A STUDY ON MOBILE BANKING OF SOUTHEAST BANK LIMITED

BY

TANZIN FARHANA
ID: 093-19-1185

This Report Presented in Partial Fulfillment of the requirements for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering.

Supervised By

Taslim Arefin
Assistant Professor
Department of ETE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH
AUGUST 2012

APPROVAL

This project titled "**A STUDY OF MOBILE BANKING FOR SOUTHEAST BANK LIMITED**" submitted by Tanzin Farhana to the Department of Electronics and Telecommunication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation has been held on 30th August, 2012.

BOARD OF EXAMINERS

_____

Dr. Md. Fayzur Rahman **Chairman**
Professor and Head
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. A.K.M. Fazlul Haque **Internal Examiner**
Associate Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

_____

Mr. Mirza Golam Rashed **Internal Examiner**
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

_____

Dr. Subrata Kumar Aditya **External Examiner**
Professor and chairman
Department of Applied Physics, Electronics and Communication Engineering
University of Dhaka

ACKNOWLEDGEMENT

First I express my heartiest thanks and gratefulness to almighty Allah for His divine blessing makes me possible to complete this project successfully.

I feel grateful to and wish I profound my indebtedness to **Taslim Arefin, Assistant Professor,** Department of ETE Daffodil International University, Dhaka. Deep Knowledge & keen interest of my supervisor in the field of wireless network influenced us to carry out this project .His endless patience , scholarly guidance , continual encouragement , constant and energetic supervision, constructive criticism , valuable advice , reading many inferior drafts and correcting them at all stage have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Md. Fayzur Rahman**, Professor and Head, and Department of ETE, for his kind help to finish my project and also to another faculty member and the staff of the ETE department of Daffodil International University.

I would like to thank my entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

DECLARATION

I hereby declare that, this project has been done by me under the supervision of **Taslim Arefin, Assistant Professor, Department of ETE**, Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

_____

Taslim Arefin
Assistant Professor
Department of ETE
Daffodil International University

Submitted by:

_____

Tanzin Farhana
ID: 093-19-1185
Department of ETE
Daffodil International University

ABSTRACT

This project is on "**A study on Mobile Banking of Southeast Bank Limited**"**.** The focus of this project is on the future of Mobile Banking, based on IT department. This project is about the security of mobile banking platforms. Researching and observing the mobile banking procedure, software, database and security system where the main task in this project. Also assuring the security system of mobile banking software, assembling the progresses and research the flaws were the major part of this project. The experience of implementation of mobile banking sectors got covered in this internship period.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER-1

Introduction

1.1 Introduction

Across the developing countries, millions of people rely on formal and informal economic activity and local level networks to earn their living. Most of these populations are from BOP **(**according to World Bank people who earns less than $2 a day: annual income less than PPP US$ 3000) and they don't have access to basic financial service e.g. banks as access to those is costly, not inconvenient and very limited. Accesses to financial services or banks are vital for those people as- "This lack of access to finance in some parts of the developing world stifles entrepreneurship, stunts development and leaves people trapped in a poor, cash-only society". Developing countries are still struggling to ensure access of most of its unbanked BOP citizens and the informal sector to the formal financial services.

Mobile banking can be seen as one solution to these problems. Advancements in mobile technology have changed our lives over the past ten years. It has the potential to even more powerfully transform the lives of the world's poorest people. The technology is no doubt the cheapest and most convenient way to connect people and provide an array of innovative services. At the start of this century, just 12% of the world's population had a mobile phone. Now that figure is well over 61% percent (ITU, 2008).

1.2 Objective

- Online banking has given more freedom to customers to deal with their accounts without requiring them to actually step into a branch
- The goal of mobile banking is to expand that freedom to users even more, by making it so the user is not even required to be near a computer

- One of the newest pieces of mobile technology that is becoming widely popular is the iPhone
- Currently, mobile banking applications for the iPhone allow the user to view account balances, make transfers, and pay bills.

1.3 Formation

- Chapter one is about introduction, objective and formation of this report.
- Chapter two is what is mobile banking, its conceptual model, business model, service, Future functionalities in mobile banking, Challenges for a mobile banking solution and Mobile banking in the world.
- Chapter three is the main topics of mobile banking that is security of mobile banking. And mobile banking channel platform.
- Chapter four is demonstrative structure and key features of the software.
- Chapter five is why we need this security for banking.
- Chapter six is the conclusion of this report.

CHAPTER-2

Mobile Banking

2.1 What is Mobile Banking

Mobile banking (also known as M-Banking, mobile banking) is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device such as a mobile phone or Personal Digital Assistant (PDA). The earliest mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of the first primitive smart phones with WAP support enabling the use of the mobile web in 1999, the first European banks started to offer mobile banking on this platform to their customers.
Mobile banking has until recently (2010) most often been performed via SMS or the Mobile Web. Apple's initial success with iPhones and the rapid growth of phones based on Google's Android (operating system) have led to increasing use of special client programs, called apps, downloaded to the mobile device.

2.2 A mobile banking conceptual model

In one academic model, mobile banking is defined as:

Mobile Banking refers to the provision and availment of banking- and financial services with the help of mobile telecommunication devices. The scope of offered services may include facilities to conduct banking and stock market transactions, to administer accounts and to access customized information."
According to this model Mobile Banking can be said to consist of three interrelated concepts:

- Mobile Accounting
- Mobile Brokerage
- Mobile Financial Information Services

Most services in the categories designated Accounting and Brokerage are transaction based. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage

services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

Mobile phone banking may also be used to help in business situations as well as financially.

2.3 Mobile banking business models

A wide spectrum of Mobile/branchless banking models is evolving. However, no matter what business model, if mobile banking is being used to attract low-income populations in often rural locations, the business model will depend on banking agents, i.e., retail or postal outlets that process financial transactions on behalf telcos or banks. The banking agent is an important part of the mobile banking business model for customer care, service quality, and cash management will depend on them. Many Telco's will work through their local airtime resellers. However, banks in Colombia, Brazil, Peru, and other markets use pharmacies, bakeries, etc.

These models differ primarily on the question that who will establish the relationship (account opening, deposit taking, lending etc.) to the end customer, the Bank or the Non-Bank/Telecommunication Company (Telco). Another difference lies in the nature of the agency agreement between the bank and the Non-Bank. Models of branchless banking can be classified into three broad categories - Bank Focused, Bank-Led and Nonbank-Led.

Bank-focused model

The bank-focused model emerges when a traditional bank uses non-traditional low-cost delivery channels to provide banking services to its existing customers. Examples range from the use of automatic teller machines (ATMs) to internet banking or mobile phone banking to provide certain limited banking services to banks' customers. This model is additive in nature and may be seen as a modest extension of conventional branch-based banking.

Bank-led model

The bank-led model offers a distinct alternative to conventional branch-based banking in that customer conducts financial transactions at a whole range of retail agents (or through a mobile phone) instead of at bank branches or through bank employees. This model promises the potential to substantially increase the financial services outreach by using a different delivery channel (retailers/ mobile phones), a different trade partner (Telco / chain store) having experience and target market distinct from traditional banks, and may be significantly cheaper than the bank-based alternatives. The bank-led model may be implemented by either using correspondent arrangements or by creating a JV between Bank and Telco/non-bank. In this model customer account relationship rests with the bank

Non-bank-led model

The non-bank-led model is where a bank has a limited role in the day-to-day account management. Typically its role in this model is limited to the safekeeping of funds. Account management functions are conducted by a non-bank (e.g. Telco) who has direct contact with individual customers.

