



Mobile Banking Technology Options

**An Overview of the different mobile banking technology options,
and their impact on the mobile banking market.**

August 2007



Extending your payments franchise!

info@troytyla.com

Author: Gavin Troy Krugel

Acknowledgements

The document was completed with thanks to the support from the following individuals and companies:

GSM Association	Adrian Dodd, Chief Engineer James Moran, GSM Security Ben Soppitt, Director Strategic Initiatives, GSMA MMT	Interviews April-June 2007 London
GCash	James Iletto, GXchange	Interview in Barcelona February 2007
Fundamo	Hannes van Rensburg, CEO	Interview in Cape Town, March 2007
Vodacom	Jacques Voogt, Mobile Banking	e-mail correspondence
Risk Frontiers	Jenny Hoffmann, CEO	Introduction and guidance
Andrew Lake and Associates	Andrew Lake, CEO	Email correspondence
Cointel – Simplus	Various staff	Knowledge base and email correspondence
	Keith Smith	Contributor

Contents

1. INTRODUCTION	1
2. MOBILE BANKING STAKEHOLDERS.....	2
3. MOBILE BANKING PLATFORM IMPLEMENTATION OPTIONS.....	6
3.1. High Level Bank Channel Architecture	6
3.2. Levels of Mobile Banking Platform Implementations	8
3.3. Mobile Banking Platform High Level Architecture	8
3.4. Implementation Options:.....	10
3.4.1. Extension of a Banks Payments Franchise to Mobile.....	10
3.4.2. New Payments Franchise on Mobile	11
3.4.3. Multiple Channel, Multi Party, Shared, Mobile Banking Infrastructure	12
4. MOBILE BANKING BEARER TECHNOLOGY OPTIONS	13
Server-Side Technologies	13
Client-Side Technologies.....	13
4.1. SMS Banking Solutions	14
4.2. Interactive Voice Response (IVR).....	15
4.3. Unstructured Supplementary Service Data (USSD)	17
The Balance of your account is 100.00.....	18
4.4. Wireless Application Protocol (WAP).....	18
4.5. JAVA/J2ME	20
4.6. SIM Based Applications.....	21
5. COSTS AND MARKET SEGMENTATION IN MOBILE BANKING	23
5.1. The Impact on Cost, Device, and SIM of Mobile Bearer Technologies	23
5.2. Mobile Banking Strategies in Market Segmentation	26

6. MOBILE BANKING APPLICATION AND DATA SECURITY	28
6.1. TRADITIONAL BANKING SECURITY OPTIONS:	29
Unencrypted Data Over an unencrypted fixed communication link:	29
Unencrypted data over an encrypted fixed communication link:	29
Encrypted data over an encrypted fixed link:	29
Additional authentication and risk mitigation as an added security measure:	29
6.2. MOBILE BANKING SECURITY OPTIONS:	30
Base Station Base Station Mobile Operator Bank.....	30
SMS Banking Data Security	31
Base Station Base Station Mobile Operator Bank.....	31
IVR, USSD Banking Data Security:	32
Base Station Base Station Mobile Operator Bank.....	32
J2ME, WAP and S@T Banking Data Security.....	33
Base Station Base Station Mobile Operator Bank.....	33
Additional Authentication and risk mitigation in mobile banking:.....	34
7. REGULATORY IMPACT ON THE MOBILE BANKING TECHNOLOGY CHOSEN	35
8. CONCLUSIONS	35
9. ADDENDUM: EXTRACT OF THE GSMA MOBILE BANKING VENDOR ANALYSIS	36
THE ROLE OF THE MOBILE BANKING VENDOR.....	37
THE ROLE OF THE MOBILE NETWORK OPERATOR	37
BEARER CHANNEL ONLY	38
BEARER CHANNEL AND APPLICATION DEVELOPMENT	38
BANK INTEGRATION AND MNO WITH A MOBILE BANKING HUB	39

SIM APPLICATION PROVISIONING.....	39
MNO AS A BANK.....	39
THE ANALYSIS EVALUATES THE FOLLOWING COMPONENTS:.....	41
GEOGRAPHIC FIT	42
FUNCTIONALITY	44
TRANSACTIONS:.....	44
CHANNELS:	45
VENDOR BUSINESS MODELS.....	45
ABILITY TO IMPLEMENT	46
TECHNICAL ARCHITECTURE OPTIONS.....	47
AUDITS/CERTIFICATIONS/ENDORSEMENTS	47

1. Introduction

Created with initial funding from the United Kingdom's Department for International Development, FinMark Trust is an independent trust, which supports and promotes institutional and organisational development towards the objective of increasing access to financial services by the un-banked and under-serviced of southern Africa.

Much has been said about the potential for cell phone banking as it rides on the back of the explosion of cell phone usage in Africa and beyond (see Figure 1: African cell phone subscribers, BMI-T), and how it could dramatically lower the cost of banking and more effectively reach the mass market. Early pioneers such as MTN Banking, Globe, Smart, Celpay and WIZZIT Bank have all been showcased as leading innovators who are using technology to expand access to financial services in their various jurisdictions.

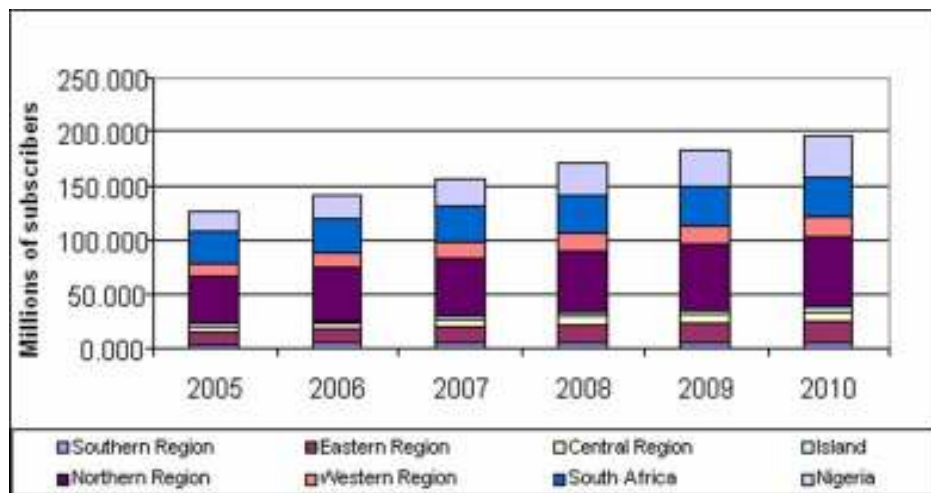


Figure 1: African cell phone subscribers, BMI-T

However, each of these cell phone banking models have different characteristics and can be classified as bank driven, joint-ventures, non-bank led or non-bank driven (Porteous, 2006). Whilst all the models vary in form, one of the driving forces behind all of them appears to be technology providers, each providing a particular technology, which is shaping the offerings and their ability to reach a particular market.

The objective of this paper is to understand what the impact of mobile transaction technology has on the business model for cell phone banking and thus the ability to interact and service consumers profitably. The paper will also look at how the business and infrastructure environment impacts the choices one can make in selecting the technology for mobile payments or cell phone banking.

2. Mobile Banking Stakeholders

The delivery of a mobile banking service to a consumer involves the participation of four primary players; A Bank, Mobile Network Operator (MNO), a Mobile Banking Technology Vendor, and the consumer.

In most instances the mobile banking vendor has been the pioneer in shaping industry adoption and lobbying the other two principle stakeholders on the value of extending the banking franchise to mobile.

The early pioneers of mobile transacting go back around 10 years. These initial visionaries have persisted in lobbying the banking industry over this time with little success, and where implemented, little consumer adoption¹.

However the consumer mobile market has matured and the various stakeholders (banks and MNOs) seem to have taken an interest and realised the potential value of the high penetration in mobile phones amongst their respective customer bases.

This is seen through the recurrent press coverage around new launches and new global initiatives to leverage this channel in banking.

This is also clear when looking at the number of known, deemed successful, implementations in the world.

The bank typically has a multi-channel approach to delivering transactional services to its customer base. Its channels include the traditional bricks and mortar branch, ATMs, POS and the internet. These channels have gone a long way in servicing the retail banks in delivering financial transaction volumes and assisting in extending the banks reach to its customers.

These channels come at a cost of infrastructure and implementation and can typically serve developed markets, or developing market urban and semi-urban areas where population density and the availability of infrastructure is readily available.

In developing markets the channels come at a cost to the consumer in the form of banking fees in exchange for the convenience of using the channel.

We have also seen a migration strategy from the banks to move their customers away from the more fixed-cost based infrastructures, such as branches, to those with less resource and operational costs such as ATMs, POS and ultimately the internet.

¹ Fundamo and Cointel-Simplus are both around 10 years old but have only had banks as customers in the past two years.

None of these channels have the ability to reach the consumer as thoroughly as the mobile phone. The coverage of the cell phone network in relation to the fixed infrastructure required for ATMs and branches ensures that the cell phone network and also the cell phone is clearly the more accessible channel by all consumers. The mobile phone is in most consumers' hands and banks have realised that the consumer does not need to travel to any bank infrastructure in order to use banking services, once they have implemented mobile banking.

Mobile banking represents a more cost efficient channel for the banks, allowing them to charge less for transactions, and permitting the consumer to have immediate access to information related to their bank accounts. These factors should translate into more transactions more often.²

The bank's mobile banking **options** include:

- *Leveraging the MNO bearer channel and infrastructure to extend its payments franchise to mobile facilities as a channel*³
- Leveraging the MNO brand, distribution network, and extended customer base to target new market segments⁴
- Allowing a MNO to use the bank's financial license and/or infrastructure to become a bank.⁵

The Mobile Network Operator (MNO) provides the mobile phone and the ability to use the mobile phone for providing banking services to the consumer.

The global mobile phone market is becoming more competitive, with reducing prices, increasing customer churn, and reduction in profits. The highly competitive mobile environment is also reflected in the number of mergers and acquisitions seen in the global market and therefore the sheer size of some of the MNO multinationals.

The MNO is increasingly focused on innovation in order to offer higher value to its customer base in an attempt to reduce customer churn, as well as a focus on new ways of generating revenue, even from sources not core to their current business.

²E.g. Increase in frequency of balance enquiries on Simplus Platform Mobile Banking Applications

³ E.g. First National Bank, South Africa, and HSBC, UK

⁴ E.g. MTN Banking, South Africa








⁵ E.g. SMART, Philippines

The MNO typically has a bigger customer base than that of a bank. In emerging markets, the number of mobile phone customers who have a relationship with a bank is significantly lower than people with mobile phones and no bank account.

The combination of the need to generate revenues outside of traditional telephony, to prevent customer churn, and the potential to leverage a requirement for financial services by un-banked mobile phone customers has led MNOs to invest in mobile banking.⁶

The MNOs mobile banking **options** include:

- *Providing the bearer channel for the bank to enable the extension of the bank's payments franchise to mobile facilities as a channel⁷*
- Lending its brand, distribution network and extended customer base to a bank to facilitate providing new banking products and services to the MNO's un-banked customers.
- Using its infrastructure, reach, customer base and cash float, to become a bank. This would be through a partner financial institution and its banking license, or through the successful application for a banking or emoney license.

