clickatell (2008) – data regarding the SMS channel,
- Flashmedia (2007), Jinny, (2008), Mark & Bang (2008) & Redknee (2008) – data regarding the USSD channel and
- Comsys (2008) – information regarding the IVR channel.

Various avenues were explored to gather information regarding handset specific and SIM card specific data, but the author was unable to obtain any usable data. Some

assumptions could be made though based on Bezuidenhout & Porteous (2008). These were:

- handsets are more likely to be WAP/XHTML enabled than Java/J2ME enabled and
- SIM cards are likely to be more restrictive than handsets when ubiquity is considered.

Therefore, the following values were assumed for these two dimensions:

- 70% of handsets in use are WAP/XHTML enabled,
- 60% of handsets in use are Java/J2ME enabled,
- 50% of SIM cards in use are capable of executing a SIM card application for WIG or SAT,
- it was assumed that all MNOs in the UK have the ability to run a commercial gateway for the purposes of a SIM card based access channel and
- in Kenya, the MNO support for SIM card based access channels was assumed to be 0%.

Even though these assumptions are not accurate, it is possible to use them to demonstrate the effect that handset capabilities, SIM card restrictions and MNO technologies can have on the ubiquity of an access channel.

Table 4.2 describes the ubiquity values assigned in South Africa for each of the selected access channels:

**Table 4.2: Summary of ubiquity values in South Africa**

| | IVR | J2ME | SMS | USSD | WAP | WIG |
|---|---|---|---|---|---|---|
| **Handset Support** | 200 | 120 | 200 | 200 | 140 | 200 |
| **MNO Support** | 100 | 100 | 100 | 100 | 100 | 90 |
| **SIM Card Support** | 100 | 100 | 100 | 100 | 100 | 50 |
| **Technology Support** | 100 | 100 | 100 | 99 | 100 | 90 |
| ***Total*** | **500** | **420** | **500** | **499** | **440** | **430** |
| ***Percentage*** | **100** | **84** | **100** | **99.8** | **88** | **86** |

Table 4.3 describes the ubiquity values assigned in the UK for each of the selected access channels:

**Table 4.3: Summary of ubiquity values in the UK**

| | IVR | J2ME | SMS | USSD | WAP | WIG |
|---|---|---|---|---|---|---|
| **Handset Support** | 200 | 120 | 200 | 200 | 140 | 200 |
| **MNO Support** | 100 | 100 | 100 | 100 | 100 | 100 |
| **SIM Card Support** | 100 | 100 | 100 | 100 | 100 | 50 |
| **Technology Support** | 100 | 100 | 98 | 66 | 100 | 100 |
| ***Total*** | **500** | **420** | **498** | **466** | **440** | **450** |
| ***Percentage*** | **100** | **84** | **99.6** | **93.2** | **88** | **90** |

Table 4.4 describes the ubiquity values assigned in Kenya for each of the selected access channels.

Table 4.4: Summary of ubiquity values in Kenya

| | IVR | J2ME | SMS | USSD | WAP | WIG |
|---|---|---|---|---|---|---|
| **Handset Support** | 200 | 120 | 200 | 200 | 140 | 200 |
| **MNO Support** | 100 | 100 | 100 | 100 | 100 | 0 |
| **SIM Card Support** | 100 | 100 | 100 | 100 | 100 | 50 |
| **Technology Support** | 100 | 100 | 100 | 100 | 100 | 0 |
| ***Total*** | **500** | **420** | **500** | **500** | **440** | **250** |
| ***Percentage*** | **100** | **84** | **100** | **100** | **88** | **50** |

The combined ubiquity measurements for the three countries are listed in Table 4.5.

**Table 4.5: Summary of combined ubiquity values**

| | IVR | J2ME | SMS | USSD | WAP | WIG |
|---|---|---|---|---|---|---|
| **Handset Availability** | 200 | 120 | 200 | 200 | 140 | 200 |
| **MNO Availability** | 100 | 100 | 100 | 100 | 100 | 90 |
| **SIM Card availability** | 100 | 100 | 100 | 100 | 100 | 50 |
| **Technology Availability** | 100 | 100 | 99 | 79 | 100 | 90 |
| **Total** | **500** | **420** | **499** | **479** | **440** | **430** |
| **Percentage** | **100** | **84** | **99.8** | **95.8** | **88** | **86** |

Take note that the *handset support* has a maximum value of 200 where all the others have a maximum value of 100. A maximum value of *500* could be assigned to any specific channel. As seen in the table, the total value was converted back to a single percentage that indicates the overall ubiquity of each of the access channels.

Below follows the motivation for the ubiquity values that were assigned.

#### 4.2.3.1 IVR

IVR uses only voice data. Since handsets are designed with voice communication as their primary function, all handsets support IVR functionality.

Similarly MNOs support voice transmission as their primary function. There is therefore a 100% MNO support for the transmission of voice data.

As with the previous two dimensions, voice data is a primary function of the handset. The SIM card is not used during voice communication except during the initial setup of the call. It can therefore be stated that all SIM cards support IVR as an access channel.

The only possible problem with IVR as a mobile access channel is the availability of an IVR server. This should typically be provided by the application provider (in the case of mobile banking, the financial institution). Depending on the specific needs of the application, these IVR servers may be rather expensive, but they are easily available in commercial and open source format. Since the MNO has no involvement in the set up of such an IVR server, the application provider can implement any available server. In all three regions it was found that there is some 3rd party provider of a hosted IVR service. A value of 100% was therefore assigned to all three regions.

#### 4.2.3.2 J2ME / Java

Not all handsets support Java applications. As indicated by Bezuidenhoudt & Porteous (2008) only *advanced* handsets support Java applications. Due to limitations, it was not possible to obtain data that indicate the number of handsets in use that support Java.

When a Java application is used as an access channel, it will generally make use of GPRS as a bearer channel. GPRS is supported by all GSM networks and is therefore regarded as completely independent of mobile networks.

Java applications on mobile devices are generally not dependent on specific SIM cards. The application is stored and run on the device. Therefore, SIM card support can be regarded as 100%.

Since all GSM networks support at least GPRS communication, the availability of the technology is regarded to be 100%.

#### 4.2.3.3 SMS

All handsets (standard and advanced according to the definition of Bezuidenhoudt & Porteous (2008)) support text messaging or SMS. A rating of 100% is therefore assigned to the handset availability of this technology.

All GSM networks support SMS messages. SMS can therefore be regarded as completely independent of the MNO. A rating of 100% was therefore assigned for MNO independence.

Since SMS messages are available on the handset irrespective of the SIM card in use, a rating of 100% was assigned to SIM card availability for SMS.

The SMS technology is dependent on a gateway between the MNO and the back-end application. These gateways may be owned by the MNO or by a third party. Often a bulk-SMS provider can be used for this purpose, but this may not always be available. Since the measurements were done in South Africa, and a bulk-SMS provider is available to all networks, a rating of 100% was assigned to this dimension of SMS. In the UK a bulk provider that services 98% of the subscriber base was found and in Kenya 100% of

subscribers can be reached via a bulk-SMS provider. This yields a combined value of 99% within the 3 regions where measurements were taken.

#### 4.2.3.4 USSD

All GSM handsets support USSD communication. Since the technology is not based on any special application, but merely on a text-message (similar to SMS) type of technology, a value of 100% is assigned to handset availability for USSD.

All GSM networks support USSD communication. It is part of the basic GSM technology that is implemented to allow voice communication. A value of 100% can therefore be assigned to the MNO independence of USSD.

Since USSD communications is a function of the handset and not of the SIM card, SIM card compatibility is regarded as 100% for USSD.

USSD requires a gateway to be installed between the back-end application and the MNO. These gateways are commercially available and can be bought. It was discovered that 99% of subscribers in South Africa, 99% in the UK and 100% in Kenya can be reached with commercial USSD gateways that are currently available.

#### 4.2.3.5 WAP

WAP browsers are not available on all handsets. According to Bezuidenhoudt & Porteous (2008) they are only available on "advanced handsets". Due to the unavailability of data, an accurate measurement of this factor could not be done.

Since WAP uses GPRS as a bearer channel and GPRS is supported by all GSM networks, a rating of 100% was assigned to the MNO independence dimension for WAP.

WAP does not make use or require any special functionality on a SIM card. It is therefore regarded as being supported by all available SIM cards and a rating of 100% was assigned for this dimension of WAP.

Since the GSM networks support GPRS communication, it implies that they also have the technology to forward Internet communications to an Internet backbone. A value of 100% is therefore assigned for this dimension of WAP. This is true for all countries where measurements were taken.

#### 4.2.3.6 WIG

According to Bezuidenhoudt & Porteous (2008) SIM card applications only require a standard handset. It is therefore regarded as being supported by all handsets and a valuation of 100% was assigned to this dimension of WIG.

SIM card applications are highly dependent on support from the MNO. Since the MNO is required to put the application on the SIM card and they are often also involved in adding security keys onto the SIM card, this can be regarded as a 100% dependence on the MNO. In South Africa, two of the four MNOs have the availability to support WIG applications. These two MNOs have the majority market share in the South African marketplace, according to recent reports (Vodacom (2008), MTN (2008) & Coetzee (2008)), and therefore a value of 90% was assigned to MNO availability for WIG within South Africa. Due to data not being available for the other countries, an accurate measurement of this feature was not possible.

Even though the majority of subscribers can be reached with WIG, since the major MNOs in South Africa support it, not all SIM cards currently in use by these subscribers have the ability to execute a WIG application. No data could be found during this project to accurately indicate the percentage of SIM cards in use that can support such applications.

GSM networks that support WIG technology, will also have the ability to send the data received from the handset to the external application. Therefore the valuation of available technology and the MNO is similar in this regard and the same value was assigned.

### 4.2.4 Usability

The focus group performed a fixed set of transactions on each of the tested access channels. Due to certain limitations, the transactions were not all available on all the channels, but during the group discussion (after the individual tests) the proposed functionality of the other transactions were explained. The users seemed to all understand the technology, to an extent where some indicated that they are using some of the technologies on a regular basis in their private life.

The focus group consisted of 14 participants. Each participant was an experienced user of mobile handsets and had been using mobile phones for more than 97 months. Each one performed a fixed set of transactions on all three available access channels and rated their experience on a scale from 1 (least liked) to 5 (most liked) for each of the heuristics. Afterwards, they were asked to order the three channels from 1 (most liked overall) to 3 (least liked overall). After the individual measurements were completed, a group discussion followed during which the author of this research facilitated a discussion that arrived at an overall measurement for each access channel.

Since the individual overall measurement was done on a basis of ordering and not a scale, the values were transformed onto the scale (where 1 was worst and 5 best). Second place ordering was assigned an average value of "3". Afterwards all values were summed to arrive at a total usability measurement for each access channel. Table 4.6 shows the averaged values for the 14 participants.

The usability measurements were assigned as follows:

**Table 4.6: Summary of assigned usability values**

| Heuristic | IVR | J2ME | SMS | USSD | WAP | WIG |
|---|---|---|---|---|---|---|
| Number of screen changes to start | | | 3.78 | 4.36 | 3.950 | |
| Number of screen changes to execute transaction | | | 4.22 | 3.71 | 3.84 | |
| Ease of executing menu options | | | 4.33 | 3.57 | 4.13 | |
| Default keypad selection | | | 4.26 | 4.14 | 3.76 | |
| Format validation | | | 4.30 | 4.00 | 3.92 | |
| Intuitiveness | | | 4.22 | 3.85 | 3.89 | |
| Editability of previously entered values | | | 4.19 | 4.00 | 4.08 | |
| Overall measurement (Individual) | | | 1.86 | 3.57 | 3.86 | |
| General overall (from group discussion) | | | 3.00 | 3.50 | 3.50 | |
| **Total** | **NA** | **NA** | **34.15** | **34.70** | **34.93** | **NA** |

A maximum value of *45* could be assigned to any specific channel if it were to score a *5* on every value.