2.4 Mobile banking services

Mobile banking can offer services such as the following:
Account information

1. Mini-statements and checking of account history
2. Alerts on account activity or passing of set thresholds
3. Monitoring of term deposits
4. Access to loan statements
5. Access to card statements
6. Mutual funds / equity statements
7. Insurance policy management
8. Pension plan management
9. Status on check, stop payment on the check
10. Ordering checks books
11. Balance checking on the account
12. Recent transactions
13. Due date of payment (functionality for stop, change and deleting of payments)
14. PIN provision, Change of PIN and reminder over the Internet
15. Blocking of (lost, stolen) cards

Payments, deposits, withdrawals, and transfers

1. Cash-in, cash-out transactions at an ATM
2. Domestic and international fund transfers
3. Micro-payment handling
4. Mobile recharges
5. Commerce payment processing
6. Bill payment processing
7. Peer to Peer payments
8. Withdrawal at banking agent
9. Deposit at banking agent

A specific sequence of SMS messages will enable the system to verify if the client has sufficient funds in his or her wallet and authorize a deposit or withdrawal transaction at the agent. When depositing money, the merchant receives cash and the system credits the client's bank account or mobile wallet. In the same way the client

can also withdraw money at the merchant: through exchanging sms to provide authorization, the merchant hands the client cash and debits the merchant account.

Kenya's M-PESA mobile banking service, for example, allows customers of the mobile phone operator Safaricom to hold cash balances which are recorded on their SIM cards. Cash may be deposited or withdrawn from M-PESA accounts at Safaricom retail outlets located throughout the country, and may be transferred electronically from person to person as well as used to pay bills to companies. One of the most innovative applications of mobile banking technology is Zidisha, a US-based nonprofit micro lending platform that allows residents of developing countries to raise small business loans from web users worldwide. Zidisha uses mobile banking for loan disbursements and repayments, transferring funds from lenders in the United States to the borrowers in rural Africa using nothing but the internet and mobile phones.

In Cote d'Ivoire, Orange has a commercial offer which allows subscribers to use ATMs to top up their mobile wallet account. Due to very flexible and modular scope software, it is easy to add further options such as the payment of utility bills or insurance premium.

Investments

1. Portfolio management services
2. Real-time stock quotes
3. Personalized alerts and notifications on security prices

Support

1. Status of requests for credit, including mortgage approval, and insurance coverage
2. Check (check) book and card requests
3. Exchange of data messages and email, including complaint submission and tracking
4. ATM Location

Content services

1. General information such as weather updates, news
2. Loyalty-related offers
3. Location-based services

Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more "tech-savvy" customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment.

2.5 Future functionalities in mobile banking

Based on the 'International Review of Business Research Papers' from World business Institute, Australia, following are the key functional trends possible in the world of Mobile Banking.
With the advent of technology and increasing use of Smartphone and tablet based devices, the use of Mobile Banking functionality would enable customers to connect across the entire customer life cycle much comprehensively than before. With this scenario, current mobile banking objectives of say building relationships, reducing cost, achieving new revenue stream will transform to enable new objectives targeting higher level goals such as building brand of the banking organization. Emerging technology and functionalities would enable to create new ways of lead generation, prospecting as well as developing deep customer relationship and mobile banking world would achieve superior customer experience with bi-directional communications.

Illustration of objective based functionality enrichment In Mobile Banking

- Communication enrichment: - Video Interaction with agents, advisors.
- Pervasive Transaction capabilities: - Comprehensive “Mobile wallet”
- Customer Education: - “Test drive” for demos of banking services
- Connect with new customer segment: - Connect with Gen Y – Gen Z uses games and social network ambushed to surrogate bank’s offerings
- Content monetization: - Micro level revenue themes such as music, e-book download
- Vertical positioning: - Positioning offerings over mobile banking specific industries
- Horizontal positioning: - Positioning offerings over mobile banking across all the industries
- Personalization of corporate banking services: - Personalization experience for multiple roles and hierarchies in corporate banking as against the vanilla based segment based enhancements in the current context.
- Build Brand: - Built the bank’s brand while enhancing the “Mobile real estate”.

2.6 Challenges for a mobile banking solution

Key challenges in developing a sophisticated mobile banking application are:
Handset operability

There are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on any type of device. Some of these devices support Java ME and others support SIM Application Toolkit, a WAP browser, or only SMS.

Initial interoperability issues however have been localized, with countries like India using portals like R-World to enable the limitations of low end Java based phones, while focus on areas such as South Africa have defaulted to the USSD as a basis of communication achievable with any phone.

The desire for interoperability is largely dependent on the banks themselves, where installed applications (Java based or native) provides better security, are easier to use and allow development of more complex capabilities similar to those of internet banking while SMS can provide the basics but becomes difficult to operate with more complex transactions.

There is a myth that there is a challenge of interoperability between mobile banking applications due to perceived lack of common technology standards for mobile banking. In practice it is too early in the service Lifecycle for interoperability to be addressed within an individual country, as very few countries have more than one mobile banking service provider. In practice, banking interfaces are well defined and money movements between banks follow the IS0-8583 standard. As mobile banking matures, money movements between service providers will naturally adopt the same standards as in the banking world.

On January 2009, Mobile Marketing Association (MMA) Banking Sub-Committee, chaired by Cell Trust and VeriSign Inc., published the Mobile Banking Overview for financial institutions in which it discussed the advantages and disadvantages of Mobile Channel Platforms such as Short Message Services (SMS), Mobile Web, Mobile Client Applications, SMS with Mobile Web and Secure SMS.

Security

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.
The following aspects need to be addressed to offer a secure infrastructure for financial transaction over a wireless network:

1. Physical part of the handheld device. If the bank is offering smart-card based security, the physical security of the device is more important.
2. The security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.
3. Authentication of the device with the service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.
4. User ID / Password authentication of a bank’s customer.
5. Encryption of the data being transmitted over the air.

6. Encryption of the data that will be stored in device for later / off-line analysis of the customer.

One-time password (OTPs) is the latest tool used by financial and banking service providers in the fight against cyber fraud. Instead of relying on traditional memorized passwords, OTPs are requested by consumers each time they want to perform transactions using the online or mobile banking interface. When the request is received the password is sent to the consumer's phone via SMS. The password has expired once it has been used or once its scheduled life-cycle has expired.

Because of the concerns made explicit above, it is extremely important that SMS gateway providers can provide a decent quality of service for banks and financial institutions in regards to SMS services. Therefore, the provision of service level agreements (SLAs) is a requirement for this industry; it is necessary to give the bank customer delivery guarantees of all messages, as well as measurements of the speed of delivery, throughput, etc. SLAs give the service parameters in which a messaging solution is guaranteed to perform.

Scalability and reliability

Another challenge for the CIOs and CTOs of the banks is to scale-up the mobile banking infrastructure to handle the exponential growth of the customer base. With mobile banking, the customer may be sitting in any part of the world (true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7 fashion. As customers will find mobile banking more and more useful, their expectations of the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence. There are systems such as Mobile Transaction Platform which allow quick and secure mobile enabling of various banking services. Recently in India there has been a phenomenal growth in the use of Mobile Banking applications, with leading banks adopting Mobile Transaction Platform and the Central Bank publishing guidelines for mobile banking operations.

Application distribution

Due to the nature of the connectivity between the bank and its customers, it would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their mobile banking application. It will be expected that the mobile application itself check the upgrades and updates and download necessary patches (so called "Over The Air" updates). However, there could be many issues to implement this approach such as upgrade / synchronization of other dependent components.

Personalization

It would be expected from the mobile application to support personalization such as:

1. Preferred Language
2. Date / Time format
3. Amount format
4. Default transactions
5. Standard Beneficiary list
6. Alerts

2.7 Mobile banking in the world

Mobile banking is used in many parts of the world with little or no infrastructure, especially remote and rural areas. This aspect of mobile commerce is also popular in countries where most of their population is unbanked. In most of these places, banks can only be found in big cities, and customers have to travel hundreds of miles to the nearest bank.