	      	MNO as Bearer	MNO as Application	MNO/Bank Joint venture	MNO as Bank
Churn Reduction		No reduction in Churn as any MNO can offer the service	Reduction in Churn	Definite reduction in Churn	Definite reduction in churn
Regulatory and License Constraints		No impact	Low impact. PCI compliance	Banks typically facilitate regulatory compliance	High regulatory and license requirements
Brand		Not used	Not used	MNO Brand	MNO Brand
Banking Systems		None required	Financial Switching only	Some required	High infrastructure requirement.
Distribution Chain for cash handling etc.		Not used	Not Used	MNO and Bank	MNO only
Transactional Risk		None	Some	Half of the risk	All of the risk
Cost Revenue		Marginal Low	Some cost Good	High cost High	Very High Costs High

⁶ Vodacom invested in bearer channel enablement only by enabling banks within its WAP portal as well as allowing banks to use its channels to deliver financial services.

⁷ Discussed in this paper

CASE STUDY: SIMPLUS

COINTEL began in the late 90s by developing a means to electronically load prepaid airtime directly to the customer's account at the MNO without the customer having to buy a paper based recharge voucher.

Cointel extended this technology to additional transaction types and eventually full mobile banking, and branded it Simplus.

Cointel also migrated to later mobile technologies such as USSD (un-structured supplementary service data), JAVA and WAP.

Originally servicing its own commerce needs Cointel now services multiple MNOs, multiple banks, and even multiple markets from its on-behalf platform in South Africa.

Cointel supports multiple bearer channels. Cointel has since packaged and licensed its Simplus technology to other markets.

Figure 2: GSM Association MNO in Mobile Banking + David Porteous.⁸

The Mobile Banking Vendor supplies the technology that integrates the mobile banking participants (MNO, banking systems, user applications, access channels) and facilitates the translation of the banking instruction from the consumer's mobile phone to that of a financial message that can be understood by the banking systems.

The mobile banking vendor is often the catalyst for mobile banking in the market in that it promotes the business case of mobile banking to the MNO⁹ and the bank¹⁰.

The mobile banking vendors have also been the innovators behind mobile banking and have been doing mobile initiated transactions for around 10 years. Examples of this are Fundamo, Cointel (Simplus), SMART (GFG), and G-Cash (Utiba). Each being pioneers in their markets.

Only over the past few years have we seen bank or MNO initiatives to aggressively chase this new market segment and technology, even though we see mobile banking activities as far back as 10-12 years ago.

⁸ PCI – Payment Card Industry Compliance to security and processing standards.

⁹ Reduced churn, increase in network usage, increase in Average Revenue Per User (ARPU)

¹⁰ Increase in reach and therefore target market, increase in transaction volumes, customer retention

The mobile banking vendor has its roots in either:

- Developing applications or platforms to service its own commerce needs (Simplus), or
- Developing applications as foresight to a future with the mobile phone as a banking channel (Fundamo).

These roots have developed into business models that offer application service provision (ASP), or packaged licensing of technology, or both. In other words one can either pay for the use of the technology to a third party on a per transaction basis or license the system for use by internal operations.

The mobile banking vendors¹¹ play an integral part in the delivery of mobile banking to the customer.

In either business model the mobile banking system vendor or technology provider delivers the ability to do mobile banking, for a Bank, through a MNO, to a consumer.

In summary, the Mobile Banking system Vendor facilitates the integration of the bank system with that of the MNO bearer channel, and provides the mobile banking platform or the mobile banking application, that enables the consumer to bank using their mobile phone.

3. Mobile Banking Platform Implementation Options

3.1. High Level Bank Channel Architecture

Mobile banking is seen to be an extension of the existing payment infrastructure of a bank to mobile phones as a channel for the leveraging of the mobile network and its reach, to deliver banking services to consumers.

The mobile banking infrastructure thus sits in a similar technical environment to the banks ATMs, POS, branch and internet banking service offerings.

A bank's core banking system, the system that houses the consumer's account and related transaction management and history, would require a means to translate banking instructions, received from consumers, through one of the bank channels such as ATMs or the internet, into a format that the core banking system can process. This translation is normally performed by an

¹¹ Banks can develop their own applications in-house, in which case the IT department would be classified as the 'vendor'.

EFT channel switch¹². The EFT channel switch would switch transactions from the channel to the appropriate area within the core banking system.

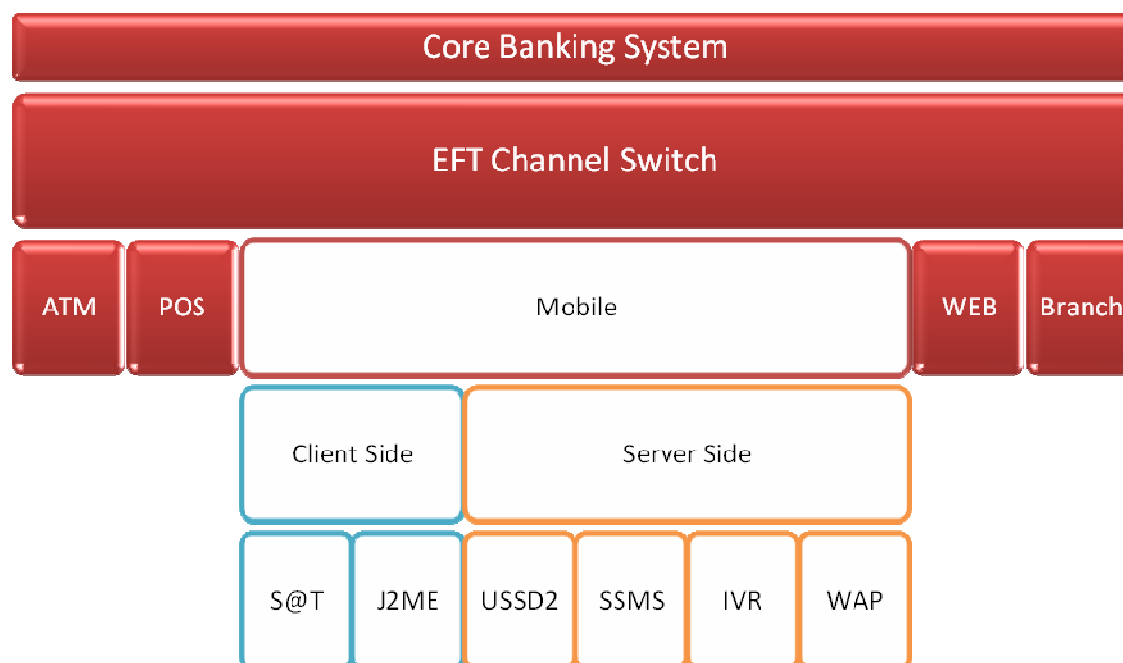


Figure 3: Mobile Banking in the overall banking architecture.

The mobile banking channel can be delivered to the consumer through two bearer or application environments.

Client-side applications are applications that reside on the consumers SIM card or on their actual mobile phone device. Client-side technologies include J2ME and S@T.

Server-side applications are developed on a server away from the consumer mobile phone or SIM card. Server-side technologies include USSD2, IVR, SSMS and WAP.

The bank would only need to select one of these bearer¹³ channels, or bearer channel strategies, for implementation. However, in some markets it would be wise to implement more than one bearer channel in order to manage consumer take up and the risk associated with non-take up of a specific technology. The selected bearer channel does not have an affect on where the mobile banking platform should sit.

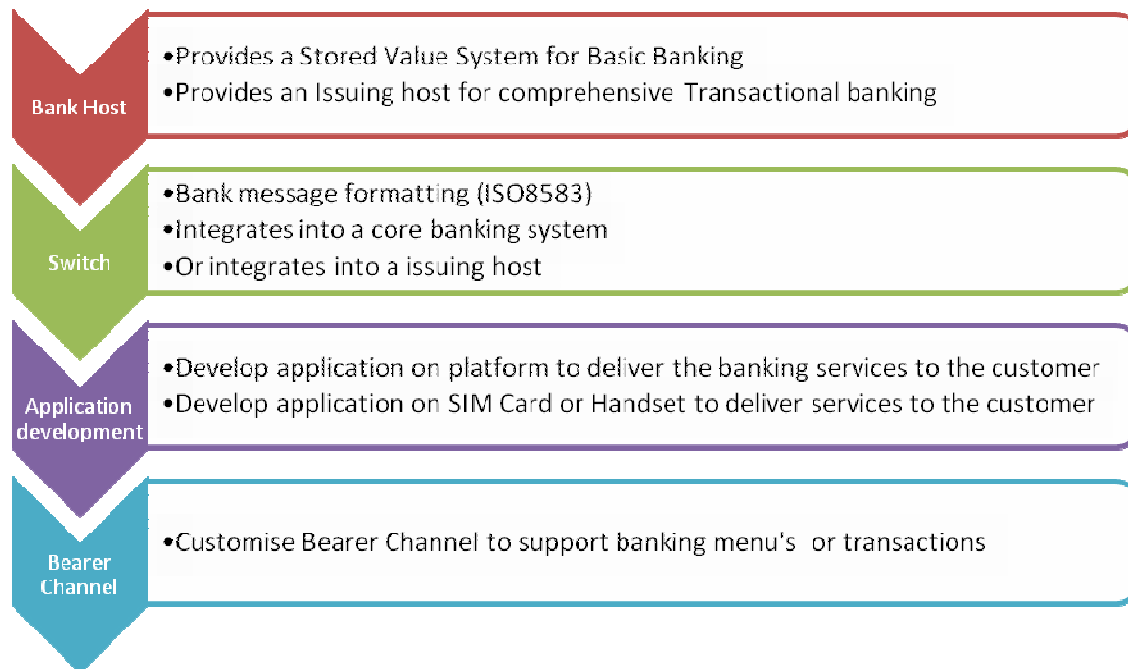
¹² An Electronic Funds Transfer, EFT, or Financial Switch accepts, translates and forwards transactions from multiple channels to the bank's core systems. This can sit within the bank or the bank's third party processor.

¹³ Access channel for a consumer from their mobile phone, such as SSMS, WAP, USSD2, etc.

3.2. Levels of Mobile Banking Platform Implementations

The extension of the payment franchise to mobile can be as simple as a bank channel enablement or as complex as a complete bank system implementation depending on what infrastructure already exists, and that which can be re-used as part of the implementation.