In the focus group discussion a number of interesting ideas were raised:

- the speed at which a transaction executes is very important,
- the users' perceived security were stronger when the PIN was entered for each transaction, rather than once per session,
- they would be unlikely to use SMS for more than balance and statement enquiries and

- multimedia branding (logos and colour) was less important than the speed at which a transaction can be performed.

These ideas played a role in the users' perceived usability of the system.

Below follows the motivation for the usability values that were assigned.

#### 4.2.4.1 IVR

This access channel was not tested for usability, since it was not available in any commercial or test environment at the time.

#### 4.2.4.2 J2ME / Java

This channel was not tested, since there was no Java application for the available handsets that enable financial transactions.

#### 4.2.4.3 SMS

This channel was tested with limited transactions. The reason for this was that payments are not possible in an acceptable way on the SMS channel. Therefore, only balance and statement enquiries were tested.

Even though only two of the three transactions were available on SMS, the users were quite happy to have limited functionality available on this channel. The author of this research explained the security issues and the users indicated that they were unlikely to do payments via SMS anyway. Since most users in the group were regular SMS users, they also found it easy to use and assigned an overall value of "3" for SMS usability.

#### 4.2.4.4 USSD

Since this technology could not be obtained in time, this channel was tested on a production system that enabled "airtime balances". This was the only available transaction which related to the three that was selected for the usability tests, and therefore the test on USSD was limited to a balance enquiry only. The available system does, however give the user an indication of how menus are selected and how the transactions are executed.

Many of the users in the group were regular USSD users for network related queries. They found the USSD channel easy to use and the fact that it is fast was considered a huge advantage. Furthermore, the fact that the PIN has to be entered for each transaction added to their perceived sense of security, since it gave them the ability to confirm each transaction. They reasoned that, because of this feature, there would be less chance of submitting an incorrect transaction. An overall usability measurement of "3.5" was assigned during the group discussion.

#### 4.2.4.5 WAP

A test system was used where all selected transactions were available on this access channel. This channel was therefore tested with all three selected transactions.

Initially, during the group discussion, the fact that it takes significantly longer to reach the main menu (than for example on USSD) was raised as a disadvantage. After some discussion, it became clear that this disadvantage is only applicable to the first transaction. After that, it was as easy as or easier than USSD. The fact that a selection of media (images and colour) is available on WAP, did not seem to be a huge advantage, however, it does add to a "nicer" experience. It was agreed that this could be an advantage for the service provider. An overall usability value of "3.5" was assigned to WAP during the discussion.

#### 4.2.4.6 WIG

A test system was available that enabled all transactions on this access channel, but at the time of the tests, there was a technical problem at the MNO which disabled the system. This channel could therefore not be tested for usability.

### 4.3 Analysis

The recorded data was analysed to test the hypotheses presented in chapter 3. $H_0$ was answered by analysing the results for all three characteristics. If multiple characteristics would suggest the same channels to be most appropriate, $H_0$ would be proven false.

$H_1$ was tested by analysing the security results (section 4.3.1). The results should show that the SIM card applications are more secure when used as access channels that any of the other options.

$H_2$ was tested through analysis of the ubiquity results (section 4.3.2). In order to prove $H_2$ true, the SMS channel should be shown as the most ubiquitous.

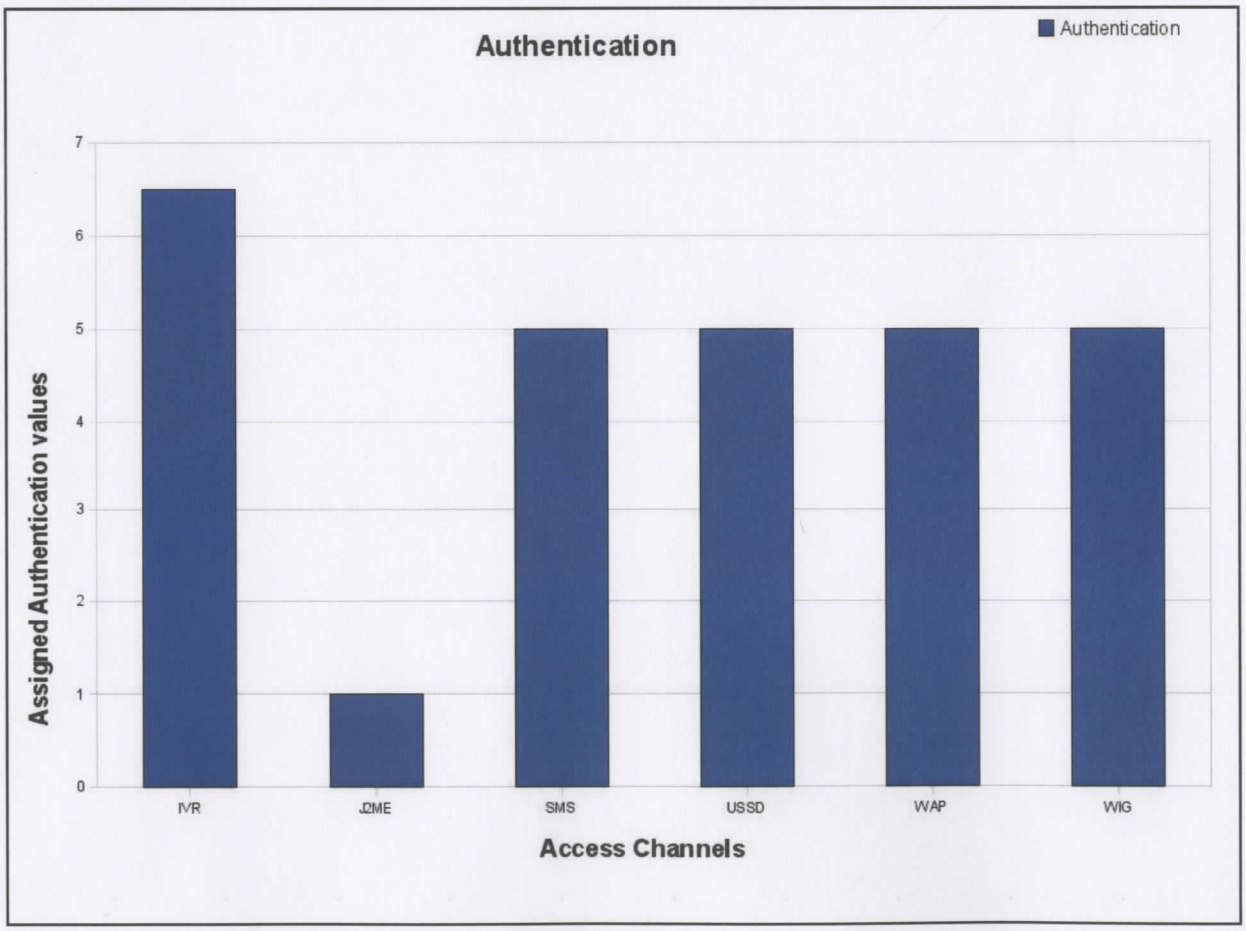
Analysis of the usability results was used to test $H_3$ (section 4.3.3). $H_3$ would be proven true if the Java channel was shown as the most usable.

### 4.3.1 Security

#### 4.3.1.1 Authentication

Figure 4.2 shows the measurements made for the *authentication* dimension of security.

**Figure 4.2: Authentication measurements**

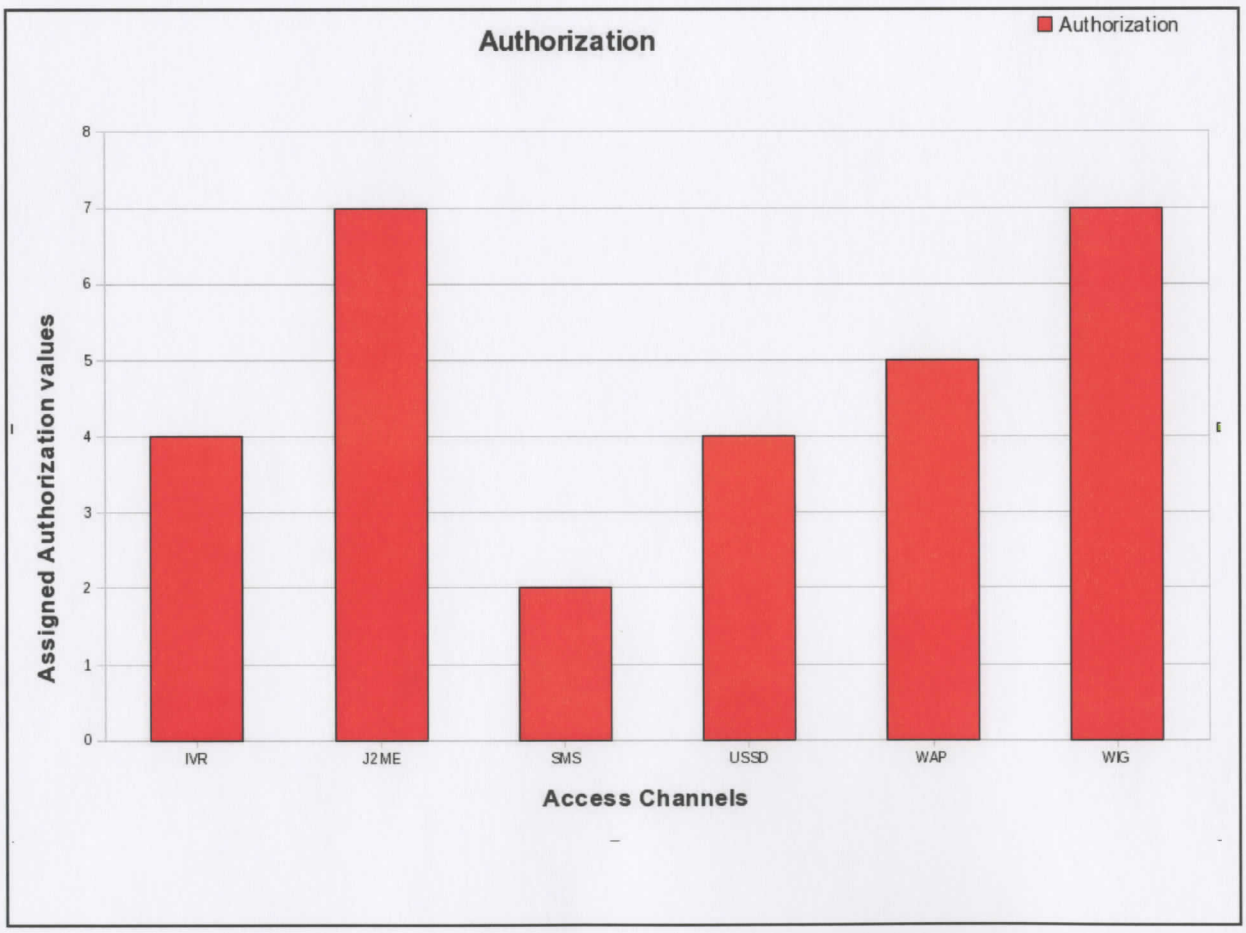


It is clear from this graph that the IVR channel has the best measurement value for the *authentication* dimension while the Java/J2ME channel has the lowest value. Note that IVR scored a 92.3% (6.5/7) value for authentication because the technology allows all three authenticators to be used. It is however important to note that (as shown later) IVR has the lowest encryption capability which makes it easy for a fraudulent agent to capture information during the IVR session.