In Iran, banks such as Persian, Tejarat, Mellat, Saderat, Sepah, Edbi, and Bankmelli offer the service. Banco Industrial provides the service in Guatemala. Citizens of Mexico can access mobile banking with Omnilife, Bancomer and MPower Venture. Kenya's Safaricom (part of the Vodafone Group) has the M-Pesa Service, which is mainly used to transfer limited amounts of money, but increasingly used to pay utility bills as well. In 2009, Zain launched their own mobile money transfer business, known as ZAP, in Kenya and other African countries. In Somalia, the many telecom companies provide mobile banking, the most prominent being Hormuud Telecom and its ZAAD service.

Telenor Pakistan has also launched a mobile banking solution, in coordination with Taameer Bank, under the label Easy Paisa, which was begun in Q4 2009. Eko India Financial Services, the business correspondent of the State Bank of India (SBI) and ICICI Bank, provides bank accounts, deposit, withdrawal and remittance services, micro-insurance, and micro-finance facilities to its customers (nearly 80% of whom are migrants or the unbanked section of the population) through mobile banking.

In a year of 2010, mobile banking users soared over 100 percent in Kenya, China, Brazil and USA with 200 percent, 150 percent, 110 percent and 100 percent respectively.

The Dutch Bangla Bank launched the very first mobile banking service in Bangladesh on 31 March 2011. This service is launched with ‘Agent’ and ‘Network’ support from mobile operators, Banglalink and Citycell. Sybase 365, a subsidiary of Sybase, Inc. has provided software solutions with their local partner Neurosoft Technologies Ltd. There are around 160 million people in Bangladesh, of which, only 13 per cent have bank accounts. With this solution, Dutch-Bangla Bank can now reach out to the rural and unbanked population, of which, 45 per cent is mobile phone users. Under the service, any mobile handset with a subscription to any of the six existing mobile operators of Bangladesh would be able to utilize the service. Under the mobile banking services, bank-nominated ‘Agents’ perform banking

activities on behalf of the banks, like opening a mobile banking account, providing cash services and dealing with small credits. Cash withdrawal from a mobile account can also be made from an ATM validating each transaction by 'mobile phone & PIN' instead of 'card & PIN'. Other services that are being delivered through a mobile banking system are person to-person (e.g. fund transfer), person-to-business (e.g. merchant payment, utility bill payment), business-to-person (e.g. salary/commission disbursement), and government-to person (disbursement of government allowance) transactions. [1]

CHAPTER-3

Security for Mobile Banking System

3.1 Mobile Banking channel platforms:

There are six mobile banking channel platforms. They are:

1. STK Menu
2. USSD Menu
3. Java Menu
4. Text sms
5. IVR
6. WAP

Mobile Banking Security Options

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

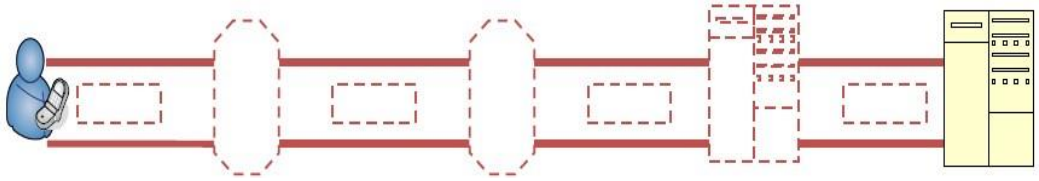


Fig 3.1: Data across the GSM Channel

The 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 of transporting data across the GSM channel may be found in the number of stops the data make 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 are also unencrypted when it hits the network operator. Thus, there is a broken encryption between the consumer and the bank. [9]

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

3.1.1 STK / SAT (SIM Application Toolkit) Menu

The SIM Application Toolkit allows for the service provider or bank to house the consumer's mobile banking menu within the SIM card. STK 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. [10]

Overview of STK

- The SIM Application Toolkit is a set of commands which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset.
- With SIM Application Toolkit, the card has a proactive role in the handset (this means that the SIM initiates commands independently of the handset and the network).
- SAT (SIM Application Toolkit) is designed as a client server application.
- The applications are stored in the SIM card, and not on the handset.
- Applications are downloaded over the air and stored in SIM card and the process is controlled by the service provider.
- Service provider keeps total control of the applications, when they are to be downloaded and when they should be removed.
- It uses the SMS for the bearer medium to transfer the information between the handset and the service provider.

STK Banking Data Security

Fig 3.2: Data across STK channel

The SAT 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 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. [9]

Features on STK Menu:

- Supported by the 100% hand set,
- SIM based menu
- Dynamic menu to choose from.
- Easy to use

Advantages

- Some manufacturers claim that STK enables higher levels of security through identity verification and encryption, which are necessary for secure electronic commerce.
- STK has been deployed on the largest number of mobile devices.

Limitations

- Updating STK applications and menus stored on the SIM can be difficult after the customer takes delivery of the SIM. To deliver updates, either the SIM must be returned and exchanged for a new one (which can be costly and inconvenient) or the application updates must delivered over-the-air (OTA) using specialized, optional SIM features. Mobile Network Operators can now (as of October 2010), for example, deliver updated STK application menus by sending a secure SMS to handsets that include a SIM alliance Toolbox (S@T) compliant wireless internet browser (WIB). When using a Bearer Independent Protocol-compliant (BIP) SIM card in a BIP-compliant handset, the updates can be delivered very quickly as well (depending upon the network connectivity available to and supported by the handset, i.e. GPRS/3G speed). It might also be possible to change the menu of wireless internet gateway (WIG) -based STK applications. The update limitations hinder the number and frequency of STK application deployments.
- STK has essentially no support for multimedia, only basic pictures.
- The STK technology has limited independent development support available. [2]

Example of STK Menu

Deliver updated STK application menus by sending a secure SMS to handsets that include a SIM alliance Toolbox (S@T) compliant wireless internet browser (WIB). When using a Bearer Independent Protocol-compliant (BIP) SIM card in a BIPcompliant handset, the updates can be delivered very quickly as well (depending upon the network connectivity available to and supported by the handset, i.e. GPRS/3G speed). It might also be possible to change the menu of wireless internet

gateway (WIG) -based STK applications. The update limitations hinder the number and frequency of STK application deployments.

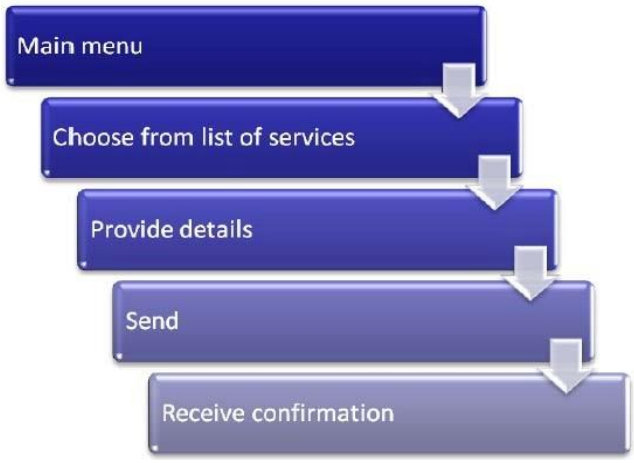


Fig 3.3: Choosing menu of SIM application

3.1.2 USSD (Unstructured Supplementary Service Data)

USSD is a unique service for mobile networks comprised of two-directional sessionbased exchange of unstructured data in GSM mobile networks. The USSD service supports high-speed real-time information exchange between subscriber and service application. [10]

USSD Banking Data Security

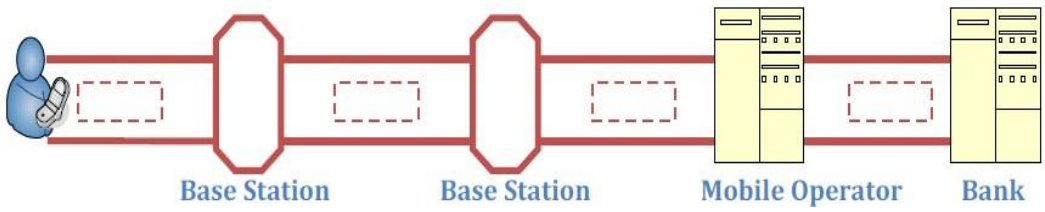


Fig 3.4: Data across USSD channel

USSD opens a single session between the device and the USSD application at the network operator, processor, or a 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 USSD 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 USSD channel the consumer's sensitive data are 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 an 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. [9]

Security threats and mitigating security risks of USSD

Mitigating Security Risks in USSD-based Mobile Payment Applications

Mobile payment applications use various communications channels which are not secure, including USSD and IP-based communications. As usage of these communications channels by payment applications increases, security flaws are becoming prime concerns for service providers.