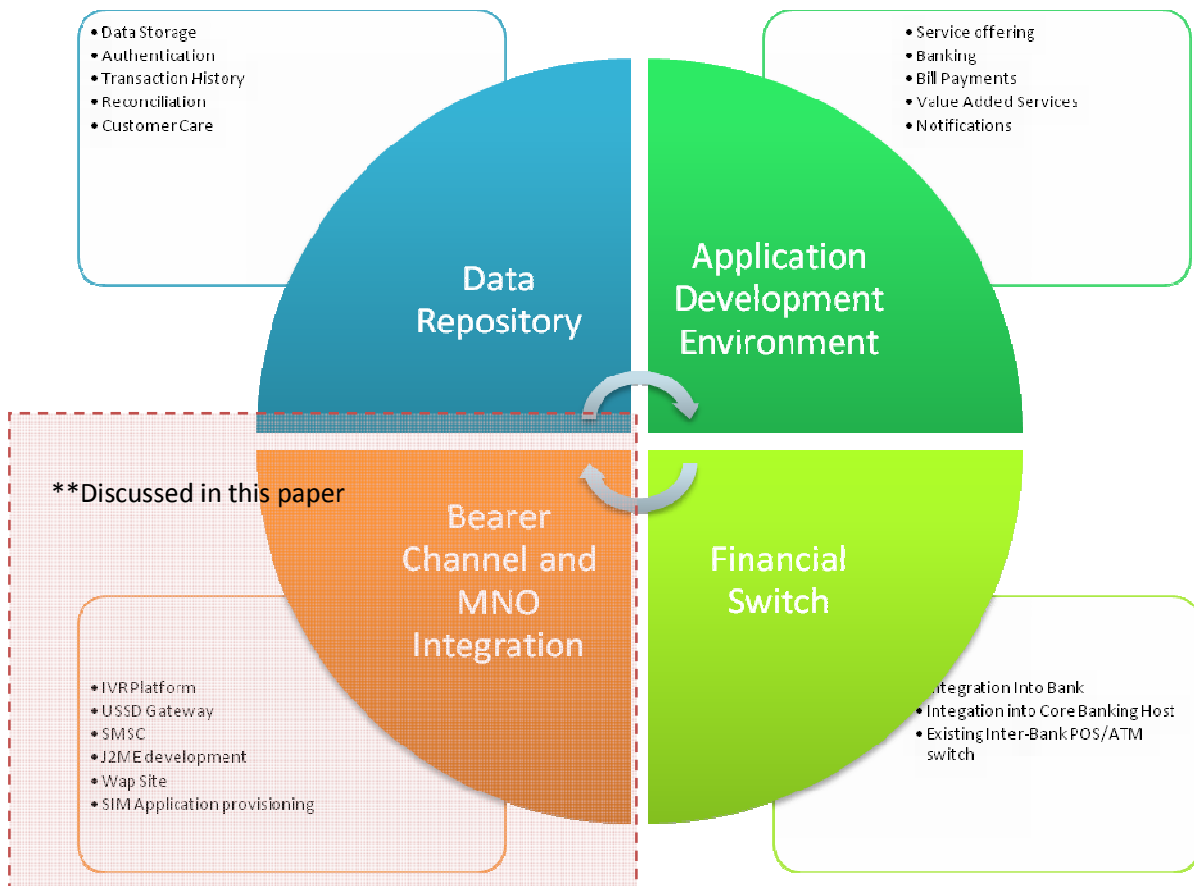
Figure 4: Mobile Banking solutions require the following layers in Mobile Banking enablement:



3.3. Mobile Banking Platform High Level Architecture

If we look at a typical bank as one that already has a core banking system, then the mobile banking platform that the bank would use, or integrate with, would have the following components:

Figure 5: Components of a Mobile Banking Platform



The diagram above reflects a typical mobile banking service. The service would require integration into an MNO to facilitate the usage of the network's bearer channels and in order to access the consumer's mobile phone.

The Data Repository stores enough customer information, to facilitate the processing of financial transactions. The data repository would also house sufficient information to authenticate the customer in each transaction. By housing transactional and consumer data, the repository would also facilitate customer care, and the reconciliation of certain financial transactions that use the application development environment to fulfil services. E.g. selling airtime would require reconciliation between the transactions processed and the airtime loaded by the network operator.

The Application Development Environment facilitates the actual service development to the consumer, such as banking menus and commands. It may house the integration of third parties in supporting value added services such as bill payments or airtime sales. The application development environment fosters the intelligence delivered to the consumers handset, whether client or server side.

The Financial Switch would act as the interface to the bank's core banking system. Instructions collected by the application development environment through the MNO interface, and using data from the data repository, are translated through the financial switch into a transaction format that the bank can use.

3.4. Implementation Options:

3.4.1. Extension of a Banks Payments Franchise to Mobile

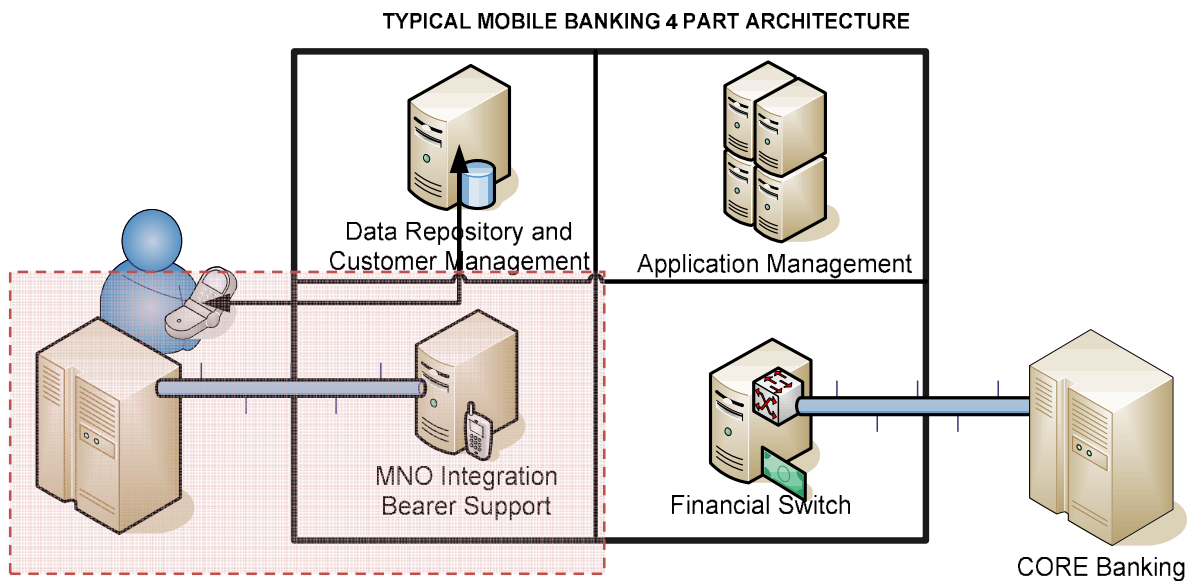


Figure 6: Architecture of a platform for the extension of the Banks payments franchise to Mobile

The diagram shows a bank that uses its existing core banking system and the implementation of a mobile banking platform to deliver Mobile Banking to its consumer base.

The platform allows a consumer with an application on their phone, or on a server, to authenticate (usually with a PIN) and deliver an instruction to the platform.

The platform, depicted in the diagram, will extract the consumer's bank account data and pass the instruction to the application management environment.

The application environment will have a set of processes to follow for this specific transaction. Once completed, the application environment will have submitted a financial transaction into the financial switch and from there into the core banking system.

The core banking system will process the transaction and submit a confirmation back into the platform that would be delivered back to the consumer.

The platform can be housed at the bank, MNO, or third-party processor. The integration effort is similar to that of interfacing into a bank.

3.4.2. New Payments Franchise on Mobile

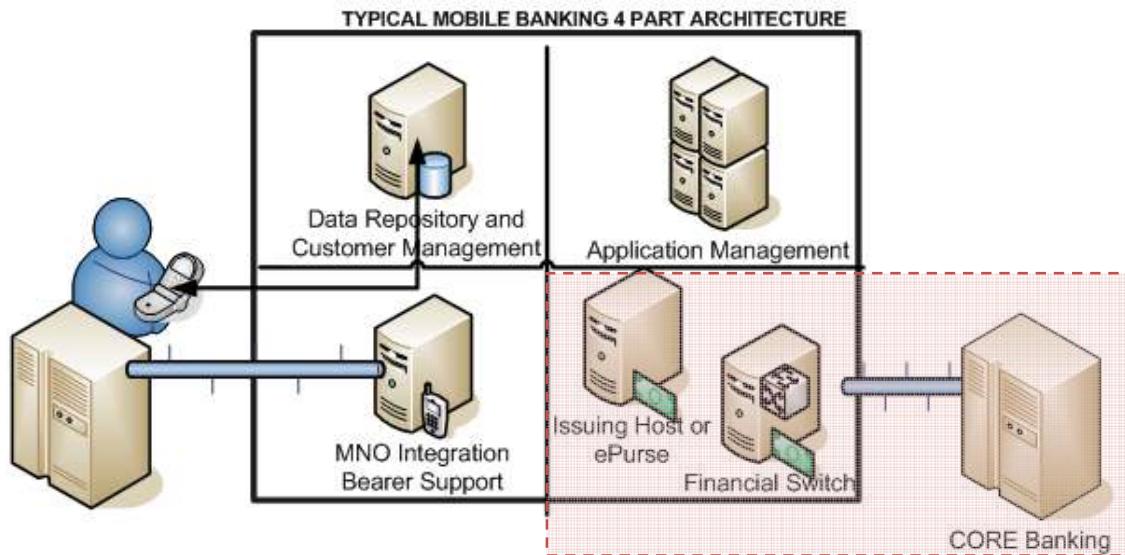


Figure 7: Platform Architecture of New Payments Franchise on Mobile

In this diagram, the implementation facilitates a pseudo banking environment away from the core banking system.

The development of a purse or stored value balance on the SIM card or on a server would allow for an entry level transactional capability because the service provider does not have to own a complete core banking system.

A key business question would be how to load the purse or stored value application with cash since there is no bank account connected to the traditional channels of electronic credits, ATMs and branches, for example.

The core banking system integration depicted above would be a means to load the stored value application from a traditional bank account and then use the stored value application balance for transacting. However this requires the customer to have a bank account as well as the wallet which may counter balance the 'ease of access' benefits and cost benefits of having a wallet in the first place.

The consumer-facing technology (bearer channel or application) would not affect the architecture, with the exception of the placement of where the stored value purse is hosted (server or client side).

The platform could once again sit in either the bank or a third party processor (which may include an MNO).