#### 4.3.1.2 Authorization

Figure 4.3 shows the measurement values for the *authorization* dimension.

**Figure 4.3: Authorization measurements**

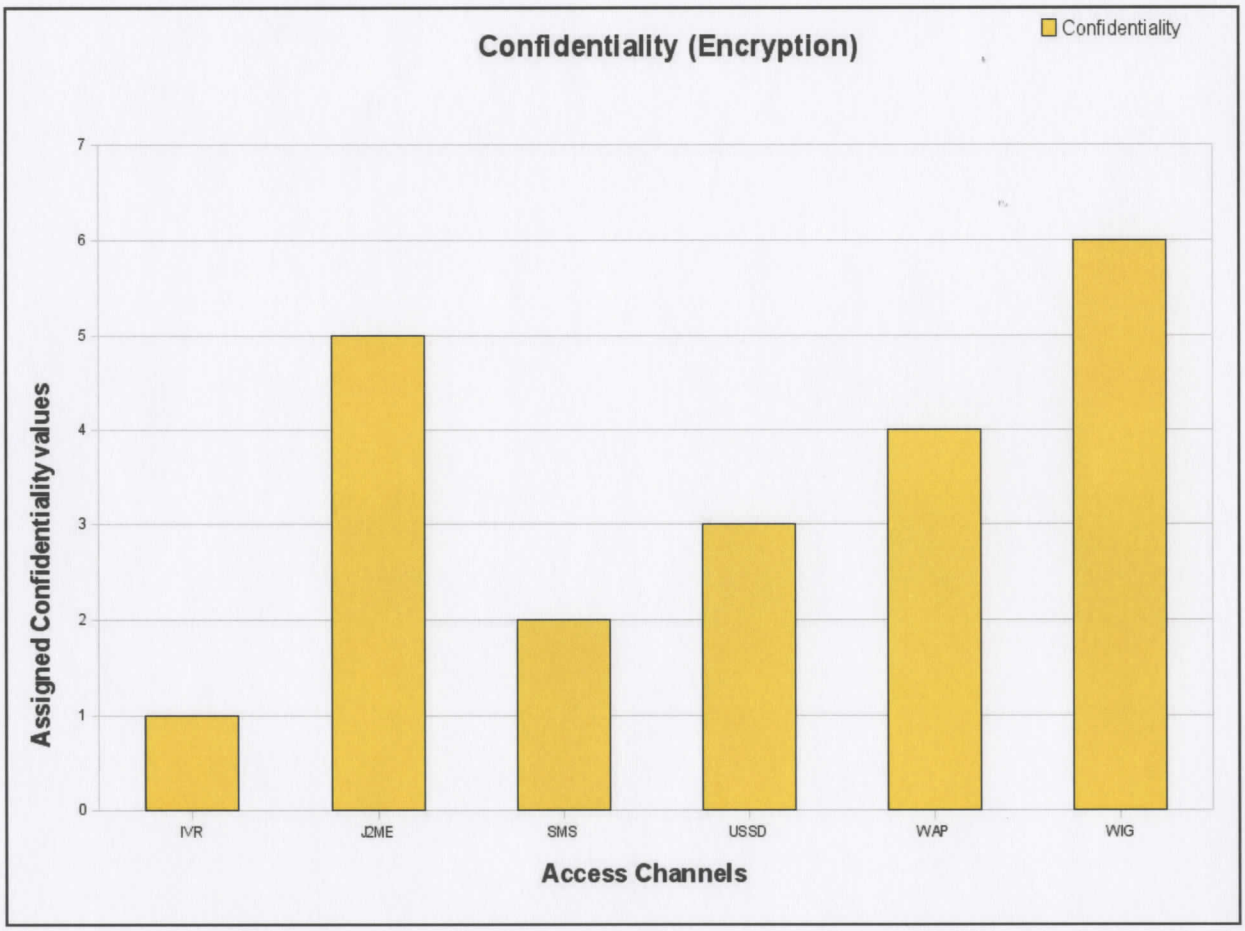


This graph shows two channels (Java / J2ME & WIG) as top scorers for authorization. Also of interest to note here is SMS with a low score of 2.

#### 4.3.1.3 Confidentiality

Figure 4.4 shows the results of the confidentiality measurements that were done on the different channels.

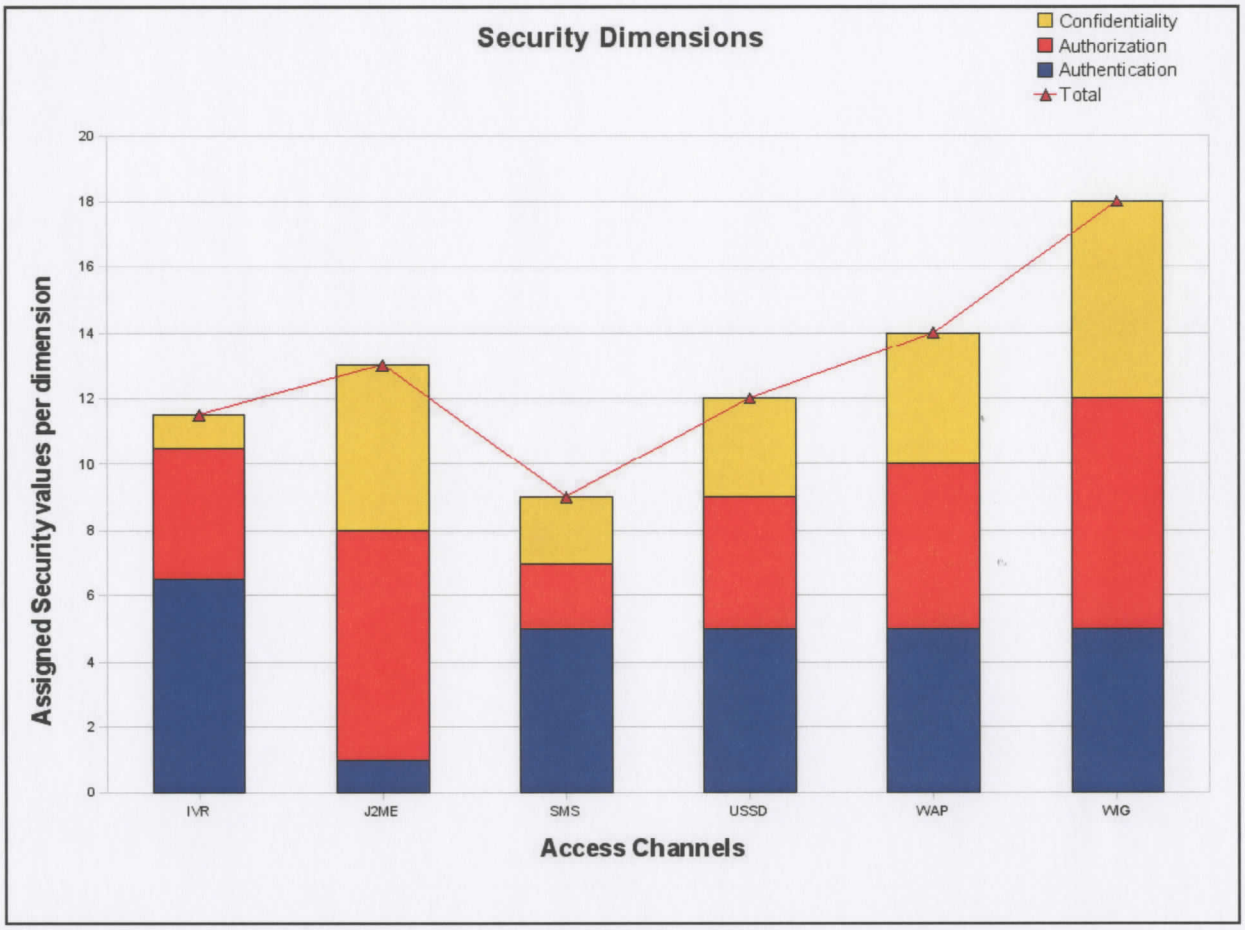
**Figure 4.4: Confidentiality measurements**




This graph shows that none of the channels was assigned a 100% score, but the highest was WIG with a 6/7 score. IVR is the lowest with a 1/7 score.

Figure 4.1 shows the combined values assigned for all security dimensions.

**Figure 4.1: Combined security measurements**




This graph indicates clearly that the WIG access channel has the highest total security measurement and that the SMS channel has the lowest. The author of this research considers the WIG and SAT access channels to have similar security measurements since the underlying technology is similar.

It is of interest to note that the WAP access channel has the most evenly distributed measurements across the different dimensions, which may make this a preferred option in some cases.

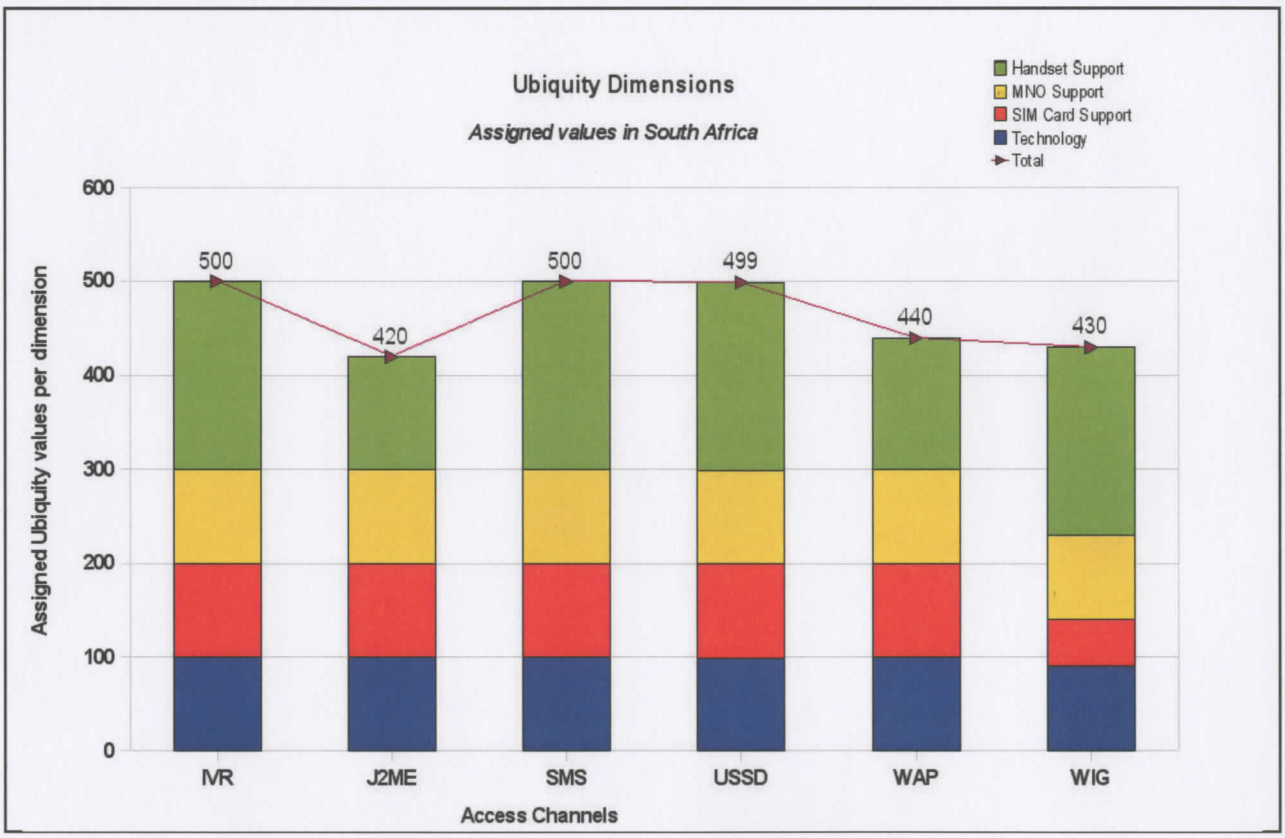
It is important to note that the different dimensions should not be considered individually. Instead, a complete security measurement can only be obtained by considering the

dimensions together. These results show that the SIM card application (represented by the WIG channel) is the most secure. Therefore, $H_1$ is true.