Critical threats such as fraudulent transactions, request/response manipulations, weak encryption, and insecure message communications have directly triggered revenue loss for mobile payment service providers. Fraudulent transactions, mobile application request/response tampering/dropping, sensitive information disclosure due to weak cryptographic implementation, improper account management, and modification of sensitive information can also cause security breaches and loss of sensitive data in USSD-based mobile payment applications.

In light of these threats, application development and integration companies, telecoms, and banks providing payment services need to assess USSD-based apps

and ensure that secure coding practices have been followed during USSD-based application software development.

- USSD Commands Request/Response Tampering

A malicious user can tamper with USSD command requests and responses. This may cause confusion for the legitimate user and can also lead to fraudulent transactions. This request and response tampering is possible through hardware and software interceptors. Weak encrypted request and response messages are prime concerns in such threat vectors.

- USSD Request/Response Message Replay Attacks

When a phone is lost, an adversary may perform fraudulent transactions through an installed USSD application. An application must authenticate USSD request originator (authentication through a combination of MSISDN (Mobile Station International Subscriber Directory Number), IMEI (International Mobile Equipment Identity), PIN and unique Message Tracking ID). If this USSD application server or application is unable to authenticate the USSD request originator, then it can perform fraudulent transactions.

- Improper Data Validation (USSD IP Mode Applications)

Improper data validation in the USSD IP mode application can lead to SQL injection, cross site scripting attacks. An adversary may purposely insert specifically crafted scripts in user input. Once successfully inserted in the database, the attacker may try to use the same to perform malicious actions on the database or at another user's active session. [8]

Features on USSD Menu:

- Supported by the 100% hand set,
- Dynamic,

- Easy to use, all users can access,
- No need to write SMS,
- Operator base dependency,
- No store and forwarding option.

Advantages of USSD Services

- Extremely low cost
- Real-time
- Fast and responsive
- Interactive navigation
- Consumer driven
- Can be used as payment method
- Automated response
- Allows for mass-usage
- Location-based, SIM and PUK-based and user selected customization and segmentation

Disadvantages of USSD Services

- Little in the way of aesthetics
- Messages cannot be saved or forwarded
- USSD codes aren't as memorable as other Common Short Codes (CSC)
- Not always reliable due to session-based timeouts. [3]

USSD Used Applications

Services ideal with USSD as the bearer include mobile chat, m-commerce, prepaid balance inquiry, mobile banking, call-related services and any other service that requires interaction between the user and the application.

- Menu Browsing.
- Alternative to IVR
- Balance Enquiry
- Card Validity
- Prepaid Recharge (from any visiting network also)
- "Pull" based Services like informational services.
- News – Weather
- Movies – Sports Update
- Currency Update – Stock Market • Telephone Directory – Yellow Pages
- Push Services.

- Voting / Polling
- Flash Emergency Information
- Customer care /service management.
- – Service Activation / Deactivation
- – Voice Mail
- – MMS
- – Roaming
- Information query: News, Weather, Sports, Finance, Train schedules, real time Currency Converter.
- Reservations (Train / Movie).
- Sponsored Menu Item / Advertisement.
- Companies / Shops / Theaters can get listed
- On the Menu and promote their services
- Contests.
- Tele-voting.
- Virtual Money Transaction.
- Debit Card.
- Interactive Interface to Corporate ERP.
- Voice Chat.

Roaming: This has huge advantages while roaming. This is because USSD services are well available in roaming networks and all the USSD messages are directed towards the subscriber's Home Network itself, thus, same set of services that are available in home network can be given in a visited network too, giving subscribers a Virtual Home Environment (VHE). Information query: News, Weather, Sports, Finance, Train.

Example of USSD Menu:

A typical USSD message starts with an asterisk (*) followed by digits that comprise commands or data. Groups of digits may be separated by additional asterisks. The message is terminated by a number sign (#).
Example USSD codes:

- *101#

- *109*72348937857623#

After entering a USSD code on a GSM handset, the reply from the GSM operator is displayed within a few second. [12]

3.1.3 Wireless Application Protocol (WAP)

WAP is wireless application protocol used over GPRS. It is similar to Internet banking. The consumer's handset needs to be WAP enabled. WAP banking is open to similar threats as Internet banking. [10]

WAP Banking data Security

Fig 3.5: Data across WAP channel

WAP allows for a GPRS session to be opened between the handset's 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. [9]

Features:

- GPRS supported handset,
- Need active WAP connection
- Internet using knowledge

How to get: An IP address will direct users to the WAP site of Mobile Banking

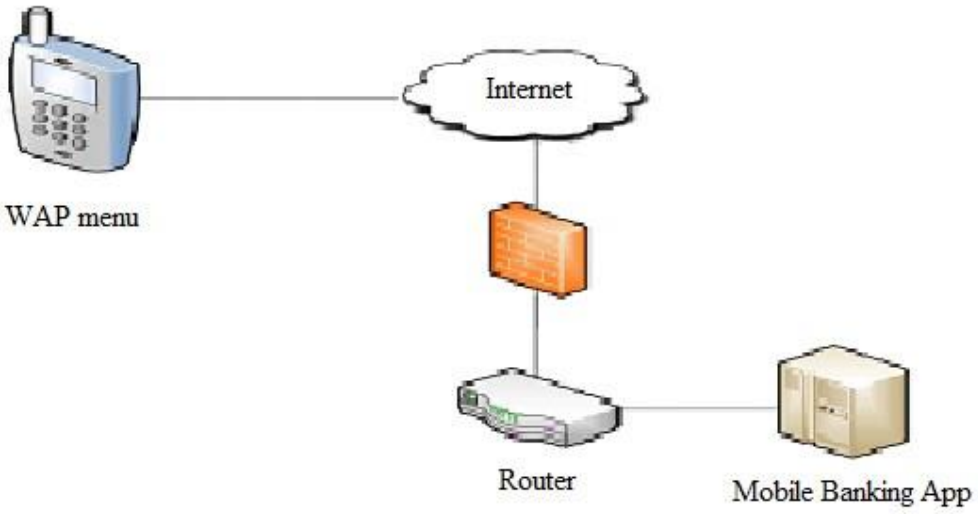


Fig 3.6: Network diagram for WAP

3.1.4 Java menu (J2ME)

Java Platform, Micro Edition, or Java ME, is a Java platform designed for embedded systems (mobile devices are one kind of such systems). Target devices range from industrial controls to mobile phones (especially feature phones) and set-top boxes. Java ME was formerly known as Java 2 Platform, Micro Edition (J2ME).

J2ME Banking data Security:

Fig 3.7 Data across J2ME channel

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 bank's application in order to obtain sensitive data from the consumer. [9]

Features:

- Only Java supported handset, • Need internet connection, Easy to use,
- Internet using knowledge.
- More than 80% JAVA Support phone set on the market

How to Get: By sending a simple SMS we can get a link to download the JAVA menu.