3.4.3. Multiple Channel, Multi Party, Shared, Mobile Banking Infrastructure

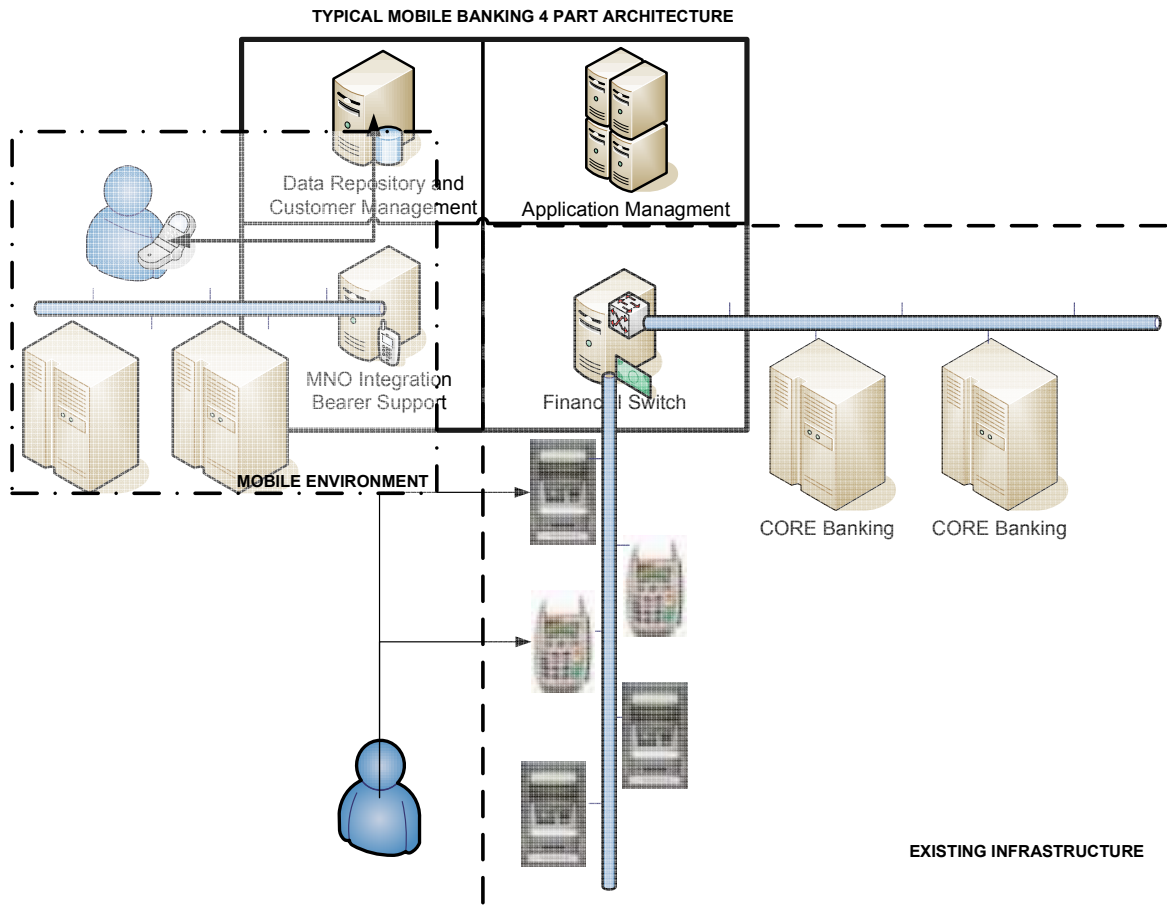


Figure 8: Shared Infrastructure Architecture

The diagram above depicts a typical shared, or on-behalf, platform in a market. Here, the mobile banking infrastructure has been implemented around a shared industry ATM/POS/EFT switch.

If this environment is implemented in a bank, and in a MNO neutral fashion, the platform owner would be able to service multiple banks and multiple MNOs thus allowing the clients of any of those banks or those MNOs to transact with each other.

The bearer channel supported would not affect the architecture but may affect the customisation of the consumer-facing technologies. Server-side applications are easily customisable, as they are in a central location, Client-side applications would require customisation per bank and per device or SIM type.

The same ATM switch can be used for the processing of mobile banking transactions.

This architecture could be implemented at a third-party processor (not bank or MNO) or multi-industry agreed location.

Addendum 1: EXTRACT: GSMA Mobile Banking Vendor Analysis Overview. This addendum will give some guidelines on what to look for when sourcing a mobile banking vendor.

4. Mobile Banking Bearer Technology Options

This section addresses the front-end component or consumer-facing Mobile Banking Technologies. This component of the end-to-end mobile banking value chain is typically supplied or customised by either a mobile banking vendor or the specialised technology unit within a bank.

These Mobile Banking Technologies can be categorised into two environments:

Server-Side Technologies

Server-side technologies are those applications built on a server, away from the consumer's SIM or Mobile handset. Examples of server-side technologies would be SMS, IVR, USSD2 and WAP.

Client-Side Technologies

Client-side technologies are those applications, solutions and service offerings built or embedded on a consumer SIM or mobile handset. Examples of client-side applications are S@T and J2ME (JAVA).

These consumer-facing technologies each have differing characteristics and processes.

Each of these technologies requires that the consumer register or activate the application with the bank/MNO/vendor offering the service in the market.

This registration process is defined by the service provider and serves as an initial identification of the consumer to ensure ongoing trust in, and security of, the transaction. There are numerous methods of registering or activating customers in existence, all of which require the endorsement of the bank offering the service.

Consumer registration often creates a barrier to consumer adoption, but serves as a necessary step in the process of eliminating fraud and potential transactional risk in the offering (as well as being a regulatory requirement).

In server-side applications, consumer data that enables the processing of transactions, such as account/card details, are typically stored in a secured environment, on a server at a bank or at their allocated service provider/vendor.

In client-side applications, the consumer data is typically stored on the application, or entered by the consumer, and encrypted by the application in the SIM or handset.

Each of the server-side and client-side applications are briefly described below.



4.1. SMS Banking Solutions

SMS (Short Messaging Service) allows users to send and receive text messages on a mobile phone using the numbered keypad on the handset to input characters. Each message can be up to 160 characters long and sent to and from users of different operator networks. All mobile phones available today support SMS. Indeed, SMS has become a global phenomenon, with billions of text messages sent worldwide every week. It is estimated that a worldwide total of 1 trillion text messages were sent in 2005.

In addition to the person-to-person SMS, a large variety of content-based text messaging services are available. The majority of GSM operators offer users the ability to subscribe to services that send news, sport and entertainment content direct to a mobile phone in the form of an SMS.¹⁴

SMS Banking requires a registered customer to initiate a transaction by sending a structured SMS (SSMS) message to the Mobile Banking Service.

This SSMS requires a tag word identifier to instruct the SMS gateway to submit the message to the correct SMS application. A tag word is the first word in the SSMS.

The balance of the SSMS would hold the instruction from the customer to the Mobile Banking application.

E.g.: '**bank_balance_PIN**' for a sms based bank balance enquiry;

or

bank_transfer_cheque_savings_100.00_PIN' for a transfer from a cheque account to a savings account of an amount of 100.00.

¹⁴ www.gsmworld.com

In each of these examples the SSMS would be sent to a SMS short code or address (a shorter version of a phone number). The SSMS would pass from the consumer's handset through the GSM Network to the MNO SMSC (Short Message Service Centre).

A SMSC stores and forwards the SSMS to the SMS Gateway allocated to the short code used by the Mobile Banking Service Provider.

The Mobile Banking Service Provider would use the consumer's mobile number, forwarded by the SMSC with the SSMS, to identify the consumer and respond to the consumer's request.

The response would follow the same return path and, in the examples given above, would respond to the consumer with an SMS confirmation message. E.g. 'Bank Balance 150.00' or 'Transfer from cheque to savings of 100.00 successful'.

4.2. Interactive Voice Response (IVR)

In *telephony*, interactive voice response, or IVR, is a phone technology that allows a person, typically a telephone caller, to select options from a voice menu and interact with the phone system. A pre-recorded voice prompt is played and the caller presses a number on a telephone keypad to select an option, i.e. "press 1 for yes, press 2 for no". *Speech recognition* can also interpret the caller's simple spoken answer such as "yes", "no", or more complex words, sentences and business names, or a number as a valid response to the voice prompt.

DTMF signals (entered from the telephone keypad) and *natural language speech recognition* interpret the caller's response to voice prompts.¹⁵

IVR is the oldest form of consumer-facing mobile banking technology. IVR has been used prior to the existence of mobile phones in the form of telephone banking and is still in use today.

IVR requires a registered consumer to make a call to a published telephone number and be answered by a pre-recorded voice that presents various menu options to the consumer.

The IVR system would then take the necessary instructions from the consumer by recording the tones of the number selections that the consumer enters on the key pad, or through spoken commands, and creates an instruction that is given to the service provider/bank.

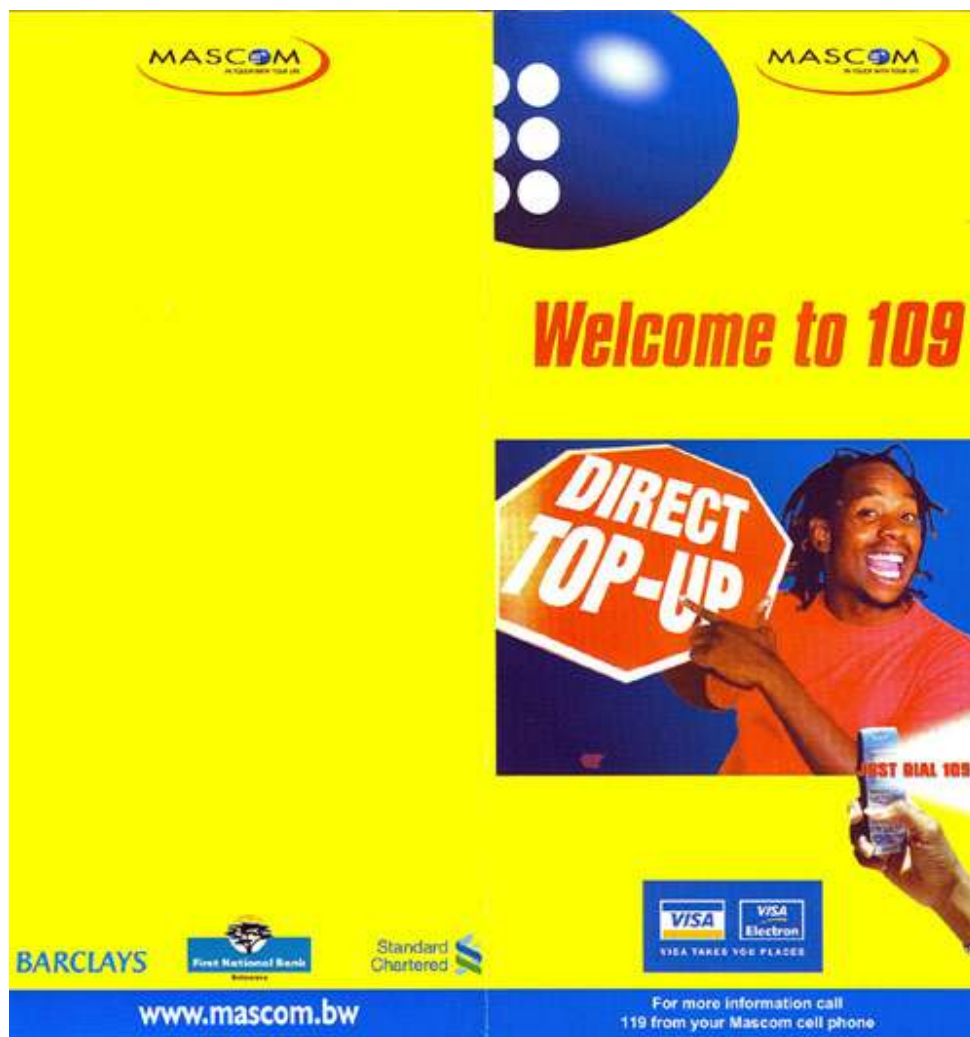
The service provider would use the consumer's mobile number forwarded by the network operator to identify the consumer and as a factor of authentication.

¹⁵ www.wikipedia.org

The channel can be used by any mobile device and any consumer capable of making a call.