### 4.3.2 Ubiquity

Figures 4.5, 4.6 and 4.7 show summarized graphs of the ubiquity measurements taken in the different countries while Figure 4.8 shows a combined graph for all three countries. The reader should keep in mind that some values were purposely assigned to be fairly low to demonstrate the effect those dimensions would have.

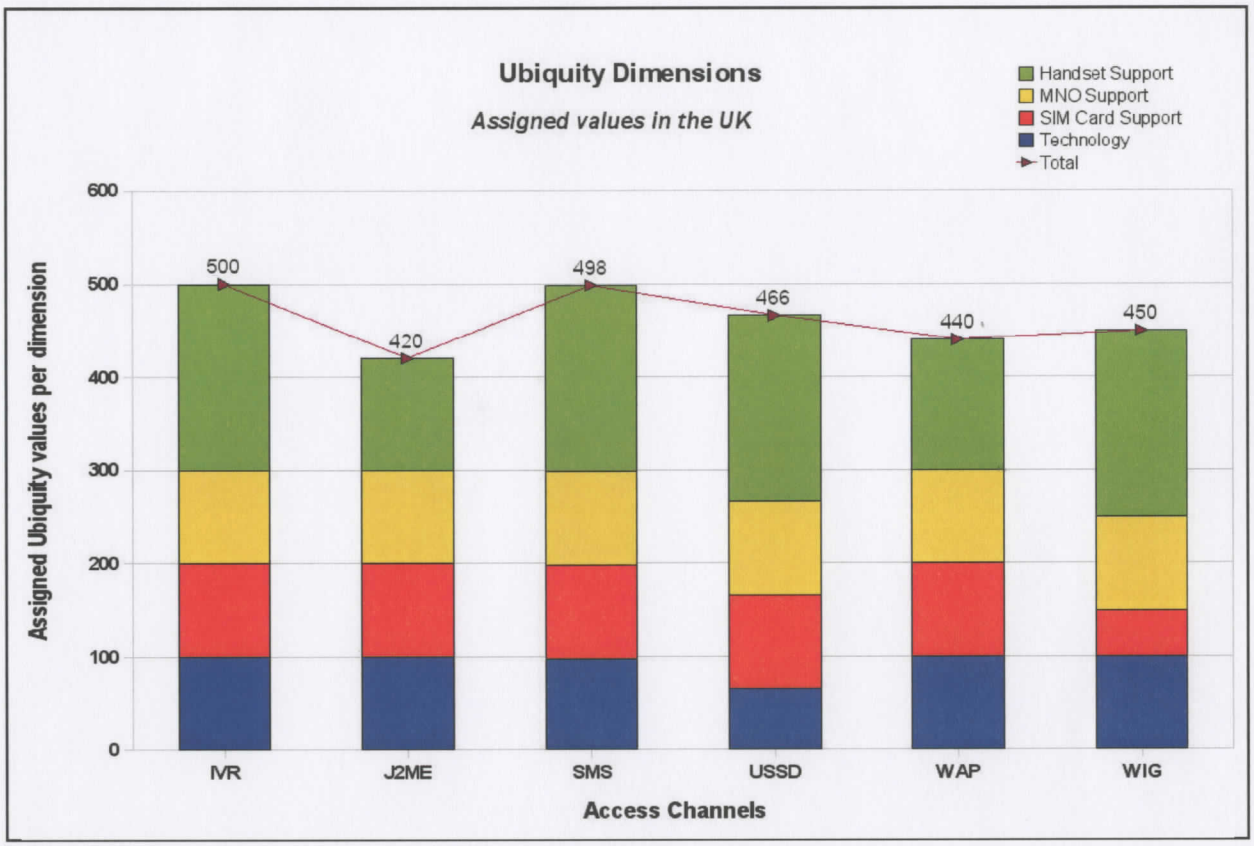
**Figure 4.5: Ubiquity measurements in South Africa**




This graph shows that, in the South African marketplace, IVR, SMS and USSD have very similar ubiquity. This could be due to the fact that for all three of these, a third-party provider of commercial services is available that has links to all the MNOs. WAP and

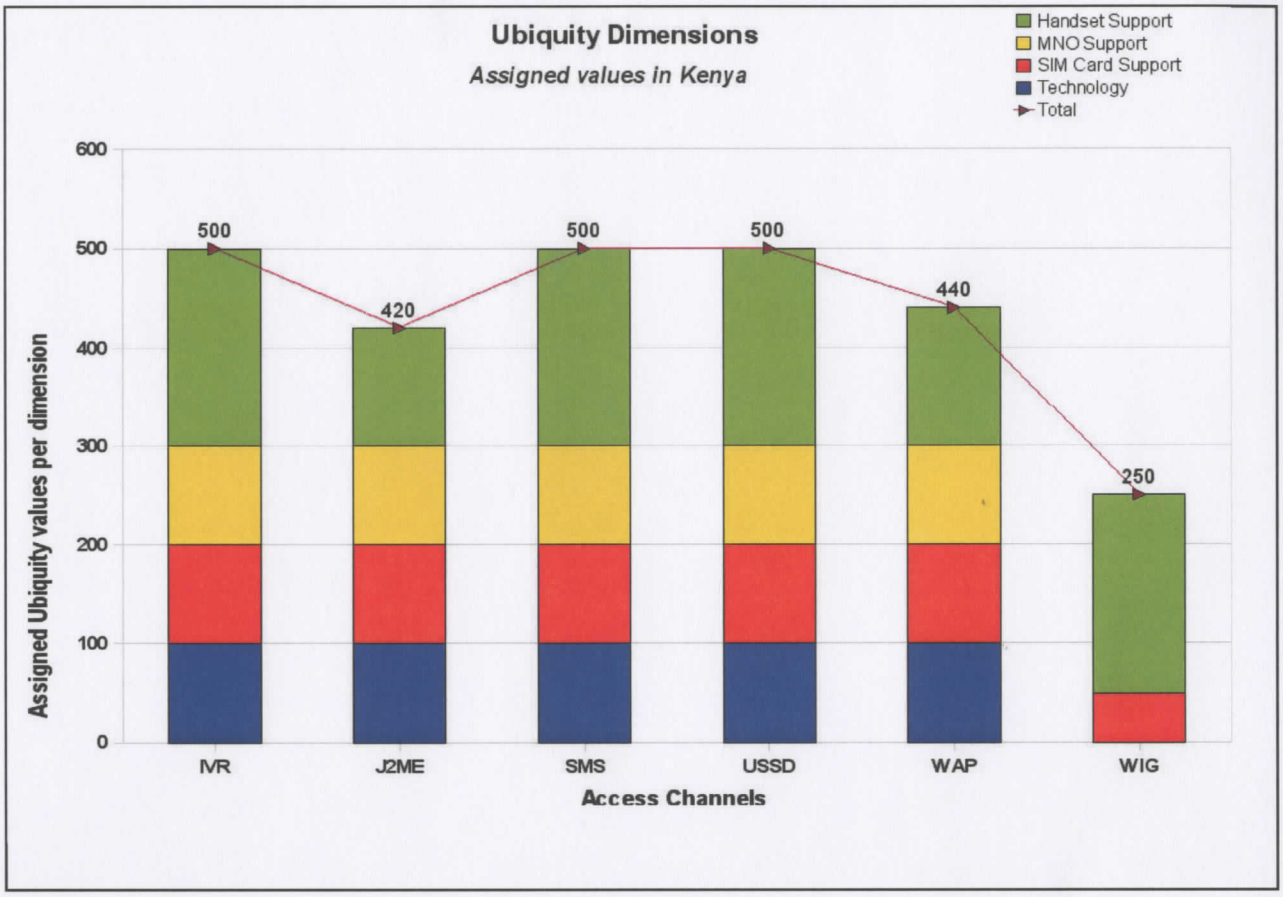
J2ME have lower measurements, due to their dependency on handsets that may not be readily available, while WIG has a limitation on MNO support.

**Figure 4.6: Ubiquity measurements in the UK**



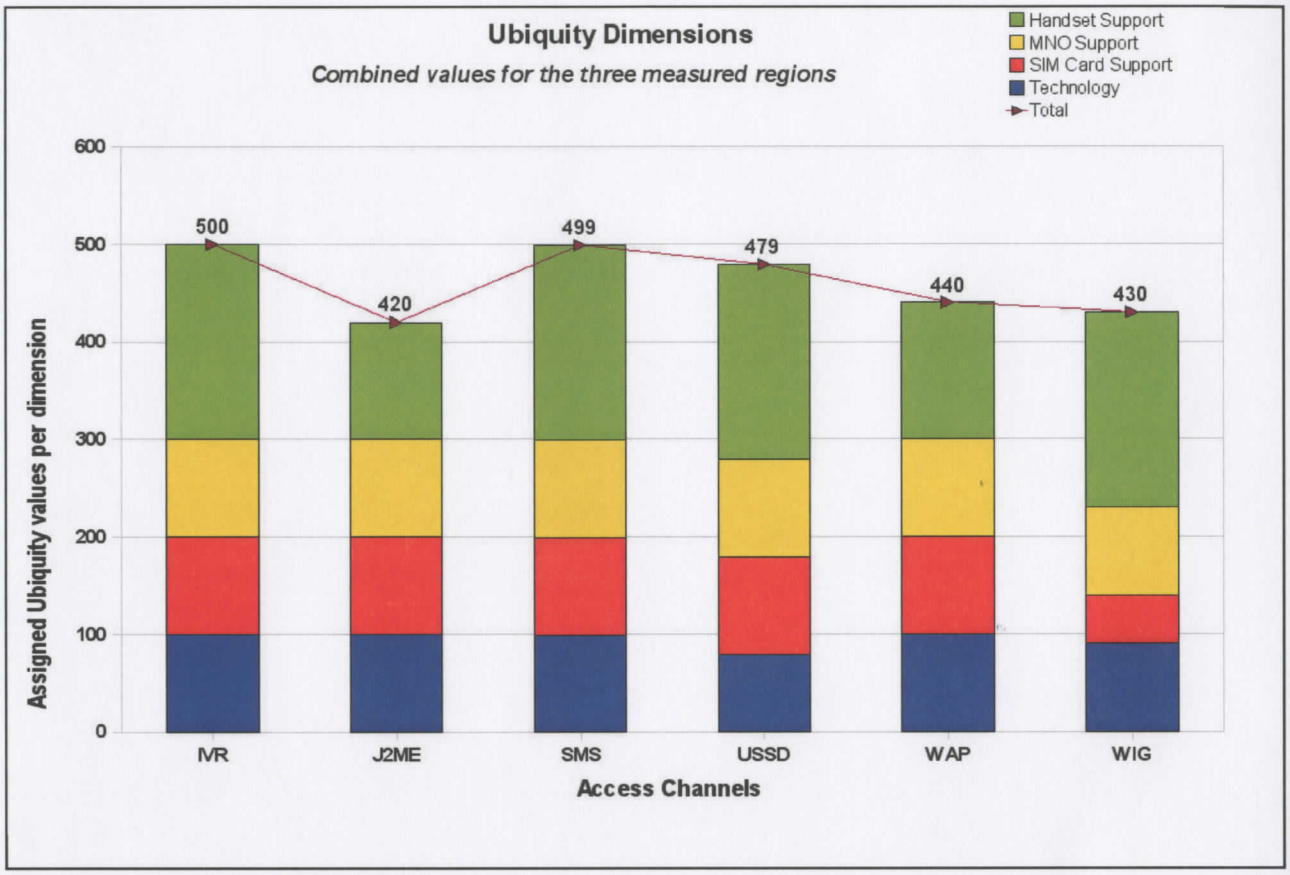

This graph shows clearly results are not very different from the South African graph. In the UK IVR and SMS have similar values, with USSD notably less. As in South Africa, WAP and J2ME are dependent on handset capabilities, while WIG (or in the case of the UK, SAT) is dependent on MNO support. With the exception of USSD which is notably less ubiquitous than in South Africa, the trends seems similar to those in South Africa.