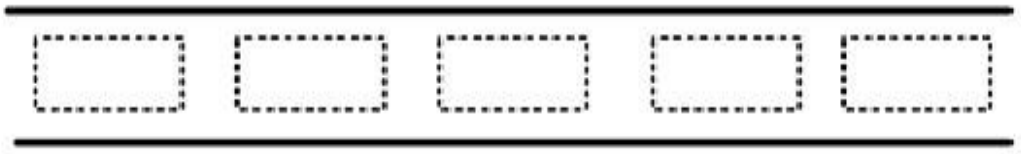


Fig 3.8: Unencrypted data through an encrypted channel

3.1.5 IVR (Interactive Voice Response)

IVR Banking data Security: Highly secured as inserted PIN (**by pressing buttons**) cannot be traced by the Telco.

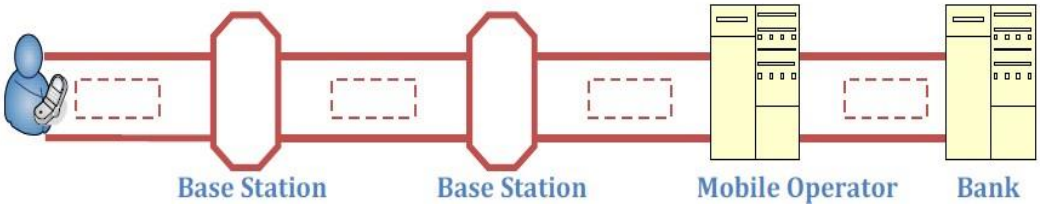


Fig 3.9: Data across IVR channel

IVR, being a voice call, is protected by both the encrypted GSM communication layer25 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.

In the IVR banking channel, 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 an 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. [9]

Features:

- 100% handset support
- Easy to use
- Keyword typing hassle free.

How to Get:

Dialing to a Short Code user will hear a pre-recorded voice which will direct and give answers to queries.

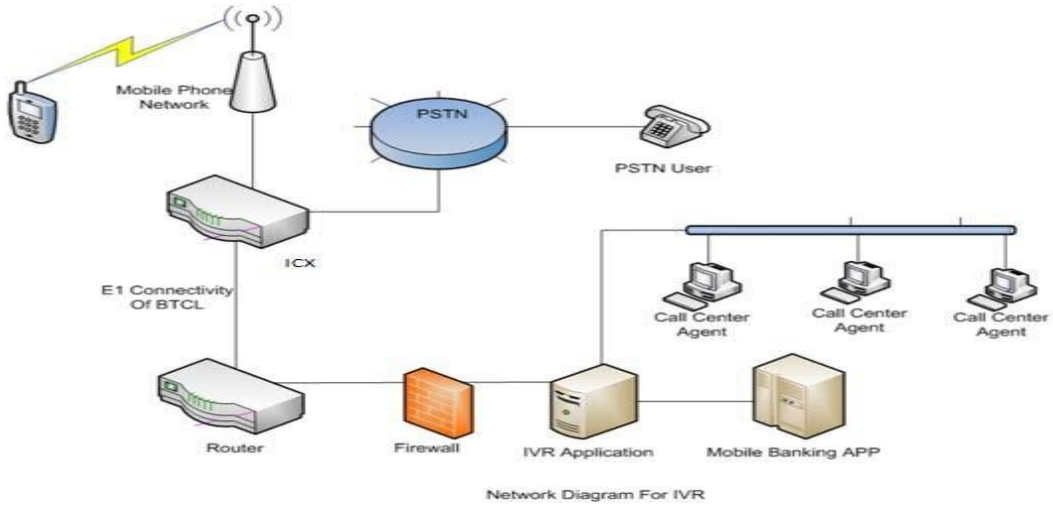


Fig 3.10: Network diagram for IVR

3.1.6 Short Message Service (SMS)

SMS is the simplest form of mobile banking. It is largely used for information-based services. SMS has the maximum reach amongst consumers since all the mobile phones support SMS. Short messages are stored and forwarded by SMS centers. These messages have some security issues. [7][10]

SMS Banking Data Security:

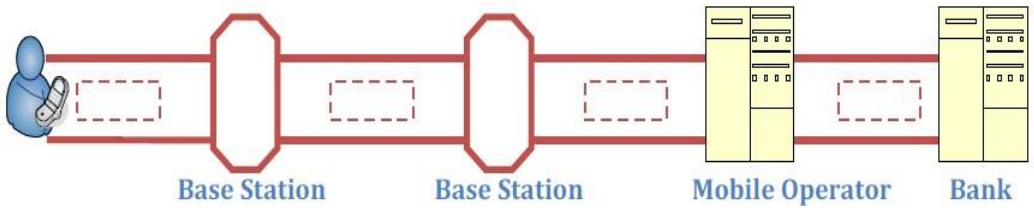


Fig 3.11: Data across SMS channel

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.

In SMS banking channel, 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 an 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. [9]

Message Structure

The secured SMS message is divided into multiple fields to accommodate for the various security checks required for the protocol. To ease the understanding of the message structure, Figure 4 shows the structure overview for a secure SMS message. The numbers above the fields are the minimum number of bytes required for each field in the message. The number of bytes for each field can be increased depending on the implementation requirements.

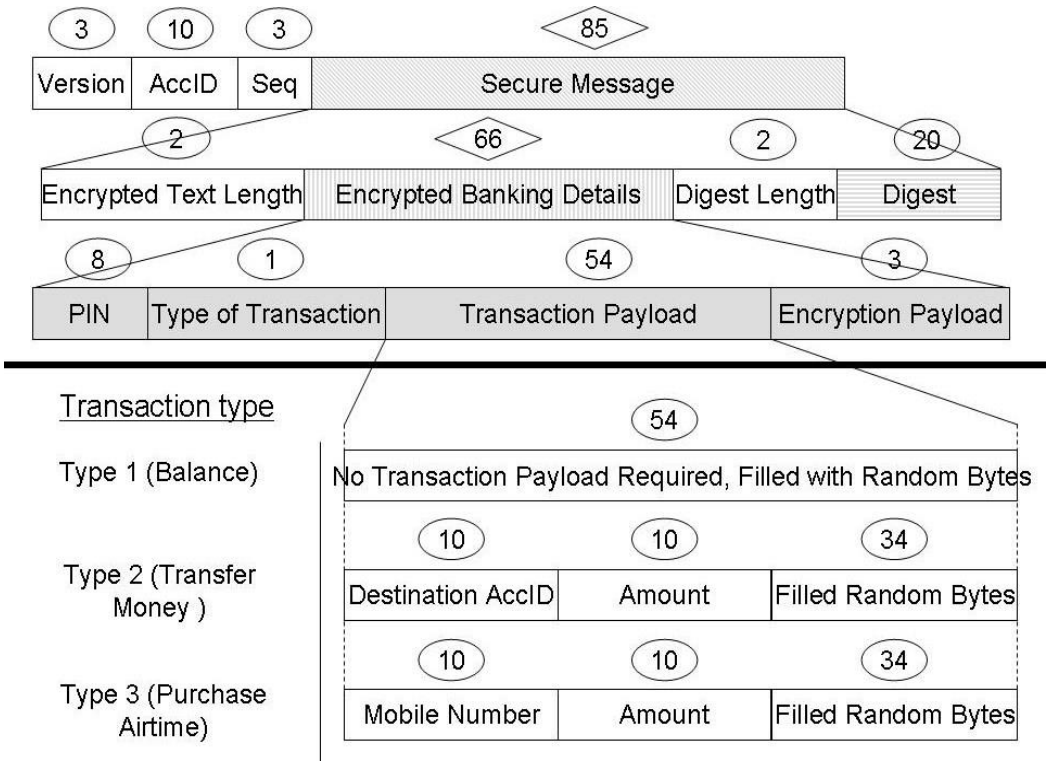


Fig 3.12: The Structure of a Secure SMS Message

The use of each labeled structure is explained below:
The *Version* is the mobile application version number. It contains a specified byte pattern. The receiver checks if the first three bytes of the received SMS message are valid for the bank application. If the message version number does not match the application version, then the message is discarded. As there are possibilities that the server can receive accidental SMS messages that are not intended for the bank server. The usage of the version bytes is to help to eliminate these erroneous messages.