The service provider is required to have an IVR system which can cost as little as US\$7000.00. However, it can also scale up to be fairly expensive depending on the number of customers that need to be served.

IVR systems are user friendly but may prove expensive to maintain and expensive to the consumer who needs to make what can be a relatively lengthy call. Of course, this is dependent on who pays, depending on whether it is a free phone number or not.





4.3. Unstructured Supplementary Service Data (USSD)

In its simplest definition, USSD is a menu driven form of SMS where a customer would receive a text menu on their phone as opposed to a string of words.

USSD is a data bearer channel in the GSM network. Like SMS, it transports small messages of up to 160 characters between the mobile handset and the network. Unlike SMS, which is 'store and forward', USSD is session based and can provide an interactive dialog between the user and a certain set of applications. In other words, both sides of the dialogue happen during a session whereas an SMS based interaction is broken into each segment of communication between the client and the service.

USSD1 only allows one way communication to the network, USSD2 allows two way communications between the user and the network. With USSD1, the interaction between the user and the service would be broken into each communication segment, much like SMS. With USSD2 it would be held in the same session and allow for a flowing conversation between the user and the service. This is similar to e-mail and instant messaging, e-mail waits for the recipient to read and respond while as instant messaging allows for immediate dialogue. USSD is as standard a feature as SMS and is available in an estimated 95% of handsets today¹⁶.

USSD requires no pre-configuration on the consumers SIM or handset and is already built into most GSM networks. MNOs do, however, need to commercialise the product by establishing the necessary bearer channel billing capability, and promoting the use of USSD for value added services in addition to internal network and customer care use. E.g. from *100# which would deliver an SMS balance of your prepaid airtime account to a more intuitive full service menu as discussed below.¹⁷

A registered consumer would dial a number that includes *s and #s. This number could be saved in the consumer's phone book as the bank's name to avoid confusion in dialling or having to remember the USSD string.

¹⁶ GSMA chief Architect

¹⁷ SICAP

Welcome to BANK, reply with:

1 for balance enquiries

2 for inter-account transfers

3 for person to person payments

4 for bill payments

5 for airtime top up

An example of a USSD string would be *120*2265#. 2265 spells bank and therefore could be marketed as *120*bank#. ¹⁸

Once the consumer has entered, and dialled the USSD string, the consumer's request for the service would be passed through the network to the USSD gateway at the MNO, which in turn would recognise who the service provider/bank was and forward the request to that service provider. ¹⁹

The service provider would respond by forwarding to the consumer, through the MNO, a text based menu similar to the one on the left.

The consumer would receive this menu on their screen, press the reply button on their phone and enter the number of the option that they required.

Example: Press reply, enter 1.

To which the service provider would collect the balance information for the consumer and send back a message that says:

The Balance of your account is 100.00.

4.4. Wireless Application Protocol (WAP)

WAP is best described as the internet on a mobile phone.

¹⁸ Live demo application are provided by Simplus which can be used by any Vodacom or MTN South Africa mobile phone

¹⁹ USSD strings are registered with the MNO in order for the MNO to recognise where to send the request. E.g. *120*949# belongs to Wizzit Bank and is registered at MTN, Vodacom and Cell C and is switched to Wizzit or their processor for completion.

WAP is an open international standard for applications that use **wireless communication**. Its principal application is to enable access to the **Internet** from a **mobile phone** or **PDA**.

A WAP browser provides all of the basic services of a computer based **web browser** but is simplified to operate within the restrictions of a mobile phone. WAP is now the protocol used for the majority of the world's mobile internet sites, known as WAP sites.

Mobile internet sites, or WAP sites, are **websites** written in, or dynamically converted to, WML (**Wireless Mark-up Language**) and accessed via the WAP browser.²⁰

WAP or mobile internet banking offers a consumer a similar experience to that of internet banking.

The consumer would browse to a mobile internet site by accessing the WAP browser on their mobile phone and entering the website address.

The actual banking application resides at the bank and is secured and monitored in the same way as an internet banking website.

The mobile phone and bearer (GPRS) is used to display or transmit the data between the consumer and the bank.

A consumer's handset would need to be capable (functionality developed/loaded by the handset manufacturer), and have the right configuration (provided by the MNO), in order to support WAP Banking.

MNOs often segment this functionality to post-paid customers only.

WAP IMPLEMENTATION

[HTTPS://WWW.NEDBANKMOBILE.CO.ZA](https://www.nedbankmobile.co.za)

[HTTPS://IB.ABSA.CO.ZA/IB/MB.DO](https://ib.absa.co.za/ib/mb.do)

²⁰ www.wikipedia.org



4.5. JAVA/J2ME

J2ME (Java 2 Micro Edition) is a feature that allows the device to run small, user-installable software applications written especially for mobile devices such as phones.²¹

J2ME requires a phone that can support the GPRS download of the initial application, assuming the phone is not pre-provisioned with the application.

The phone would have to also have enough memory capability to support or house the application, and sufficient graphic ability to display the application.

Once installed on the phone, the application would use GPRS, USSD or SMS to carry the consumer data or instruction from the device to the service provider. This can be in an encrypted format.

The J2ME environment can be MNO agnostic in that the application can be downloaded and used across any MNO that supports mobile internet.

The user experience is similar to that of a web site and brings the same content and graphic rich benefits of the internet to the mobile phone. But the application can impact the consumer in the initial download process due to their phone not being provisioned properly by the handset manufacturer or their GPRS capability not being enabled at the network.

These barriers affect all client-side applications.

A consumer would browse through his phone menu until they find the J2ME application, select and launch the application, and follow the JAVA browser menus to complete a transaction.

The data is typically encrypted prior to leaving the handset and being sent to the service provider or bank. Once received, the service provider or bank would decrypt the message and process the consumer's instruction.

J2ME applications can be pushed to the mobile phone by a service provider²² or downloaded by a consumer by accessing the service provider's mobile internet site.

²¹ www.phonescoop.com

²² Including banks



4.6. SIM Based Applications

The SIM Application Toolkit (SAT/S@T) allows for the service provider or bank to house the consumer's mobile banking menu within the SIM card.

*The SIM Application Toolkit (commonly referred to as STK) is a standard of the **GSM** system which enables the **SIM** to initiate actions which can be used for various value added services.*

The SIM Application Toolkit consists of a set of commands programmed into the SIM card which define how the SIM should interact directly with the outside world and initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user, and access or control access to the network. The SIM also gives commands to the handset, such as 'display menu' and 'ask for user input'.

STK has been deployed by many mobile operators around the world for many applications, where a menu-based approach is required, such as mobile banking and content browsing.²³

The challenge in SIM based applications is getting the application onto a SIM card that already exists in the market.

The service provider has the option of sending the application Over The Air (OTA), which entails the delivery of several encrypted SMS messages that self-configure the application on the SIM, or, provisioning a new SIM card with the application already embedded within the SIM.

The latter has an economic impact on the network operator and the existing consumer in that the consumer would have to obtain a new SIM card in order to use the application.

Once the application is on the SIM, instructions from the consumer can be entered, encrypted, and transported by SMS to the service provider or bank.

There may be difficulty in upgrading or making changes to the application on the SIM as the consumer would have to re-provision the application in a process similar to that described

²³ www.wikipedia.org

above; or the network operator would have to re-load the application over the air to each and every SIM card each time they make a change to the application.

A benefit of SIM Based Applications is the ability of the network operator or bank to own a piece of the real estate on the SIM Card. Since the SIM card is provided by a specific MNO, this ensures the prevention of churn for that MNO, and ensures that the bank's specific application is on the SIM and therefore provides similar benefits to the bank.

5. Costs and Market Segmentation in Mobile Banking

5.1. The Impact on Cost, Device, and SIM of Mobile Bearer Technologies



GXChange, known as GCash is a Globe Telecom initiative in the Philippines.

The service focuses on mobile initiated person-to-person payments, bill payments, international remittance transactions, and includes 6000 partner merchant locations.

Initially launched around three years ago, GCash built the application on a SIM card and provisioned the service, which was targeted at higher income groups that would have, or could afford, the higher specified US\$2 SIM.

The consumer was required to exchange their old SIM for a SIM that incorporated the new application.

The uptake was dismal, and after a year, GCash moved to develop an application that did not require the user to swap their SIM, and that is SMS banking.

GCash customers register for the service at one of 6000 outlets and, once registered, are only required to send an SMS in order to process a transaction.

The consumer uptake improved dramatically and is largely attributed to the bearer channel and the large distribution chain.

Admittedly, the SMS bearer does not offer the end-to-end security that a SIM based application would offer. This however was weighted against the risk of no or marginal uptake.

Over the past few years GCash have saturated the market with SIM embedded applications and are now at a saturation level that would allow them to begin to seamlessly migrate their customer base across to the more secure client-side application.

	Handset Penetration	SIM	Initial Download	Transaction Cost
SSMS	100% - all handsets	100% all SIM cards	No download	US\$0.03 up to US\$0.08 per SMS. Average transaction would require two SMS from the consumer and two returned from the bank. The bank would pay for their leg at a negotiated bulk rate. Total Consumer bearer cost per transaction would be US\$0.14 and for the bank US\$0.06.
IVR	100% - all handsets	100% all SIM cards	No download	As per consumer tariff. US\$0.32c per minute.
USSD2	95% of handsets	100% of SIM cards	No download	US\$0.03 per 20 seconds, average transaction 40 seconds. Transaction cost to consumer US\$0.06.
WAP	Post-paid customers for GPRS connectivity, higher end handsets. Approx 30% penetration and also at the top of the market for WAP2.	100% SIM cards	No download of application	GPRS data rates. Transaction would use up around 1-2kb and would be priced between US\$0.01 and US\$0.03 per transaction.
J2ME	Post-paid customers for GPRS connectivity, Java capable handsets. Approx 30% and also at the top of the market.	Does not affect SIM card	Initial download of application across GPRS, GPRS rates would apply. US\$0.29c per meg.	GPRS data rates. Transaction would use up around 1-2kb and would be priced between US\$0.01 and US\$0.03 per transaction.
STK	Handset capable of 32k and up SIM Card – approx 98% South African market.	32k and up. May require a customer to purchase a new SIM card. Free, if consumer does not mind changing their mobile number, up to US\$20.00. Predominantly post-paid customers would require a SIM swap as they do not churn as often as prepaid. Suggested	Initial download using packet data across SMS. 5-8 SMSs typically. Free to the consumer. If charged would be charged to the bank at a bulk rate of US\$0.03 per SMS. Maximum of US\$0.24c.	SMS bearer for the encrypted messages

Figure 9: Impact of bearer technology on Device, SIM, Consumer and Bank transaction costs²⁴:

The initial cost to the consumer is affected by the type of handset required, and whether or not the consumer has a capable SIM card to house the application.

It seems that the higher the requirement for a more capable handset, the lower the cost of transacting and the better the consumer experience (colours and graphics).

²⁴ Namibia, South Africa and Kenya. Market costs and device penetration estimates from Vodacom, MTN and MTC Namibia.

This implies that the higher-end technologies such as WAP and J2ME can be targeted only at the top 30% of the mobile and banking market, and that SMS, USSD2, S@T and IVR can be targeted at the bulk of the market.