**Figure 4.7: Ubiquity measurements in Kenya**




It is clearly seen in this graph that lack of MNO support hinders the ubiquity of the WIG channel. This graph has a different trend from the previous two. It is however interesting to note that IVR, SMS and USSD all score 100% due to the availability of third-party providers of commercial services. J2ME and WAP show similar trends to the other two graphs because of their dependency on handset support, but the biggest difference is WIG, which has no support in Kenya.

**Figure 4.8: Combined Ubiquity measurements**




Overall it can be seen that there are no marked differences between the ubiquity of the different access channels. The following interesting facts can be seen:

- MNO support is very similar,
- SIM card support is very similar except for the "assumed" value of *WIG*,
- technology support is the only factor that hinders *USSD* and
- handset support hinders the ubiquity of *J2ME* and *WAP*.

The results show that the IVR channel has a higher ubiquity (even with a very small margin) than the SMS channel. $H_2$ states that SMS is the most ubiquitous and therefore, $H_2$ is false.

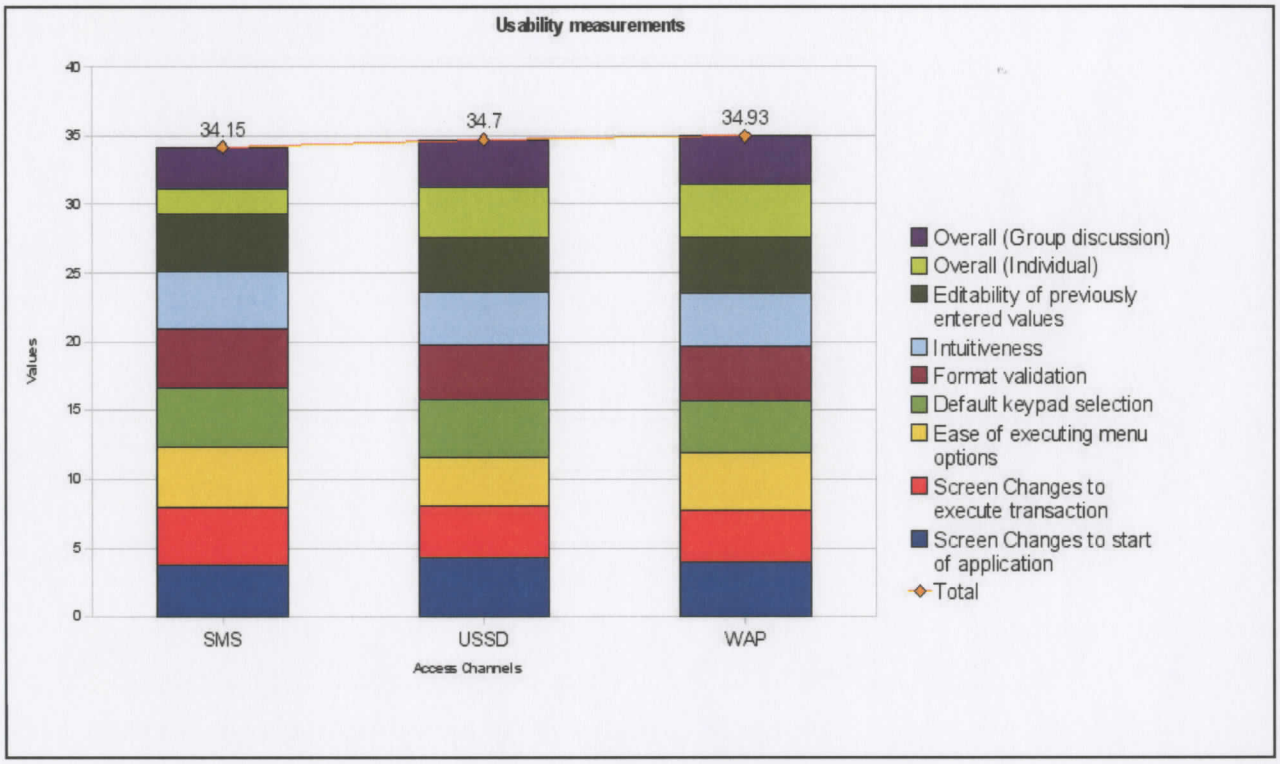
### 4.3.3 Usability

Figure 4.9 shows the usability measurements for the different access channels. This graph is divided to show the measurements for each of the heuristics. Of interest to note

here is that there is very little difference between the three access channels as far as usability is concerned. SMS is slightly less usable than USSD, and WAP is slightly more usable than USSD, but the differences are almost insignificant.

The author of this research found that the main reason for the differences is the fact that USSD asks for PINs to be entered on each transaction (thereby, giving the user the opportunity to back out of a transaction at that stage) and the fact that some of the channels have less functionality than others due to security reasons. The fact that WAP has the ability for more media (images and colour) is seen as a drawback, rather than an advantage, since it slows down the system.

**Figure 4.9: Combined Usability measurements**




The key on the right hand side indicates the graph values from top to bottom.

The results show that the WAP channel is the most usable. The Java channel, stated as the most usable by $H^3$, was not measured due to a lack of available technology. Based on available data, $H_3$ is therefore, false.

### 4.3.4 Overall analysis

In order to prove or reject $H_0$, the results of the three characteristics needed to be combined. It is clear that, if only one of the characteristics was considered, each characteristic would cause a different channel to be considered the most appropriate. Since $H_0$ states that "no single channel can be regarded as the most appropriate", it is proven true.

## 4.4 Summary

The results show clearly that different characteristics have different rankings for access channels. It is therefore clear that a choice of access channel cannot be made based on only one characteristic, but rather they should be regarded in combination with one another.

The measurements for the different characteristics were made completely independently of one another. When a financial service provider needs to choose between the different access channels, decision makers may want to consider them with some form of dependency. Especially when ubiquity is considered, it is possible that some SIM cards that are quite capable of handling a SIM card based application, do not contain the necessary security keys to make them as secure as possible. Similarly, the usability factor of an access channel may be dependent on the specific handset being used, since some handsets have better accessibility than others. These dependencies were NOT considered as part of this research project.

The results show that the SIM browser technologies (SAT and WIG) are the most secure access channels, SMS is the most ubiquitous and of the limited set that was measured, WAP is the most usable access channel. Even though there are differences, the usability results show that there are little difference between the channels and the ubiquity results show that the difference between the top channels are also very small. As far as security is concerned, there are a much larger differences, but the less ubiquitous channels seem to have higher security figures.

The next chapter contains the conclusion as well as some recommendations when a choice of access channel has to be made by a financial service provider.

# CHAPTER 5

## CONCLUSION

### 5.1 Introduction

This chapter describes the conclusions of this research, based on the data and measurements described in the previous chapters.

Three factors were measured for six of the different identified access channels. The selection of channels was based on availability, since it was clear that some of the channels were not available at all. Since the research was conducted mainly within South Africa, channels that were not available in South Africa were eliminated from the measurements.

All three measured factors are considered important when a decision is to be made on whether or not to support a specific access channel within an application. This is particularly important for mobile banking applications, since there are a number of limitations (legal and other) that restrict the use of such applications. Furthermore, a specific installation may have limitations that are not applicable to other installations, e.g. a specific mobile operator may not support commercial USSD implementations.

The author of this research therefore strongly advises that installation-specific constraints should be taken into account when a decision is made.

### 5.2 Conclusion

$H_0$ is shown to be true or false by combining the results of the three individual characteristics. Since each of the characteristics shows another access channel to be the most appropriate if it was to be considered in isolation, $H_0$ is proven true, since it clearly states that no single channel is the most appropriate. Results and conclusions based on individual characteristics are given below.

### 5.2.1 Security

Security measurements were done on each of the access channels. In order to do proper security measurements, the author of this research always assumed the best possible scenario for all these factors and therefore the only factor taken into account was the underlying technology of the specific mobile access channel. Even though it was not within the scope of this research, the bearer channel for each of the access channels did play a role in the respective security measurements.

The six selected access channels were all measured for three different security dimensions. These dimensions were identified through the literature and selected based on the ability to measure each of them considering the access channel technology rather than other factors. The three selected dimensions were:

- authentication,
- authorization and
- confidentiality.

Each of the dimensions was analysed and seven different levels were identified for each of them. Each of the channels was then assigned a value for each dimension based on information that was gathered from the literature. The values were graphed. The graph showed clearly that the SIM card technologies (WIG and SAT) were the most secure channels available, and that the SMS channel was the least secure.

Even though this is an indication that providers of mobile banking services should seriously consider SIM card technologies for their applications, it is the intention of the author of this research that other technologies may prove to be just as attractive when other factors (see section 5.2.2, 5.2.3 and 5.4) are taken into account. This therefore proves that hypotheses $H_1$ was correct.

### 5.2.2 Ubiquity

Ubiquity measurements were taken in three regions, South Africa, Kenya and the UK. The intention was to gather data in the three different regions to get a universal measurement.

Ubiquity measurements were expressed as a percentage of mobile users that can be reached through a specific access channel. In order to determine a proper ubiquity measurement, the following four factors were measured:

- technology support,
- SIM card support,
- MNO support and
- handset support.

As indicated by Ling (2008) the handset support was measured and multiplied by two to double its weight compared with the other factors.

It is important to note that the measurements were done independently of any other factors that may influence a decision on whether or not to support a specific channel. E.g. the SIM card measurement was taken purely based on whether it is possible to load an application onto the SIM card. The fact that the SIM card may or may not already contain security keys that may be required by a banking application, was not considered at all.

After the measurements were complete, it became clear that there are small differences in the ubiquity of the different channels. There are, however, other differences that may influence a decision on whether or not to support a specific access channel.

The following conclusions (purely based on ubiquity) could be made.

- IVR is the most ubiquitous access channel.

- The ubiquity of SMS is almost the same as that of IVR and if more data were available, they may very well be identical.
- USSD is slightly less ubiquitous, mainly due to the fact that commercial USSD gateways are not available to all MNOs. There are, however, a number of providers to USSD gateways and if the application provider has the money to spend, they can even implement their own gateway. This implementation could eliminate the difference between IVR/SMS and USSD completely.
- The Java/J2ME channel has a low ubiquity, because of the limited handset support. This limitation is overcome by the fact that the latest handset models mostly have Java support and as they become cheaper, the ubiquity of this channel will increase.
- WAP (similar to J2ME) is hindered by limited handset support. However, there is more support for WAP than Java, which gives it a higher rating.
- WIG/SAT is limited not only by SIM card support, but also by MNO support. This causes this to be the least ubiquitous access channel.