- The *AccID* contains the bank account identifier of the user.
- The *Seq* is the user's current sequence number of the one-time password.
- The *Encrypted Text Length* contains the number of next bytes that are the ciphered message.
- The *Digest Length* contains the number of next bytes that contains the message digest.

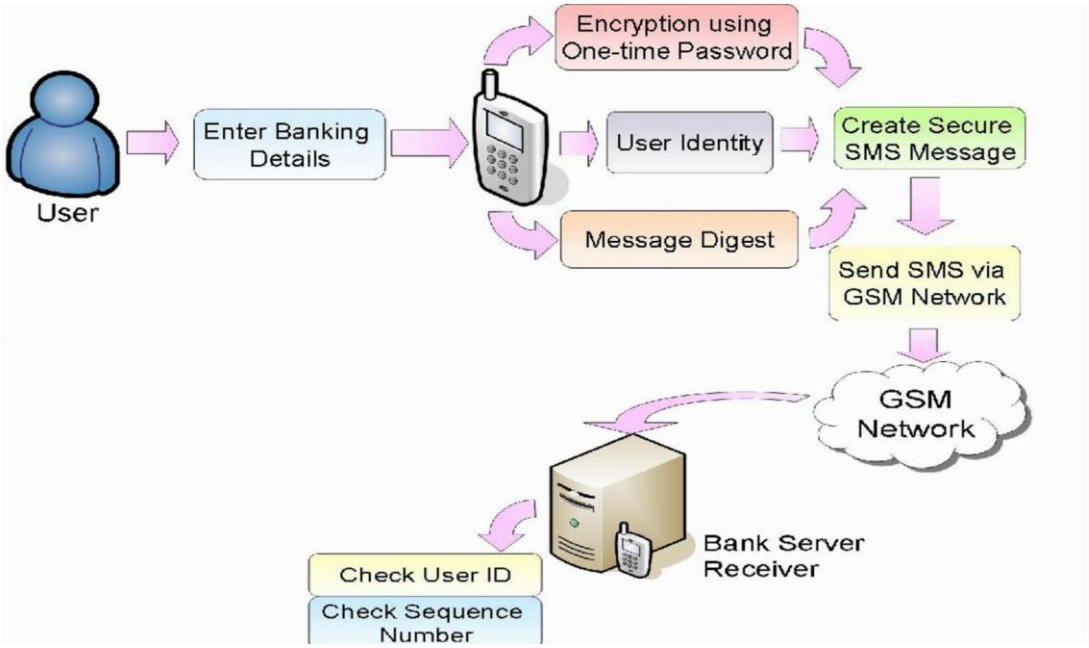
- The *Digest* contains the calculated digest value of the message. The use of the digest is for the server to check for message integrity. For the secure SMS banking protocol, a single digest of the following fields is calculated: *Version*, *AccID*, *Seq*, *PIN*, *Type of Transaction* and *Transaction Payload*.

The content of the following fields is encrypted using the generated session key.

- The *PIN* contains the user predefined password. This is used by the receiver application to authenticate the user.
- The secure SMS message can be used for different types of transactions. The *Type of Transaction* is used by the bank server application to identify the type of transaction it should perform.
- The *Transaction Payload* is the extra data that are used for a transaction, but it is not used for any security purpose. The content of the Transaction Payload depends on the type of transaction requested. The structure of the payload depends on the type of transaction offered by the bank.

Protocol Sequences

In the GSM network, SMS messages are sent asynchronously to the receiver, because of this the Secure SMS protocol is asynchronous. The figure below illustrates the overview of the secure SMS protocol.



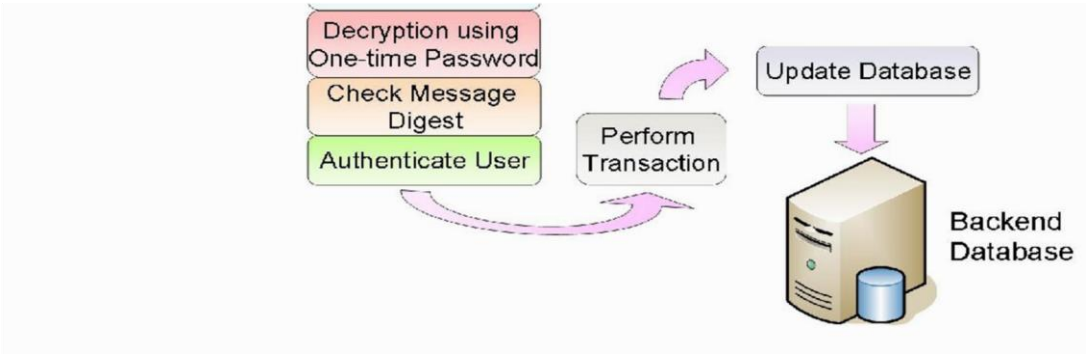


Fig 3.13: Protocol Sequence

We can consider the Secure SMS protocol to be divided into two parts. The first part is the message generation. The mobile phone generates the message and sends it to the server. The second part is the message security checks. The server reads the received message, decodes the contents and performs security checks. The following subsections describe each part of the protocol.

Generating and Sending Secure SMS Messages

The mobile phone captures all the required security information from the user. This information is used to generate the secure SMS message to be sent to the server. The mobile application has a preset version byte pattern, this pattern is inserted into the message.

The message hash value a number which can ensure message integrity for the receiver side. The requirement of maintaining the message integrity is that at least some of the contents that are used for calculating the message digest need to be encrypted. This can ensure message integrity because if the message is intercepted, the attacker cannot use the encrypted contents to generate another digest. The integrity validation will not pass if any part of the original message is altered.

The fields of content that need to be encrypted are dependent on the needs of the developer. The protocol requires that the message to have some identification details not to be encrypted. This is for the receiver to identify the account holder's identity.

The algorithm used for encryption must be a symmetric encryption algorithm. The key used for encryption is generated from the one-time password entered by the user. The one-time passwords are only known by the server and the user.

After the application completes processing the security contents, the contents are placed in the SMS message according to the message structure described in the Message Structure section. The SMS message is sent to the server via the GSM network.

Receiving and Decoding Secure SMS Message

When the server receives the message from the cellular network, it breaks the message down according to the structure described in the Message Structure section.
The server first checks for the version bytes pattern. If the version is correct, it is assumed that the message is suitable for the secure SMS protocol. Next, the server reads the account identifier from the message and checks if the account identifier exists in the server database. After this, the server retrieves the current sequence number for the given account identifier. The server checks if the sequence number read from the message matches the sequence number read from the server database.

If the above security checks all passed, the server proceeds to retrieve the one-time password from the database. The password is indexed by the account identifier and the sequence number. Thereafter the server uses the retrieved password as the decryption key to decode the encrypted contents. If the decryption is successful, then the used one-time password is discarded and the server is a sequence counter for that account gets incremented by the value of 1.
After the decryption, the server reads the secure contents that are required for the calculation of the message digest. The message digest is calculated using the same algorithm as the algorithm used by the mobile application. The server compares the two digests for message integrity. If the message is proven not to have been altered, then the server retrieves the PIN (the account holder's personal password) from the message and compares it against the account holders PIN from the server database. If all of the above security checks pass, the server performs the requested transaction.

Secure SMS Message Structure

The secured SMS message is divided into multiple fields to accommodate for the various security checks required for the protocol. Following figure shows the structure overview for a secure SMS message. The use of each labeled structure is explained below.