The 30% WAP and J2ME market probably have access to internet and are also used to a higher graphic content. They would grasp the technology requirements more easily, and thus be able to download an application or find the browser on their phone and browse to a mobile banking website.

The 70% base of the market may not be so technically literate and would thus rather make a call or send an SMS as this is what they are used to doing.

S@T, along with USSD2, SMS and IVR, offer close to full market penetration. However, literacy levels may prove to make S@T more difficult to download and then to browse through the phone's menus to find the application.

5.2. Mobile Banking Strategies in Market Segmentation

Selecting the right technology for your market will, firstly, require some work to understand the market's technology environment. Some key elements are:

- Who is your target market and which mobile devices do they have?
- What kind of user experience and value proposition would be sufficient/appropriate in servicing your target market?
- What are the bearer channel costs related to this transaction and is it affordable to your target market?
- Does your target market have access to the bearer channel?
- Are you able to get the application onto your consumer's phone or handset without requiring the consumer to have an in-depth knowledge of the technology?
- Is the bearer channel selected secure enough for the risk profile of the customer you are targeting? Is it secure enough to protect the bank from any reputation risk if security is breached? Are there sufficient means to manage the risk around the bearer channel chosen?
- Does the channel comply with any financial processing rules and regulations relating to: the method of processing; authentication of the customer; transfer of data; and levels of encryption, yet still deliver on the business requirement?

A bank with a single market segment that a certain bearer technology suits in regard to access; cost; and device and SIM dependency, should implement this single bearer channel and focus its efforts on consumer education and increasing usage.

In a more complex market segment, or an unknown market environment, a multi-bearer strategy may suit. In this way you mitigate the risk of one technology not being taken up by the consumer.

There are good examples of focused as well as spread bearer technology strategies:

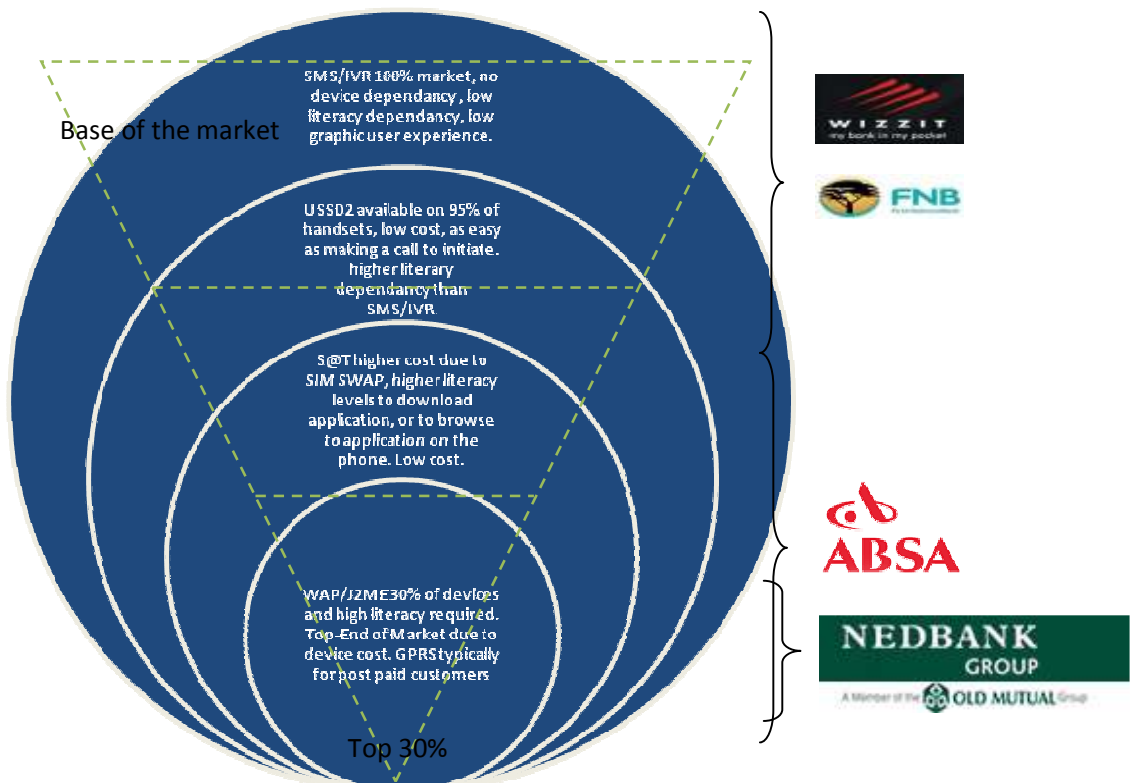


Figure 10: Market Segmentation by Mobile Bearer and Banking Market Segment

6. Mobile Banking Application and Data Security

‘Over-the-air’ or ‘in-the-clear’ are terms often used in the financial industry when referring to banking transactions transported across unencrypted communication protocols.

The mobile bearer channels have been seen to be ‘in-the clear’ largely due to the understanding that your data travels across the air (literally) and thus can’t possibly be safe. The concerns are that a fraudster is able to tap-in or listen in to your call, or data transmission, and record the data for malicious or fraudulent reasons.

The facts prove differently. GSM security is as strong, and if not stronger, than that of your traditional fixed line communications. It would take money, time and effort to be able to actually penetrate the GSM network, steal data, and then use it fraudulently. Moreover, if this were probable in Mobile Banking, the fraudster would still only be able to access a limited amount of funds from a consumers account for the reasons given below.

An overview of what it would take to ‘listen’ in on a call or data transmission over the GSM networks follows:

The fraudster would have to know where the customer would be at the time of the call, and also know the customer’s mobile number, and be able to travel as fast as the call is travelling from one base station to the next. On top of the mobility challenge, the fraudster would then still need to decipher the GSM encryption, and find a way to identify the particular mobile communication, considering that the customer identification as a GSM consumer is kept hidden for privacy purposes.

If one assumes that the fraudster was able to do achieve all of the above, they would then be subjected to the relevant velocity checks and transaction limits levied by the bank or their platform provider.

It therefore seems not feasible for a fraudster to expend his money and energies on attempting to break the communication layer. But it may still not be sufficient for banking in that it only provides unencrypted data through an encrypted channel.

In comparing fixed line communication protocols to that of mobile, a clear differentiation on the protection of the carried data emerges and is outlined below.

6.1. Traditional Banking Security Options:

The diagrams below show the options that are available for securing data across traditional fixed-line communication:

Unencrypted Data Over an unencrypted fixed communication link:



This is not an ideal solution for banking in that it offers no protection of the data or the actual communication protocol, leaving the communication link easy to penetrate and the data easily accessible.

Unencrypted data over an encrypted fixed communication link:



This would secure the outer communication layer, making it difficult for anyone to tap into the communication layer in order to get to the data that is being carried to the bank. However, the unencrypted data is at risk.

Encrypted data over an encrypted fixed link:



This is typically how a bank's data is carried from its consumer through its channels to its host. Encrypted data sent across an encrypted communication layer. The data is typically encrypted at the channel i.e. at the ATM or POS.

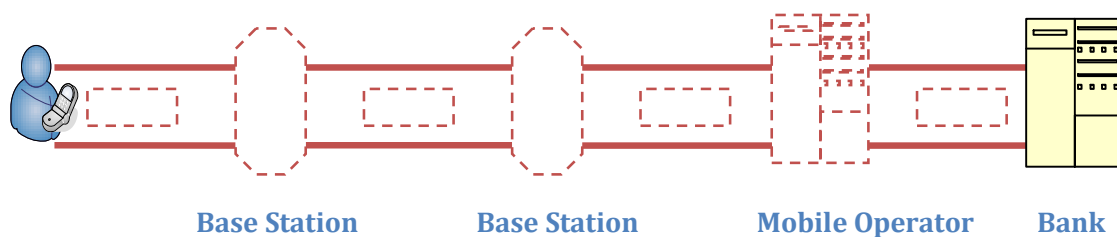
Additional authentication and risk mitigation as an added security measure:

In traditional banking environments we have risk mitigation and consumer authentication such as:

- Two factors of authentication such as the ATM card and ATM PIN ensures that you are able to confirm that it is the consumer you are receiving transactions from.
- Fraud monitoring and prevention, such as consumer spend behaviour and geographic spend behaviour.
- Velocity checks and spend limits, preventing no more than a defined number of transactions from occurring and also preventing no more than a set amount per day from being spent.

6.2. Mobile Banking Security Options:

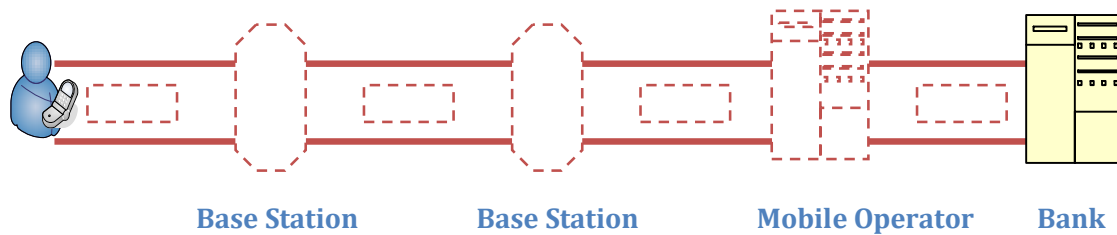
The diagram bellow shows the options you have for securing data across the GSM Channel:



Data carried across the mobile network is protected by the standard GSM security protocols at the communication layer. The subscriber identity is also protected across this chain. The risk in transporting data across the GSM channel may be found in the number of stops the data makes before reaching the bank. Unlike fixed line communication, data being carried across the mobile network jumps from one base station to the next, which means that the chain of encrypted communication is broken. The data is also unencrypted when it hits the network operator. Thus, there is a broken encryption between the consumer and the bank.

This differs per bearer channel or application used in mobile banking:

SMS Banking Data Security



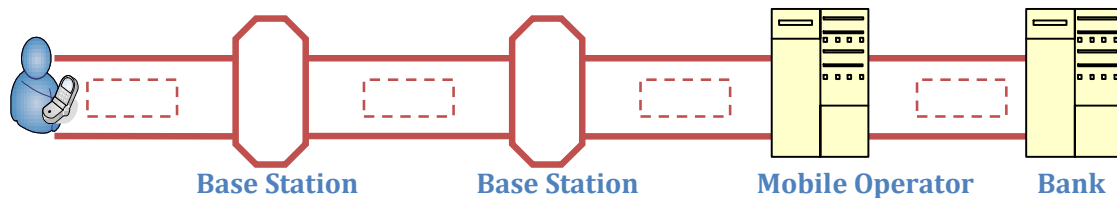
SMS banking is deemed to be the least secure of the mobile bearer channels. This is due to the number of points that the SMS data is available to others in a clear or unencrypted format.

A consumer would initiate a transaction by sending an SMS to the bank using the bank's SMS short code as a terminating address.