This does not conclusively prove that hypotheses $H_2$ was correct. The most ubiquitous access channel may be IVR and not SMS. Therefore, $H_2$ was proven to be false.

### 5.2.3 Usability

Only a limited number of the access channels could be measured during this research project. This was due to the unavailability of technologies at the time of measurement. The usability results showed that there was very little difference between the measured channels. The following findings were revealed during the measurement of usability.

- WAP is the most usable, even though only by a very small margin.
- SMS is the least usable by a slightly but not significantly bigger margin.
- Users would be happy to use SMS for informational financial transactions.
- Users appreciate the "confirmation" of a transaction with the entering of a PIN. This enhanced their sense of security and provides an opportunity to back out of a

transaction at a late stage. This is often NOT the case when multiple transactions are performed within a single session.

- There is very little difference between the usability of the different access channels.

Therefore hypotheses $H_3$ proved to be false. The reason for this is mainly the lack of a testable J2ME access channel. Had one been available the hypotheses may have proved to be correct. Instead, for the purpose of this research, the most usable access channel (even though by a very small margin) was shown to be XHTML/WAP.

## 5.3 Recommendation

During this research project, the author discovered that the question around choice of access channel for mobile banking applications is not an easily answerable one. Apart from the three characteristics measured in this project, there are also others that can be considered. Ultimately, the answer will also be dependent on *who* the provider of the mobile banking/payment service is. The author had numerous discussions with a number of role players and therefore makes some recommendations. These recommendations are based on the following:

- mobile banking requires a high degree of security,
- financial service providers would like to reach a wide an audience as possible as well as increase their own market share in their respective areas and
- usability should not play an important role in deciding which technology to use.

### 5.3.1 Mobile operator as service provider

As shown by Pau (2004) it is becoming more common to see MNOs in the role of a money flow handlers – which means that the MNO becomes the financial service provider. In such cases, it makes a lot of sense to use a technology that is tightly bound to the MNO. Access channels such as *USSD*, *WIG*, and *SAT* satisfy these conditions, but with the higher security rating of the SIM card technologies, MNOs should consider using *WIG* or *SAT* as their preferred access channel. Even though it was not measured during this project, these technologies might come at a significant cost, since the subscribers may

need to do SIM swaps in order to get access to the service. The *USSD* gateway is a less secure option, but it also comes at a cost, since a gateway needs to be secured if it does not already exist.

### 5.3.2 Bank (or other institution) as service provider

The more traditional approach would be for an existing bank to extend its services to include mobile banking as an option for its clients. In such cases, the banks would probably prefer NOT to be bound to a specific MNO, which means that they will consider technologies that are not bound to MNOs. These technologies include the following:

- IVR,
- Java / J2ME,
- SMS (if a 3rd party provider is available),
- USSD (if a 3rd party provider is available) and
- WAP / XHTML.

Since security is no doubt high on the priority list, *SMS* as an access channel should not be considered for financial transactions. Even though it is dependent on handset availability, *WAP / XHTML* and *Java / J2ME* come to mind as being preferable. These two access channels have reasonable security ratings (similar to a normal Internet application) and also have high usability ratings.

## 5.4 Future Research

This research project attempted to answer the question: "Which mobile access channel is most appropriate for mobile banking applications?" There were limitations during the research project, which caused some factors not to be considered. The author recommends that the following areas of future research should be considered to obtain more results.

- How application design can influence the measurement (security, ubiquity, usability) of a specific channel.

- Cost analysis of each of the channels and how it will influence the desirability of each of the access channels.
- Consideration of the availability of security keys on SIM cards to make a more complete ubiquity measurement.
- The influence of specific handsets on the usability of access channels.
- The collection of data can be extended to include the attributes that were unavailable during this project.
- One might want to consider the "marketing value" of an access channel.

## 5.5 Summary

**Table 5.1: Summary of hypotheses**

| Accepted | Rejected |
|---|---|
| $H_0$: If only a single characteristic were considered, a different *most applicable* channel would be selected in each case. | $H_2$: The IVR channel was found to be the most ubiquitous, even though by a very small margin. |
| $H_1$: SIM card application clearly have a higher security rating than other channels. | $H_3$: WAP / XHTML were found to be the most usable channels. The difference between the channels' usability was very small. |

It is clear that there are a number of factors that need to be considered to decide which access channel will be most appropriate for a specific mobile application. This research project attempted to answer some of these questions. The author did measurements on three factors that may influence the answer:

- security,
- ubiquity and
- usability.

During the project, it became clear that no one factor could be considered in isolation, but rather the specific needs of the installation should be considered.

Six different channels were measured in terms of the three factors mentioned. Each of the factors had a different "preferred" channel if it was considered in isolation. However, the factors could not be considered in isolation.

Based on the results obtained during this research project, the author was able to make certain recommendations as possible answers to the original research question. These recommendations depend on the type of institution that provides the mobile banking services.

## REFERENCES


Adams, A. & Sasse, M.A. 1999. Users are not the enemy. *Communications of the ACM*, 42(12):40-46.

Agoston, T.C., Ueda, T. & Nishimura, Y. 2000. Pervasive computing in a networked world. *Proceedings of the 10th annual Internet Society Conference, Pacifico, Yokahama, Japan, 18-21 July 2000*. http://monsterdesign.co.kr/reference/pervasive1.doc [22 June 2009].

Anderson, R., Manifavas, C. & Sutherland, C. 1996. Netcard – a practical electronic cash system. *Proceedings of the Fourth Cambridge workshop on security protocols, Cambridge UK, April 1996:49-57*.

Andreadis A., Benelli G., Giambene G. & Marzucchi B. 2001. Analysis of WAP over SMS-GSM. *CommsDesign:* 4 September 2001. http://www.commsdesign.com/showArticle.jhtml?articleID=192200651 [22 June 2009].

Anonymous. 2007. Unbanked need more info on cellphone banking. *Mail & Guardian Online:* 15 March 2007. http://www.mg.co.za/article/2007-03-15-unbanked-need-more-info-on-cellphone-banking [22 June 2009].

Arumuga, S. 2006. Effective method of security measures in virtual banking. *Journal of Internet Banking and Commerce*, 11(1). http://www.arraydev.com/commerce/JIBC/2006-04/VB.asp [22 June 2009].

Arunachalam, L. & Sivasubramanian, M. 2007. Theoretical framework to measure the user satisfaction in Internet banking. *Academic Open Internet Journal*, 20. http://www.acadjournal.com/2007/V20/part6/p3/ [11 June 2009].

AuthenticationWorld.com. 2006. *The business of authentication*. http://www.authenticationworld.com/ [11 June 2009].

Bachen, C. 2001. The family in the networked society: A summary of research on the American family. *STS Nexus*, Winter 2001.

Barkhuus, L. 2003. How to define the communication situation: Context measures in Present Mobile Telephony. *Proceedings of the fourth International and Interdisciplinary Conference on Modelling and Using Context, Stanford, California, 23-25 June 2003.* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.91.251&rep=rep1&type=pdf [22 June 2009].

Barkhuus, L. & Dey, A. 2003. Is context aware computing taking control away from the user? Three levels of interactivity examined. *Proceedings of the 5th annual Conference on Ubiquitous Computing, Seattle, USA, 12-15 October 2003:150-156.* http://www.springerlink.com/index/3rb1hq49n3143fdf.pdf [22 June 2009].

Bertini, E., Gabrielle, S., Kimono, S., Catarrh, T. & Santiago, G. 2005. Global methodology for evaluation of usability in mobile computing. *Report 7.3.7*, Multichannel Adaptive Information Systems. http://www.mais-project.it/documenti/pdf/R%207.3.7-MAIS-2005-UniRoma1.pdf [22 June 2009].

Bezuidenhoudt, J. 2008. Personal interview on 23 April 2008.

Bezuidenhoudt, J. & Porteous, D. 2008. Managing the risk of Mobile Banking technologies. *Bankable Frontier Associates*, FinMark Trust. http://www.finmark.org.za/documents/MBTechnologies_risks.pdf [22 June 2009].

Buyukkokten, O., Garcia-Molina, H., Packet, A. & Wingspread, T. 2000. Power Browser - Efficient web browsing for PDAs. *Proceedings of the CHI 2000 Conference on Human factors in Computing Systems, The Hague, 1-6 April 2000:430-437.*

Castells, M., Fernandez-Ardevol, M., Qui, J.L. & Se, A. 2004. The mobile communication society: A cross-cultural analysis of available evidence on the social uses of wireless communication technology. *Proceedings of the International workshop on Wireless Communication, Sonenberg School of Communication, University of Southern California, Los Angeles, 8-9 October 2004.*

Chakraborty, S. 2006. Mobile phone Usage Patterns Amongst University students: A comparative study between India and USA. *Thesis of Masters' Degree*. School of Information and Library Science, University of North Carolina, Chapel Hill.

Chau, S. 2003. The use of e-commerce amongst thirty-four Australian SMEs: An experiment or strategic business tool? *Journal of Systems & Information Technology*, 7(1): 49-66.

Chikomo, K., K Cong, M., Arab, A. & Hutchison, A. 2006. Security of Mobile Banking. Department of Computer Science, University of Cape Town, Cape Town.

Chmielarz, W. 2002. Profitability aspects of electronic banking applications for small companies. *Proceedings of the 10th European Conference on Information Systems, Glans, Poland, 6-8 June 2002:1578-1588*.

Cho, N. & Jung, J. 2005. A study on the influence factors in Internet- and mobile banking. *Proceedings of the 2005 International Conference on Business and Information, Hong Kong, 14-15 July 2005*. Taiwan: Academy of Taiwan Information Systems Research.

Chovanova, A. 2006. Forms of electronic banking. *National Bank of Slovakia Banking Journal (BIATEC)*, XIV(6/2006):22-25.

Claessens, J., Prenatal, B & Vanderbilt, J. 2001. Combining World wide web and wireless security. *Proceedings of the International Federation for Information Processing Conference*, Leaven, *26-27 November 2001:153-171*.

Clickatell. 2008. Message Pricing. *Clickatell.* http://www.clickatell.com/pricing/message_cost.php [11 June 2009].

Coetzee, K. 2008. Personal email received on 11 April 2008.

Coldwell, D.A.L. 2007. Is research that is both casually adequate and adequate on the level of meaning possible or necessary in business research? A critical analysis of some methodological alternatives. *Electronic Journal of Business Research Methods*, 5(1):1-10.

Comsys. 2008. Interactive Voice Response Services. *Comsys UK*, http://www.comsys.uk.com/ivr.htm [11 June 2009].

Corkrey, R. & Parkinson, L. 2002. Interactive voice response: Review of studies 1989 – 2000. *Behaviour Research Methods, Instruments, & Computers*, 34(3):342-353.

Couper, M.P., Singer, E. & Tourmaline, R. 2004. Does voice matter? An interactive voice response (IVR) experiment. *Journal of official statistics*, 20(3):551-570.

Coursaris, C.K. & Kim, D.J. 2006. A qualitative review of empirical mobile usability studies. *Proceedings of the 12th Americas Conference on Information Systems*, Acapulco, *Mexico, 4-6 August 2006*.

Derballa, V. & Pousttchi, K. 2004. Extending knowledge management to mobile workplaces. *Proceedings of the 6th International conference on Electronic commerce, Delft, Netherlands, 25-27 October 2004:583-590.*

Doern, R. & Fey, C.F. Undated. The emergence of eBanking in Russia. *A Working paper from Stockholm School of economics in St Petersburg*, Russia.