Account No.	Session Key	Cipher Text	Message Digest
(6 digit)	(Generated From MPIN)	(Plain Text + MPIN)	

Fig 3.14: Secure SMS message structure

Secure SMS message structure proposed by us consists of 4 fields as shown in above figure.

Account Number: - It is a customer account number in a bank which is first field used for authentication purpose. This information is stored in a plain test format

so that at the server end, information can be retrieved to get required keys from the database.

Session key: - It is onetime key randomly generated from customer MPIN inputted into the bank server database during M-Banking registration process. This key is stored in 2nd field of the message. The customer makes a request to get the session key from his handset to bank server. Bank server will reply this with encrypted session keys stored in file, which will be stored on customer handset.

Cipher Text: - This text is created from a combination of plain text and MPIN and stored in 3rd field of the message structure. The main idea behind this is to protect data from malicious attacks. As MPIN is the most important data and from which session keys are created to be used for encryption and decryption purpose, hence its send in encrypted manner.

Message Digest: - Message digests is used for checking integrity. A customer message digest is calculated from a combination of plain text and MPIN and stored in the 4th field of secure SMS. MD5 algorithm is used to calculate message digests on both ends. This received digest will be compared with calculated digest at the bank server end , if not fond of the same size then the message will be discarded as fake transaction and no message will be sent to a mobile handset from which request is sent.

Sending Secure SMS from Client Mobile

Whenever customer wish to make any transaction using M-banking, he will run applications installed on the handset and provide all necessary details. We have used 6 transactions for testing purpose and information collected from users on his handset is used to generate secure SMS. After registration customer will get mobile application installed once on his windows mobile. The customer will enter 4-digit MPIN which will be stored in the server database in encrypted format using his password. For nonrepudiation purpose we have added concept of one time session key. The server uses customer MPIN to generate session key randomly and again stored them in encrypted format.

The customer runs the banking application and feed details about 6-digit account number, 4-digit MPIN and 4-digit password and click button to get the session key. The server sends generated session key to customer handset which will be stored in encrypted format on his handset. The customer goes to the menu screen, chooses requires account type and the type of transaction he wishes to perform and goes to the next screen. The mobile client application shows 4 entries on next screen consisting of session key received, generated fixed plain text message depending upon transaction chosen, cipher text created from a combination of plain text and MPIN and 4-part secure message. Secure SMS contains the account number in plain text, session key in encrypted format, cipher text created from plain text and MPIN and message digest calculated from the message. The customer will send a message to server using as a normal message.

Receiving and Replying Secure SMS from Server Module

Proposed Server is running on the computer installed with required software like VB.NET, Windows mobile device center and SDK, .NET compact framework, MS access and Server side application. Server side application has four modules as SMS Service, Information Manage, Transaction Manage and User Requests. SMS service module retrieves SMS received on the Server side handset and decode it to get the original query send by the customer. Server application process query, get required data from bank database and then sends it in encrypted format to customer mobile through the bank side modem.

Whenever Customer sends any secure SMS containing his transaction query to server side GSM Modem, Server application automatically retrieves secure SMS and deletes it from server attached handset to avoid flooding of message Inbox. We have used an ActiveX control for this purpose. Bank Server application splits are received secure SMS in same 4-parts.

The server reads first part, a plain text 6-digit account number and compares it with database stored account numbers. If a match is not found, it will send message "Wrong Account Number" to customer handset. If account match is found then the server uses 2nd part of secure SMS, which is session key send by user to decrypt 3rd part of receiving secure SMS.

After decrypting 3rd part of SMS, server application gets a combination of plaintext as customer original transaction query followed by 4-digit MPIN. Server application compares received MPIN with stored MPIN from server table if a match is not found, will send message "Wrong Pin Number" to customer handset. The server calculates a message digest of 3rd part received using MD5 algorithm and compare it with received message digest, the 4th part of secure SMS to check for message integrity. If a match is not found, the server generates message on the server side "Fake Transaction" and sends nothing to customer side handset as it may be of any malicious use.

If all security checks are proper, Server application process query of customer and get required data from database encrypts data using the session key received from customers and sends automatically to customer handset. [10]

Advantages of Text SMS

- Allows you to request and receive banking information from your bank on your mobile phone
- You can manage bank accounts, check account balances, perform check requests and pay some bills.
- If you are in a business you can access your account whenever you need to
- It is more convenient because you don't have to go to a bank to complete a banking transaction.
- It's quite discrete, so you can view it when you are doing everyday jobs and you don't have to set aside time to go to the bank.

Disadvantages of Text SMS

- If you don't have the internet on your mobile you can't access what you need in your bank account.
- You could get your phone stolen and it will have all of your details on it, so people can gain access to your account as well as your phone.
- It causes more people to use their mobile phones and can cause radiation. [5]

Current SMS Banking Services in South Africa

Currently South African banks, such as Standard Bank and ABSA use the Wireless Internet Gateway (WIG) for mobile banking. First National Bank (FNB) uses the Unstructured Supplementary Services Data (USSD) with SMS approach. FNB requires the user to first send a USSD string with the users PIN to the banking server. Then the server returns a message to notify the user that the server is ready to accept a banking SMS message. This approach is not secure because every users detail is transmitted in plain text. The mobile network operator has full access into the banking details sent by the user.

Security Problems with SMS

The initial idea of SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, endto-end security, no repudiation was omitted during the design of GSM architecture. In this section we discuss some of the security problems of using SMS.

Forging Originators Address

SMS spoofing is an attack that involves a third party sending out SMS messages that appear to be from a legit sender. It is possible to alter the originator address field in the SMS header to another alphanumeric string. It hides the original sender's address and the sender can send out hoax messages and performs masquerading attacks.

SMS Encryption

The default data format for SMS messages is in plain text. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available. The encryption algorithm used is A5 which is proven to be vulnerable. Therefore a more secure algorithm is needed. [4]

3.2 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

Fig 3.15: 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

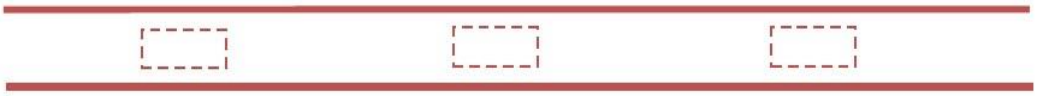


Fig 3.16: Unencrypted data over an encrypted fixed communication link

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 are at risk.

Encrypted data over an encrypted fixed link

Fig 3.17: 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.

3.3 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 behavior and geographic spend behavior.
- Velocities 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.

3.4 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:

- MSISDN 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 MSISDN 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 PCI 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 Offset. 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.
- A 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 to another. E.g. SMS initiated banking in 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, behavior, 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. [5]

3.5 Results

The following table shows a comparison of the present mobile banking implementations and our proposed solutions.

Table 3.1

Current Mobile Banking Solution

	Current Solutions		
	USSD + SMS	**WIG + SMS**	**WAP**
Security	USSD String sent in plain text. Authentication relies on IMEI.	USSD string and SMS message transmitted in plain text.	Standard WTLS protocol. No End to End encryption.
Cost for Customer	USSD is for free. One SMS message required.	Multiple SMS Messages required.	Depends on the amount of data required to be sent. GPRS is generally cheaper than SMS.
Cost for Bank Server	One SMS message in reply.	Multiple SMS reply messages required.	
Transmission Speed	The transmission sp eed of all the mobile banking solutions depends on numerous factors. It depends on the strength of the signal received by t he users mobile phone. Therefore it depends o n the location of the user, the traffic of the network, the number of base towers in th e area around the users mobile and etc. All these factors can influence the speed of transmission, thus no actual experiment can be conducted.		
Connection type	USSD is synchronous. The	Asynchronous. Each transaction waits for the server to reply. SMS	Synchronous. If the connection is lost
And Reliability	user gets an immediate response from the bank server.	messages are stored in the message buffer at the SMSC until it is delivered.	then it reconnects to the bank server.
Compatibility	Any mobile phone that can support USSD and SMS can use this service.	Requires mobile phone to be SIM Application Toolkit (SAT) Compatible. It is SIM card Dependent.	Requires mobile phone to be WAP capable and GPRS, EDGE or 3G Enabled.
Usability	Requires no menu. The user interface depends on how the users interact with their mobile phone to send SMS messages.	Menu based user interface.	Mobile phone WAP browser interface.