The SMS would be automatically **stored on the handset** and be available to anyone that looks at the consumer's phone. The SMS would then pass through the **encrypted GSM communication channel**, through the base stations and terminate at the mobile network operator, where it is typically **stored unencrypted**. The MNO may at this point pass the message onto the bank's wireless application processor, SMS gateway, or mobile banking processor (which may be a third party), where it is stored either encrypted or **unencrypted**. The third party would then pass the message to the bank across an **encrypted** fixed line to the bank where it is typically stored in a **secured environment**.

As can be seen, there are many points of exposure.

IVR, USSD Banking Data Security:



IVR, being a voice call, is protected by both the **encrypted GSM communication layer**²⁵ as well as the **GSM protection of the subscriber identity** of the consumer²⁶ and it is carried across the mobile network to the bank's IVR. Only at this point are the entries that the consumer has keyed into their phone, stored. If this is in the bank's environment it should be **secure**, but if on an 'on-behalf' platform it **may not be secure**.

USSD2 is similar to IVR for to data security in that it opens a **single session** between the device and the USSD2 application at the network operator, processor, or bank. In other words the transaction is completed while the session is open and is not stored for subsequent completion.

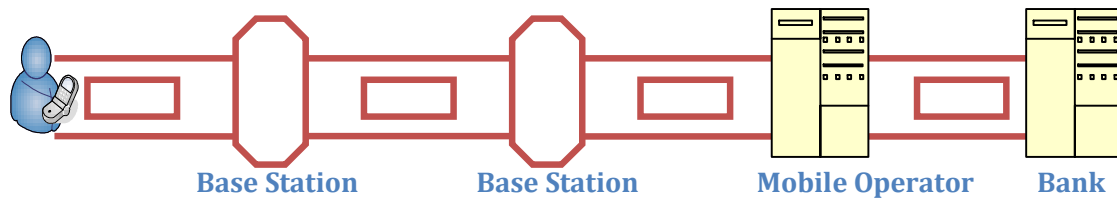
The end-to-end transaction flow is across the **encrypted GSM communication layer** and the **subscriber identity is also hidden**. The data can also be **encrypted** as soon as it terminates at the USSD2 gateway sitting at the network operator, processor or bank, thus preventing any internal risk of misuse of data. Therefore the only risk is that the data carried within the communication layer is **not itself encrypted**. If someone were to be able to break the GSM encryption, they would have access to the data.

In IVR, USSD2, and SMS banking channels, the consumer's sensitive data is typically kept on a server and **not on the handset**. This data is **encrypted**. The data entered into the handset is limited to **authentication** of the consumer (the PIN) and the banking instruction from the consumer, without having to enter account or personal details. The threat remains that if the **handset and the SIM card and the authentication data is stolen**, and used on the mobile banking channel to transact, then the consumer is at risk. The data is useless without these four elements. This is similar to the ATM Card and Pin environment.

²⁵ GSM Security Standards

²⁶ GSM Security Standards

J2ME, WAP and S@T Banking Data Security



WAP allows for a GPRS session to be opened between the handset web browser and the web application at the bank. This session is protected once again by the *encrypted GSM communication layer* and then can be further protected by *encryption of the actual banking website* that is being accessed. This makes WAP banking open to *similar threats as internet banking*, yet further secured in that the *bank can establish* that the session has been initiated by the consumer's SIM.

J2ME uses the same bearer channel as WAP. However J2ME applications can have *additional security* around the application that is resident on the handset. Thus the data entered into the J2ME application can be *encrypted at that point* and sent across the GPRS channel as described above. It would only be decrypted at the bank or processor. J2ME is however open to certain attacks in that the consumer needs to establish that the application is being *downloaded from the correct source* and that the source is not that of a malicious attempt to copy the banks application in order to obtain sensitive data from the consumer.²⁷

S@T is the *most secure* method of mobile banking. It allows the bank to *load its own encryption keys onto the SIM card* with the bank's own developed application. Thus the *consumer's data can be stored* on the SIM Card and the consumer *can be authenticated on the handset* prior to having to carry any data across the mobile network. The data is also *encrypted prior to leaving* the handset and *only decrypted using the banks encryption keys* within the bank.

²⁷ Known as Spoofing

Additional Authentication and risk mitigation in mobile banking:

The following additional steps should be used to mitigate the gaps in the mobile banking security environment:

- **MSISDN²⁸ and PIN authentication** is used in almost every implementation, creating a form of digital signature that says that the consumer is initiating the transaction from their SIM card and that they are entering their secret PIN to prove that they are the owner of that SIM card. This is a powerful tool that the mobile operator provides for consumer authentication. Work does need to be done in controlling access to the linking and de-linking of MSISDN²⁹ from the SIM card as in some markets this is left to the control of the MNO's distribution channel.
- Where using 'server-side' bearer channels, data, sufficient to perform a transaction, should not be sent from the handset but rather **stored in a central location** and secured using standards similar or the same as PCI³⁰ data security and compliance.
- The PIN should be **customer selected PIN**, and never stored on the mobile banking platform or application as a PIN but rather as a **PIN Offset³¹**. As an additional measure it is recommended that the customer be asked for certain elements of their PIN for validation (**challenge response**) as apposed to the full PIN.
- **Dual bearer channel** in a single transaction is advised to prevent any possible spoofing or public internet gateway³² initiated transactions. This would mean that the consumer initiated transaction is on one bearer and the banks response on another. E.g. SMS initiated banking with USSD2 response. This would mean that the response would go back to the registered mobile phone as apposed to the phone/gateway that initiated the transaction.
- Fraud, behaviour, and spend pattern monitoring of all transactions, ideally real time, as well as **spend and velocity limits** should be in place to cap the bank's exposure.
- Adequate identification of the consumer at **registration**.

²⁸ Mobile number sent from your SIM card through the network.

²⁹ Consumer changes their SIM due to it being lost or stolen or changes their mobile number or network

³⁰ Payment Card Industry

³¹ Pin Offset is an encrypted format of the PIN that is compared each time the consumer enters their PIN.

³² Web sites that allow you to send SMSs

7. Regulatory Impact on the Mobile Banking Technology Chosen

There do not seem to be any regulatory restrictions on the mobile banking technology selection.

There are, however, Association (Visa and MasterCard) and International Payment Card Industry guidelines, governing the levels of security required for the transportation and storage of financial data.

The regulatory impact results from the actual application of the technology. When a bank decides to add the mobile option, it will need to consider the necessary KYC, AML, branchless banking (agency), emoney, and data privacy regulations that are relevant to the implementation. There may also be a need to assess the potential risk of fraud and to make provision for it, especially in the light of the Basle II implementation.

Some regulators appear to be pro-active in supporting mobile banking, as well as open to discussion on how relevant regulations can be implemented or existing regulation can be changed to support implementations, yet still protect the consumers.

8. Conclusions

Mobile banking is moving up on the adoption curve, which is evident in the number of implementations known in the world and the level of interest and discussion around the technology and its implementation. It is also evident in the number of technology providers emerging in the mobile banking space.

There are several choices when considering how to implement mobile banking. These choices include whether or not to develop the technology within the bank, use a shared infrastructure, or purchase the enabling technology from one of many vendors.

The choices also include various mobile bearer channels, suited to differing market segments and differing capabilities of consumers handsets. Each of the bearer channels has unique requirements in provisioning and securing applications, transactions and consumer data.

The selected implementation option including bearer channel, vendor and value proposition, should be driven by consumer adoption of the technology, technical capability of the handsets in the target market, affordability of the bearer channel, and the consumers ease of accessing the service.

9. Addendum: Extract of the GSMA Mobile Banking Vendor Analysis



GSMA MOBILE BANKING VENDOR ANALYSIS OVERVIEW DOCUMENT

This document provides an introduction and overview of the leading Mobile Banking/Commerce vendor solutions available to MNOs and Banks. *The document is intended for MNOs in the GSM Association ("Association") as an overview of the Mobile Banking solution and Vendor Environment. The vendors chosen in the analysis were selected through sourcing information from implementations around the world, as well as web, and conference materials.*

The data used was supplied through the vendor's websites, vendor data submissions, face-to-face meetings, and telephonic discussions.

The document is not an accreditation of the vendor or its solution and is to be used for informational purposes only.

Access to and distribution of this document is restricted to the persons listed under the heading Security Classification Category. This document is strictly confidential to the Association and is subject to intellectual property protection, including copyright. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available by the recipient, in whole or in part, to persons other than those listed under Security Classification Category without the prior written approval of the Association. The information contained in this document is provided "as is" and the Association makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or currency of the information contained in this document. Recipients who use this document and rely on any information herein do so at their own risk. Recipients should therefore verify information obtained from this document before they take any action upon it. The information contained in this document may be subject to change without prior notice.

Copyright Notice

Copyright © 2007 GSM Association

GSM and the GSM logo are registered and owned by the GSM Association.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

THE ROLE OF THE MOBILE BANKING VENDOR

The Mobile Banking environment requires both a bank and a MNO to deliver a transactional or informational banking service to a consumer through the mobile phone.

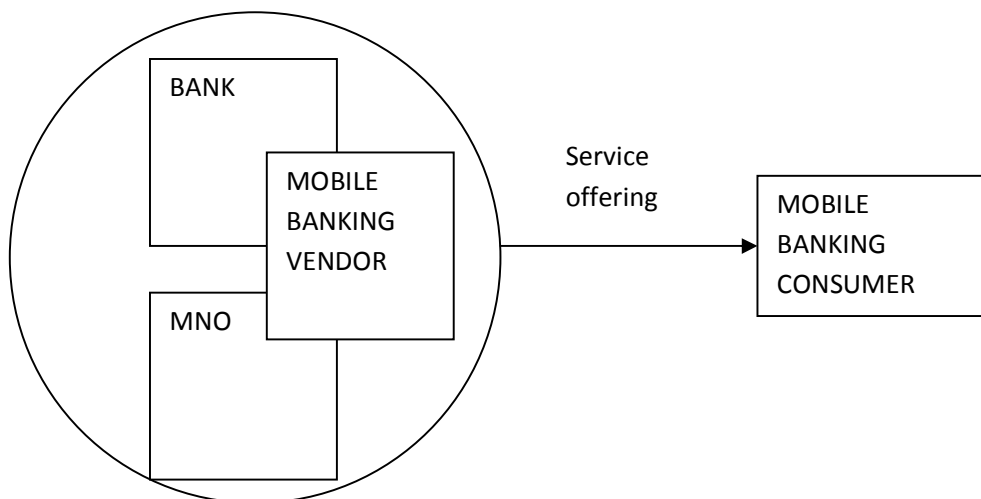
In this description, neither the bank, nor the MNO, can deliver the solution to the consumer in isolation.

In some examples, the MNO has delivered a MNO branded bank/banking application to the consumer, however the MNO has had to still partner with a bank for their financial license or processing capability or acquire a banking license and source bank processing capability.

In some cases, the bank has delivered a bank branded mobile banking application to the consumer. However the bank has had to make use of, or partner with the MNO for its infrastructure to provision the application and for ongoing financial transactions.


Often times, the debate as to who owns the customer for a mobile financial service is the deal breaker between the two parties.

The Mobile Banking Vendor plays the pivotal role of integrating the bank and the MNO and technically delivering the application to the consumer.