Fang, X., Xu, S., Brzezinski, J. & Chan, S.S. 2006. A Study of the feasibility and effectiveness of Dual-Modal information presentations. *International Journal of Human-Computer Interaction,* 20(1):3-17.

Fischmeister, S., Hagleitner, G., Pree, W. & Pomberger, G. 2001. Symbolon – A novel concepts for secure e-commerce. *Proceedings of the First IFIP conference on E-commerce, Zurich, Switzerland, 4-5 October 2001.*

Flashmedia. 2007. Our partners. *Flashmedia.* http://www.flashmedia.co.za/index.php?option=com_content&view=article&id=182&Itemid=282 [11 June 2009].

Forum Nokia. 2007. XHTML and other markup languages. *Forum Nokia technical library*. http://www.forum.nokia.com/document/Forum_Nokia_Technical_Library_v1_35/contents/FNTL/XHTML_and_other_markup_languages.htm [11 June 2009].

Garzonis, S. & O'Neill, E. 2006. Factors contributing to Low Usage of Mobile Data Services: User requirements, Service Discovery and Usability. *Proceedings of the 20th BCS Human-Computer Interaction Group conference, Queen May, University of London*, 11-15 September 2006.

Goel, S., Imielinski, T., Ozbay, K. & Nath, B. 2003. Grassroots – A scalable and robust information architecture. *Traffic Congestion and Sprawl.* Federal Highway Administration, US Department of Transportation. Technical Report DCS-TR-523(G).

Gomes, P., Tostao, S., Goncalves, D. & Jorge, J. 2001. Web Clipping - Compression Heuristics for displaying text on a PDA. *Proceedings of Mobile HCI 2001: Third International Workshop on Human Computer Interaction with Mobile Devices*, *Dunlop, M.D. & Brewster, S.A. (Eds), IHM-HCI 2001 Lille, France, 10 September 2001.* http://personal.cis.strath.ac.uk/~mdd/mobilehci01/procs/gomes_cr.pdf [22 June 2009].

Hampe, J.F., Swatman, P.M.C. & Swatman, P.A. 2000. Mobile electronic commerce - reintermediation in the payment system. *Proceedings of the 13th international Bled Electronic Commerce Conference, Bled, 19-21 June 2000. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.13.5578&rep=rep1&type=pdf* [22 June 2009].

Hellmund, M. 2003. Smart personalization for wireless applications. *Thesis in partial fulfilment of degree*, Diplom-Informatiker (FH). Media and Computer Science, Department of digital media, University of applied Sciences, Furtwagen, Germany.

Hellstrom, M. 2003. Java applications in mobile devices – concerning business services at Telia Mobile AB. *M.Sc. Dissertation*, Royal Institute of Technology, Stockholm, Sweden.

Hoffman, J. 2007. Terms of reference: Managing the risk of mobile banking technologies. *Finmark Trust.*

Janse van Rensburg, J. 2007a. *Personal Interview* on 16 March 2007.

Janse van Rensburg, J. 2007b. *Personal Interview* on 10 August 2007.

Janse van Rensburg, J. 2008. *Personal Communications* on 22 February 2008.

Jarecki, S. & Odlyzko, A. 1997. An efficient micropayment system based on probabilistic polling. *Proceedings of Financial Cryptography, First International Conference, FC'97, Anguilla, British West Indies, 24-28 February 1997:173-191.*

Jinny. 2008. USSD. *Jinny™.*

Karem, K. 2003. Internet Banking in Estonia. *A working paper from PRAXIS Center for Policy Studies*, Estonia, 2003:1-28.

Kiyingi, K.K. 2007. Customers send money using phones. *AllAfrica.Com:* 22 October 2007. http://allafrica.com/stories/printable/200710221934.html [11 June 2009].

Kreyer, N., Pousttchi, K. & Turowski, K. 2002. Characteristics of mobile payment procedures. *Proceedings of the 1st International Workshop on M-Services – Concepts, Approaches and Tools, Lyon, France, 26 June 2002.* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.10.437&rep=rep1&type=pdf [24 June 2009].

Krugel, G.T. 2007. Mobile banking technology options. *Finmark Trust.* http://www.finmark.org.za/documents/MBTO_report.pdf [24 June 2009].

Lee, K.S., Lee, H.S. & Kim, S.Y. 2007. Factors influencing the adoption behaviour of Mobile Banking: A South Korean perspective. *Journal of Internet Banking and Commerce*, 12(2). http://www.arraydev.com/commerce/jibc/2007-08/HyungSeokLee_Final_PDF%20Ready.pdf [22 June 2009].

Ling, A. 2007. *Personal interview on* 28 August 2007.

Ling, A. 2008. *Personal interview* on 4 March 2008.

Lipscomb, T.J., Totten, J.W., Cook, R.A. & Lesch, W. 2007. Cellular phone etiquette among college students. *International Journal of Consumer studies*, 31(1): 46-56.

Mahmoud, Q.H. 2004. Design challenges and possible solutions to wireless applications development. *Proceedings of Software Engineering Research and Practice (SERP) 2004* 2:782-788, Las Vegas, Nevada, USA.

Mallat, N., Rossi, M. & Tuunainen, V.K. 2004. Mobile Banking Services. *Communications of the ACM,* 47(5):42-46.

Mark, O. & Bang M. 2008. Dawn of e-commerce loom as banks leaps into mobile banking. *Business Daily Africa:* 15 July 2008. http://allafrica.com/stories/200807150222.html [11 June 2009].

McCullagh, A. & Caelli, W. 2000. Non-repudiation in a digital environment. *First Monday*, 5(8). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/778/687 [22 June 2009].

McKitterick, D. 2003. A web services framework for mobile payment services. *Thesis in partial fulfilment of degree M.Sc. In Computer Science*, University of Dublin, Dublin.

Mehrotra, P. 2007. Brewing India on the VAS map. *Hindustan Times:* 11 July 2007. http://www.hindustantimes.com/StoryPage/Print.aspx?Id=5ec7d572-a2d1-4f50-8199-b2ac21786e45 [11 June 2009].

M-Indya.com. 2005. MExE basics and a detailed discussion of MExE. http://www.m-indya.com/mexe/ [11 June 2009].

Mitchell, C. 2004. Security for Mobility. *Institution of Electrical Engineers.* http://books.google.com/books?id=C4MBvvyNcs8C&printsec=frontcover#PPP1,M1 [11 June 2009].

MTN. 2008. MTN Group – Media Centre – Overview. *MTN*. http://www.mtn.com/Media/overviewdetail.aspx?pk=359 [11 June 2009].

Myers, M.D. 2008. Qualitative Research in Information Systems. *MIS Quarterly*, (21:2):241-242 June 1997. *MISQ Discovery*, archival version, June 1997, http://www.misq.org/discovery/MISQD_isworld [11 June 2009].

Odlyzko, A. 2002. Roxane Googin's predictions and the telecom world. *The cooking report on the Internet*, 11(1-2):53-58.

O'Gorman, L. 2003. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE 91(12):2021-2040, December 2003.*

Oliver, B. & Barrett, C. 2004. Comfort & Ubiquity = Adoption: Enhancing first year students' communication skills with handheld computers. In Atkinson, R., McBeath, C., Jonas-Dwyer, D. & Philips, R. (eds), Beyond the comfort zone: *Proceedings of the 21st ASCILITE Conference, 5-8 December 2004.* http://www.ascilite.org.au/conferences/perth04/procs/oliver-b.html [24 June 2009].

O'Meara, D. 2007. Texting for more than flirting. *Financial Post – Part of the Canada.com network:* 19 October 2007. http://www.canada.com/components/print.aspx?id=0947771e-5bc2-4172 [26 October 2007].

Pau, L-F. 2004. Mobile operators as banks or vice versa - and - the challenges of mobile channels for banks. *ERIM Research Report:* ERS-2004-015-LIS. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=513770 [24 June 2009].

Potts, G. 2004. College students and cell phone use: Gender variation. *HC Rhetoric 160.*

Qualcomm. 2003. BREW™ and J2ME™ – A complete Wireless Solution for Operations Committed to Java™. Qualcomm Incorporated. http://www.qualcomm.com/brew/images/about/pdf/brew_j2me.pdf [4 October 2008].

Ratha, N.K., Connell, J.H. & Bolle, R.M. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, 40(3):614-634.

Redknee. 2008. Customers worldwide – Europe. *Redknee.* http://www.redknee.com/results/customers_worldwide/europe/ [11 June 2009].

Riivari, J. 2005. Mobile banking - A powerful new marketing and CRM tool for financial services companies all over Europe. *Journal of Financial Services Marketing,* 10(1):11-20.

Salmenjoki, K. & Jantti, R. 2002. Using mobile devices for personalized information. *Proceedings of the 5th Joint Conference on Knowledge-Based Software Engineering, Maribor, Slovenia, 11-13 September 2002*:154-163.

Scholtz J. & Richter, H. 2001. Report from Ubicomp 2001 Workshop: Evaluation Methodologies for Ubiquitous Computing. In Abowd, G. (ed). *ACM SIGCHI Bulletin* 2002:9.

Schwenke, F. & Weideman, M. 2007. Mobile application access channels – technologies, attributes and awareness. *Proceedings of the 9th Annual conference on WWW applications, Johannesburg, South Africa, 5-7 September 2007.*

Schwenke, F., Weideman, M. & Janse van Rensburg, J. 2008. Mobile access channel characteristics: a comparison of security dimensions. *Proceedings of the 10th Annual conference on WWW applications, Cape Town, South Africa, 3-5 September 2008.*

Schwenke, F., Weideman, M. & Janse van Rensburg, J. 2009. Measuring the ubiquity characteristics of mobile access channels. *Proceedings of the 10th Annual conference on WWW applications, Port Elizabeth, South Africa, 2-4 September 2009.*

SearchSecurity.com. 2008a. What is authentication? - definition from Whatis.com. *SearchSecurity.com* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html [22 February 2008].

SearchSecurity.com. 2008b. What is authorization? - definition from Whatis.com. *SearchSecurity.com* http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci211622,00.html [22 February 2008].

Setiawan, T. 2001. The use of J2ME with a Campus portal for Wireless devices. *Preliminary draft of Thesis in partial fulfilment of M.Sc.*, San Jose State University, San Jose.

Siam, A.Z. 2006. Role of electronic banking services on the profits of Jordanian banks. *American Journal of Applied Sciences*, 3(9):1999-2004.

SmartTrust. 2003. WIG Push Request Protocol Specification – Delivery Platform 6. SmartTrust AB.

Taddesse, W. & Kidan T.G. 2005. e-Payment: Challenges and opportunities in Ethiopia. *United Nations Economic Commission for Africa*.

Talbot, C. 2007. Mobil users frustrated with complexity, usability. *eChannelLine Daily News:* 11 March 2007. http://www.usernomics.com/news/2007/03/mobil-users-frustrated-with-complexity.html [11 June 2009].

Thompson, V. 2000. What the hell is...MExE? *The Register:* 29 March 2000. http://www.theregister.co.uk/2000/03/29/what_the_hell_is_mexe/ [11 June 2009].

Van der Merwe, P.B. 2003. Mobile commerce over GSM: A banking perspective on security. *Thesis Master of Science (Electronics)*, Faculty of Engineering, University of Pretoria.

Various authors. 2007. Main: how can I get the cellphone number. *Sony Ericsson Developer World.* http://developer.sonyericsson.com/thread/35328 [27 May 2008].

Vodacom. 2008. Vodacom results for the period ended December 31, 2007. *Vodacom*. http://www.vodacom.com/vodacom/mccomcrdetail.do?id=1084&action=detail [11 June 2009].