THE ROLE OF THE MOBILE NETWORK OPERATOR

The MNO's role in the delivery of Mobile Banking Applications varies from that of bearer channel provisioning where the MNO's role is marginal to that of full platform provisioning where the MNO is central to the delivery of the banking application.



	MNO as Bearer	MNO as Application	MNO/Bank Joint venture	MNO as Bank
Churn Reduction	No reduction in Churn as any MNO can offer the service	Reduction in Churn	Definite reduction in Churn	Definite reduction in churn
Regulatory and License Constraints	No impact	Low impact. PCI compliance.	Banks typically facilitate regulatory compliance	High regulatory and license requirements
Brand	Not used	Not used	MNO Brand	MNO Brand
Banking Systems	None required	Financial Switching only	Some required	High infrastructure requirement.
Distribution Chain for cash handling etc.	Not used	Not Used	MNO and Bank	MNO only
Transactional Risk	None	Some	Half of the risk	All of the risk
Cost Revenue	Marginal Low	Some cost Good	High cost High	Very High Costs High

Bearer Channel Only

Low MNO impact/involvement where a MNO only supports the bearer channel or normal consumer voice/data usage and the mobile banking application is built away from the MNO and does not require the MNO for provisioning or support. An example of this would be a JAVA application built by a vendor, where the download of the application is dependent on the network supporting GPRS but not necessarily facilitated by the MNO.

This environment fosters an easy consumer churn as there is no lock-in to the MNO and no benefit to the MNO over any other network in the market. It is a fairly network agnostic environment.

Bearer Channel and Application Development

An example of fairly low network involvement is where the MNO is required to complete some of the application development due to the bearer channel supported. An example of this would be where the vendor/bank makes use of the MNO's hosted USSD2 gateway or IVR platform in the provisioning of the service. There is a dependency on the network to develop the USSD2 menus or the IVR voice flows. This environment assists

in creating value for the MNO in the service offering, but is not much of a competitive differentiator as most MNOs would be able to offer similar solutions.

Bank Integration and MNO with a Mobile Banking Hub

An example of fairly high levels of integration and network involvement is where the network operator would facilitate the implementation of a Mobile Banking platform or Hub and offer the solution in a hosted environment to the banks in the market.

This would require integration into the banks, customer data repositories, financial switches, etc. The solution would also require auditing and certification.

This requires a high level of MNO involvement and also control over the application.

This option gives value to the banks and to the MNO consumers, and thus preventing churn and generating new revenue streams.

SIM Application Provisioning

This requires a large amount of MNO involvement, but results in ownership of the application which resides on the SIM which is MNO real estate.

This adds value to the consumer's SIM and assists in prevention of churn and perceived value from the MNO to the consumer.

The MNO would need the application to be embedded in the SIM prior to shipping and/or have OTA technology in place to get the application onto the SIM. The MNO would also need data encryption on the SIM and integration into a financial institution for the processing of transactions.

MNO as a Bank

This is the highest level of MNO involvement in Mobile Banking or commerce. Where the MNO enters into a joint venture with a bank or obtains a license to be a bank.

The MNO would own the entire value chain. This would be resource and technology heavy and will take time to implement. This level of involvement would require: banking hosts; switches; customer management systems; bearer channel development; audit trails; reporting; etc.

It would add value to the consumer but may not be a core function in the networks business.

VENDOR ANALYSIS

The vendor analysis has been completed for the purpose of providing MNOs with adequate information about what the vendor landscape looks like and what considerations should be taken into account when selecting a vendor. This document supports, and should be used in conjunction with, the *GSMA Mobile Banking Vendor Analysis Spread Sheet* and the *GSMA Mobile Banking Vendor Contact Sheet*.

The analysis evaluates the following components:

Geographic Fit

Functionality

Service Offering (Financial Transaction Type)

Bank Product Support

Bearer Channel/Consumer Application

Vendor Business Model

ASP

Licensing

Engineering

Ability to Implement

Implementation Status

MNO Integration

Bank Integration

Complexity of Implementation

Technical Architecture Options

Wireless Application Service Providers

Application Development

Bank System Support

Additional Components

Audits/Certifications/Endorsements

Note that all elements of the analysis were done on a 'have completed and launched' basis as opposed to 'possible or in development or trial'.

GEOGRAPHIC FIT

Assessing the vendor's location, implementation, and representative footprint assists in establishing the likelihood of the vendor being able to deliver the solution in your market.

Geographic fit is defined as:

Actual geographic presence (where the office is);

Where the vendor has implemented their solution.

It is advisable to also establish where the vendor has representation in the form of actual staff/partnerships that can adequately foster implementation as opposed to just representation in the form of sales offices.

	MULTIPLE MARKETS	AFRICA	AMERICAS	MIDDLE EAST	EUROPE INC.UK	SOUTH ASIA	ASIA PACIFIC
Bharti TeleSoft						<input type="checkbox"/>	
C-SAM	<input type="checkbox"/>		<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
Fundamo	<input type="checkbox"/>	<input type="checkbox"/>					
G-Cash							<input type="checkbox"/>
GFG							<input type="checkbox"/>
Jigrahak						<input type="checkbox"/>	
mCheck						<input type="checkbox"/>	
MiPay	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>		
MobiComp					<input type="checkbox"/>		
Monitise	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		
Movensis					<input type="checkbox"/>		
mPay							
Mpesa	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>	
mTranZact		<input type="checkbox"/>					
OBOPay			<input type="checkbox"/>				
PayBox	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
PayM8	<input type="checkbox"/>	<input type="checkbox"/>					
S1(Postilion)	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>		
Simplus	<input type="checkbox"/>	<input type="checkbox"/>					
SMART							<input type="checkbox"/>
Utiba	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>
Valista			<input type="checkbox"/>		<input type="checkbox"/>		

FUNCTIONALITY

The core functionality offered is the extension of a bank's payment franchise to the mobile phone.

This involves both the bank, in the transaction offered, and the MNO, in the mobile channel used to perform the transaction.

Transactions:

While vendors support some transactions and not others, it is noted that if a vendor has implemented *transactional banking* services, they would typically be able to implement any financial transaction.

The supported transactions are categorized as:

Domestic Money Transfer	Ability to transfer money within a market
International Money Transfer	Ability to transfer money to other markets
Transactional Banking	Transactions that debit/credit an account
Informational Banking	Balance enquiries; mini statements
Top Up	Electronic reload of airtime
Bill Payments	Utility or telco bill payments
Card Acquiring	Mobile phone as a card accepting device

Key differences in supported transactions would relate to the *banking product* implemented.

Support of card based banking products would mean that the vendor could typically process MasterCard or Visa Card type transactions. If the vendor has only implemented card-based banking products they may have difficulty in implementing transactional banking services directly to a bank account. The same applies for vendors that have not implemented card-based services. If the vendor has implemented for card type payments they would probably also only be connected to a payment gateway or acquiring bank institution and thus be limited to process transactions resulting from purchases.

It is also noted that some vendors offer a proprietary purse or stored value system where there is no requirement for a bank account or bank integration. These solutions are subject to regulatory approval in each market and are not interoperable with the global payment systems.

Channels:

The mobile channel that the consumer will adopt is a key deciding factor on which vendor and which technology to support. The vendor analysis outlines what the vendor has implemented as opposed to what they can implement.

The channels identified are:

Client Side	-	SIM based/dependant applications
		JAVA/J2ME
Server Side	-	USSD2
		IVR
		SMS
		WAP

Each channel presents differing benefits and concerns and can have an affect on market adoption and the security of the application.

Ironically, the best technical and most secure solution (SIM) also has the highest barriers to implementation.

MNOs should adopt a multi-channel approach to allow consumer choice and manage the risks around application adoption, with a view to migrate the consumer as/when the market is saturated with the preferred technology.

This should ensure speed of uptake and optimise user experience.

VENDOR BUSINESS MODELS

Two principle models emerged from the vendors:

Application Service Provider, ASP, or hosted model, where the vendor owns and manages the infrastructure and banks or MNOs integrate into the infrastructure and share the services. This model has worked well in markets where the banks and MNOs do not want to invest too heavily into their own infrastructure. Examples of successful

models ASP models would be Monitise in the UK, Simplus in South Africa and mTranZact in Kenya. In these cases, multiple banks and multiple MNOs use the same infrastructure. The services are typically billed on a per transaction, per consumer, or monthly management fee basis.

Licensing model, Most of the vendors prefer an outright licensing model that allows the MNO or bank or in-market consortium to own the technology for a licensing fee. The vendor typically becomes the development and maintenance house for the application. Examples would be Fundamo with MTN Banking, and Utiba in multiple market implementations.

Some vendors offer both models where technically feasible. Some vendors insist on using single market hosting services which may pose communication and integration dependencies.

Some vendors also offer the option of having a customised and once-off application engineered for the MNO or bank.

ABILITY TO IMPLEMENT

The actual implementation of a vendor should be cross referenced and is a major factor in evaluating some of the vendors in the list. Implementation status proves that the vendor has actually implemented and has proof of such implementations.

It is especially beneficial if a vendor has a commercially viable implementation to show, or is cash flow positive as Mobile Banking is relatively new technology.

Vendors without live implementations were excluded from the analysis.

It is also worth noting that if a vendor has done both a MNO and bank level integration as these are the two major components of an end-to-end system.

MNO Integration	-	Into the bearer channels (USSD2 Gateways, SMSC)
	-	For service provisioning (OTA Downloads, etc.)
	-	In platform for direct load of purchased airtime
Bank Integration	-	Into bank switching or processing environments

Bank integrations are highly complex and time consuming considering the levels of security and standardisation that needs to be complied with.

TECHNICAL ARCHITECTURE OPTIONS

Mobile Banking Vendors play one or more of the following four roles:

Wireless Application Service Providers (WASPS)

This is where vendors facilitate the communication or transport layer of the banking service. I.e. carry the instruction to/from the consumer and no levels of integration into the actual bank. These vendors are referred to as Wireless Application Service Providers.

Application Developers

The vendor would provide the skills to develop the actual application that resides on the consumer's phone or interfaces with the consumer. This would be the WAP Site, JAVA Application, USSD2 Gateway and Menu flow, SMS Gateway, or SIM Application.

Bank System Support

The vendor would house a financial switch with the intelligence to integrate or support the bank system. The vendor would thus be able to translate the instruction from the consumer and submit it in a transaction format that the bank would accept. The vendor would thus have complied with several security requirements, audits, or certifications.

Additional Components

The vendor would be able to offer additional components such as customer management systems; card management systems; reconciliation or settlement systems; reporting functions; etc.

AUDITS/CERTIFICATIONS/ENDORSEMENTS

The banking environment is filled with audits and certifications and it is suggested that the vendor chosen also undergoes some form of third-party audit.

Examples of these audits/assessments can be found through MasterCard or Visa Vendor Programs and through Global PCI compliance.

SUMMARY

The *ideal vendor* would be able to deliver an adequate transaction set, on a broad number of bearer channels/applications that the consumer could adopt within the market.

This vendor would have shown proof of a successful implementation, and if not in your market, would show proof of ability to implement in another market.

This vendor would have completed a bank and MNO integration and complied with industry standards for security and financial transaction processing.

The vendor would preferably be supportive of the banking environment and have shown integration and development or partnership with banks or bank associations.