Wikipedia. 2008a. Authentication – Wikipedia, the free encyclopaedia. *Wikipedia*. http://en.wikipedia.org/wiki/Authentication [11 June 2009].

Wikipedia. 2008b. Non-repudiation – Wikipedia, the free encyclopaedia. *Wikipedia*. http://en.wikipedia.org/wiki/Non-repudiation [11 June 2009].

Wikipedia. 2008c. List of mobile network operators of Europe. *Wikipedia*. http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_Europe [11 June 2009].

Wikipedia. 2008d. List of mobile network operators of the Middle East and Africa. *Wikipedia*. http://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_the_Middle_East_and_Africa [11 June 2009].

Yoga, S.A. 2007. Always on! The demise of I-Mode. http://90273.blogspot.com/2007/10/always-on-demise-of-i-mode.html [11 June 2009].

# APPENDICES

## APPENDIX A – RELATIVE MARKET SHARE OF MNOs IN SOUTH AFRICA, KENYA AND THE UK

Vodacom (2008), MTN (2008) and Coetzee (2008), indicated the following market distribution in South Africa.

**Table 7.1: Market share of the different MNOs in South Africa**

| Mobile Network Operator | Number of subscribers (in 1000 s) | Percentage market share |
|---|---|---|
| Vodacom | 24255 | 56.34 |
| MTN | 14799 | 34.37 |
| Cell C | 4000 | 9.29 |
| *Virgin Mobile | ? | 0 |
| | | |
| **Total** | **43054** | **100** |

Wikipedia (2008d) indicated the market share of MNOs in the UK as follows:

**Table 7.2: Market share of the different MNOs in the UK**

| Mobile Network Operator | Number of subscribers (in 1000 s) | Percentage market share |
|---|---|---|
| O2 | 18382 | 23.34 |
| Vodaphone | 17645 | 22.40 |
| T-Mobile | 17311 | 21.98 |
| Orange | 15400 | 19.55 |
| 3 | 3900 | 4.95 |
| *Virgin Mobile | 4520 | 5.74 |
| *Tesco Mobile | 1500 | 1.90 |
| *Blyk | 100 | 0.13 |
| *MobileWorld | ? | 0 |
| *Fresh Mobile | ? | 0 |
| *BT Mobile | ? | 0 |
| *Dot Mobile | ? | 0 |
| *ASDA Mobile | ? | 0 |
| *Talk Mobile | ? | 0 |
| | | |
| **Total** | **78758** | **100** |

Wikipedia (2008c) indicated the market share of MNOs in Kenya as follows:

**Table 7.3: Market share of the different MNOs in the Kenya**

| Mobile Network Operator | Number of subscribers (in 1000 s) | Percentage market share |
|---|---|---|
| Safaricom | 6500 | 78.72 |
| Celtel | 1757 | 21.28 |
| | | |
| **Total** | **8257** | **100** |

* - So-called *virtual* networks that operate with one of the more established networks' technology.

## APPENDIX B – QUESTIONNAIRE USED FOR THE FOCUS GROUP FOR MEASURING USABILITY.

# Rating sheet

Please rate your experience for each of the following by rating each of the questions.
Each question should be rated as 1 = most disliked up to 5 = most liked.

*Please indicate how much experience you have using mobile phones:*

| Years | Months |
|---|---|
| | |

*Please complete the following tables. There is one table for each access channel and all executed transactions should be recorded in the space allocated for it.*

| **Access Channel:** | SMS |
|---|---|

| | **Balance Enquiry** | | | | | **Payment** | | | | | **Statement** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Area | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** |
| Number of screen changes to start the application | | | | | | | | | | | | | | | |
| Number of screen changes to execute the transaction | | | | | | | | | | | | | | | |
| Ease of executing menu options | | | | | | | | | | | | | | | |
| Default keypad selection on fields | | | | | | | | | | | | | | | |
| Format validation | | | | | | | | | | | | | | | |
| Intuitiveness | | | | | | | | | | | | | | | |
| Editability of previously entered values | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

| **Access Channel:** | USSD |
|---|---|

| | **Balance Enquiry** | | | | | **Payment** | | | | | **Statement** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Area | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** |
| Number of screen changes to start the application | | | | | | | | | | | | | | | |
| Number of screen changes to execute the transaction | | | | | | | | | | | | | | | |
| Ease of executing menu options | | | | | | | | | | | | | | | |
| Default keypad selection on fields | | | | | | | | | | | | | | | |
| Format validation | | | | | | | | | | | | | | | |
| Intuitiveness | | | | | | | | | | | | | | | |
| Editability of previously entered values | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

| **Access Channel:** | WAP / XHTML |
|---|---|

| | **Balance Enquiry** | | | | | **Payment** | | | | | **Statement** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Area | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** |
| Number of screen changes to start the application | | | | | | | | | | | | | | | |
| Number of screen changes to execute the transaction | | | | | | | | | | | | | | | |
| Ease of executing menu options | | | | | | | | | | | | | | | |
| Default keypad selection on fields | | | | | | | | | | | | | | | |
| Format validation | | | | | | | | | | | | | | | |
| Intuitiveness | | | | | | | | | | | | | | | |
| Editability of previously entered values | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

| **Access Channel:** | WIG |
|---|---|

| | **Balance Enquiry** | | | | | **Payment** | | | | | **Statement** | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Area | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** | **1** | **2** | **3** | **4** | **5** |
| Number of screen changes to start the application | | | | | | | | | | | | | | | |
| Number of screen changes to execute the transaction | | | | | | | | | | | | | | | |
| Ease of executing menu options | | | | | | | | | | | | | | | |
| Default keypad selection on fields | | | | | | | | | | | | | | | |
| Format validation | | | | | | | | | | | | | | | |
| Intuitiveness | | | | | | | | | | | | | | | |
| Editability of previously entered values | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |

*Please rate your overall experience for each of the access channels by ordering them from 1 (most usable) to 4 (most unusable).*

| | |
|---|---|
| SMS | |
| USSD | |
| WAP / XHTML | |
| WIG | |

## APPENDIX C – QUESTIONNAIRE USED FOR THE FACILITATORS AT THE FOCUS GROUP MEASUREMENT FOR USABILITY.

# Rating Sheet

*Please indicate the number of queries received for each of the channels measured:*

| | |
|---|---|
| SMS | |
| USSD | |
| WAP / XHTML | |
| WIG | |

# GLOSSARY

**Automatic Teller Machine (ATM)**

An ATM is a computerized system, used by financial institutions, to provide customers with the ability to access financial transactions in a public space (like a shopping mall) without human interaction.

**Binary Runtime Environment for Wireless (BREW)**

This is a mobile development environment, similar to J2ME, but with lower level access. It is available on CDMA chipsets and networks. BREW also allows for multiple programming languages to be used.

**Cell Broadcast**

Cell broadcast is a technology similar to SMS that provides a user / network with the ability to send a single message to multiple recipients. Unlike SMS, this technology only allows one-way communication from the network to the subscribers and subscribers cannot *send* such messages.

**Electronic Banking (e-banking)**

Banking services conducted by means of some electronic (as opposed to human) interface, e.g. ATM, POS, mobile handset, personal computer etc.

**High-end Handset**

This is a mobile device with advanced capabilities, such as the ability to run Java/J2ME programs or with the ability tor browse the Internet (WAP compatible sites) with a built-in browser application.

**I-Mode**

A Japanese-developed technology that allows services such as banking, content downloads and emails to be accessed from a mobile phone. The market share is limited since it is mainly contained within Japan.

**Interactive Voice Response (IVR)**

This is a technology by which a subscriber obtains voice access to a system. The system typically uses voice responses from high quality recorded voice prompts on the server side and DTMF responses or in some cases voice responses from the subscriber to select different options.

**Java 2 Micro Edition (J2ME)**

A Java program that is loaded and resident on a mobile device. Such a program can be launched by the user of the mobile device at will.

**Low-end Handset**

This is a mobile device that does not have so-called *high-end* features such as the ability to run Java/J2ME programs or a built-in Internet browser. A low-end handset will have capabilities such as voice calls, SMS and USSD.

**Mobile Access Channel (access channel / channel)**

This is a user-interface technology used for communications from a mobile device to a back-end server for the purpose of an m-commerce transaction.

**Mobile Banking (m-banking)**

Banking services provided via a cellular network to a mobile device. This is a subset of e-banking. Usually one of the functions that are made available in m-banking systems is that of m-payments.

**Mobile Bearer Channel (bearer channel)**

A bearer channel is the protocol technology that is used to transmit messages from the mobile device to the back-end application server.

**Mobile Device (device / handset)**

A hand-held mobile device used for communication via a cellular network, e.g. a cellular telephone.

**Mobile Execution Environment (MExE)**

This is a "concept" technology that does not seem to be used in any production system. It allows for subscribers to have control over the installed services on mobile devices. Some of the other technologies implement some of the features of this technology.

**Mobile Network**

A cellular network operated by a specific Mobile Network Operator.

**Mobile Network Operator (MNO)**

An institution that operates a mobile network is called a mobile network operator. This institution provides mobile devices and SIM cards to users and in return charge them for the usage of the cellular service.

**Mobile Payments (m-payments)**

These are financial payments done via a mobile-banking system.

**SIM Application Toolkit (SAT)**

This is a technology similar to WIG which enables XML-like scripts to be executed on SIM cards. The scripts are executed by an application (SIM browser) that is resident on the

SIM card and presents the user with a menu system. The SIM browser has access to special features built into the SIM card such as security keys and plug-ins.

**Security Dimensions**

These are a number of subdivisions, that could be measured individually and that together form a total security measurement.

**SIM Browser**

This is an application that is installed and executed on a SIM card. This application can execute special XML-like scripts that can also be loaded onto a SIM card. These scripts generally have access to information on the SIM card which may be hard to access by other applications.

**Short Message Service (SMS)**

A mobile text service that allows subscribers to send small text messages to one another. The technology allows for one sender to send a message to one receiver. Messages can be a maximum of 160 characters in length.

**Small to Medium Enterprises (SMEs)**

These are enterprises that are small in size in terms of financial revenue and employees.

**Spoofing**

It is a situation whereby a computer program successfully masquerades as another to gain illegal access to a system.

**Ubiquity**

For the purpose of this research, ubiquity refers to the availability of a specific technology with regards to the percentage of subscribers that can be reached with that specific technology.

**Ubiquity Dimensions**

These are subdivisions of a complete ubiquity measurement that can be measured individually.

**Unstructured Supplementary Service Data (USSD)**

USSD is a mobile messaging system similar to SMS, with the main difference that USSD is session based while SMS is message based. From an application point of view, this implies that USSD messages are processed synchronously, while SMS messages are processed asynchronously.

**WEB Clipping**

WEB Clipping is a technology that allows standard, PC-viewed web pages, normally not suited for mobile devices, to be parsed and restructured to be displayable on a mobile device. This technology is specific to a PALM device, but other similar technologies (like the Opera Mini browser) are available on other devices.

**Wireless Application Protocol (WAP)**

This is a technology that allows web content to be displayed on a mobile device. Usually the device has a built-in browser that can display the content and normally the content has to be designed specifically to target mobile devices.

**Wireless Internet Gateway (WIG)**

WIG consists of a scripting technology that allows a SIM browser (see *SIM Application Toolkit*) to execute a specific script that is loaded onto a SIM card. This technology is slightly different from SAT, but similar in structure.

**XHTML Mobile Profile (XHTML-MP)**

XHTML-MP is an extension of WAP that allows XHTML (well formed HTML) to be displayed on a mobile device. The mobile profile extensions enable specific mobile tags to be used that enable specific functionality on mobile devices.