Table 3.2

Mobile Channel Features

Channel Technology	Description	Supported on Handsets	Security of transaction on handset	End-to-end Security	Supports Multiple MNOs
IVR	A call is made to (or from) an automatic system and the user receives pre-recorded prompts and responds by selecting keys	Standard Handset	None	No	Yes
Structured SMS	A SMS text message is sent to the mFSP. The message is interpreted and acted upon and a response SMS sent		None	No	Yes
USSD	A number is called from the handset and a menu then displayed on the handset that the user navigates through and selects options and enters data		None	No	Yes (1)
SIM toolkit (WIB / SAT / Java / custom)	Implemented within the SIM that is inserted in the handset. The functionality appears as a set of additional menu/s on the handset		Provided with SIM	Yes	Possible (2)
J2ME	Applications that can run on the handset	Advanced Handset	Provided within the application	Yes	Yes
WAP	Internet Browsing using a WAP protocol browser. Same as browsing off a PC. WAP provides optimized (data usage and size of screen presentation) interaction for the mobile.		As provided by the WAP Browser	Yes – SSL	Yes
HTTPS – Internet browser	Standard Internet browsing off the mobile to the bank‘s web site. Mobile performs the function of a PC		As provided by the Internet Browser	Yes - SSL	Yes

[11]

Table 3.3

Common Mitigation Strategies and Controls

Vulnerability	Procedural intervention	Result	Applicable
Fraudulent movement of funds away from their owner	Limit Value movements to pre-defined beneficiaries	Difficult to move value away from the owner	All
Users choose weak PINs	Educate users, prevent most vulnerable PINs being used (e.g. 12345)	PINs less likely to be guessed	All
PIN obtained through social engineering (e.g. phishing) and ID theft/imposter	Control PIN change processes	Ensure that account access is not fraudulently obtained	All
Single account vs. multiple account access - the issue is that if the customer's mobile channel is breached then access is gained to all accounts	Multiple accounts with only one account 'active' for mobile channel can be used as a process countermeasure. Movement of funds into the mobile account from other accounts not possible using the mobile channel	Only the funds available in the mobile account are at risk of mobile channel failure	All
Immediate value movements - as the transactions from the mobile to the handset are immediate the velocity of a fund's movements through the system is high making it difficult to stop suspect transactions.	Delaying value movements within the bank and to third parties outside the bank is a procedural risk control strategy i.e. a transaction is executed but value movement is delayed due to normal processes such as overnight clearing. This allows for back office checks, customer queries and status notifications happen and be reacted upon	Fraudulent transactions that are delayed provide the bank a chance to analyze the transactions and intervene on suspicion of being fraudulent	All
On-us transfers have a greater chance of being managed if used for fraud as the funds are still within the same institution	Less rigorous process controls can be used for on-us than not-on-us	Funds destinations managed	All
Movement of funds to outside the MFSP‘s direct control. Not-on-us Transfers and payments are assumed to be the same thing - namely a movement of value away from the account holder to another account outside the account holder's bank.	Countermeasures available include - limiting amount per payment, limiting amount per day/week/month, limiting number of transactions, filtering new destinations and independently verifying the payments, managing destination (beneficiary) registrations, monitoring velocity to certain accounts	Limited velocity and value of transfers away from mFSP and its user leading to less risk of funds not being recoverable	All
Replay of transactions	Teach users to enter a sequence number. Can be a randomized list on a card that the user ticks off	Transactions cannot be resent / replayed	All

[11]

CHAPTER-4

Demonstrative Structure and key features of software

The Key Features and Demonstration of the Functions of The

Mobile Banking Software

4.1 Main structure of mobile banking for SEBL

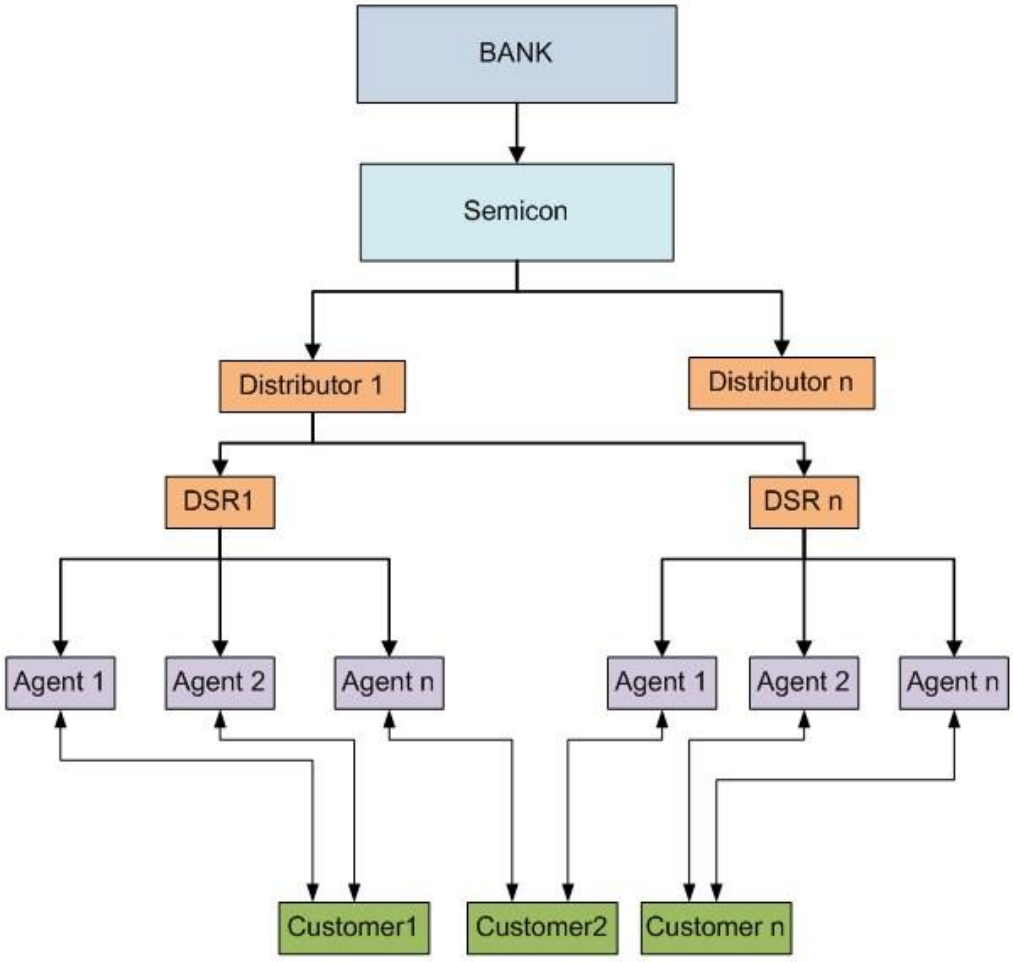


Fig 4.1: Distribution Channel of Semicon Private Limited

1st step: From the bank user information goes to the Semicon system, where they maintain the security.

2nd step: From Semicon the information goes to Distributor and DSR

3rd step: DSR sends the information to agents and via agents the customers get the required information and customers to also send the request by those agents to.

4.2 The security system and bridge through the three systems of mobile banking

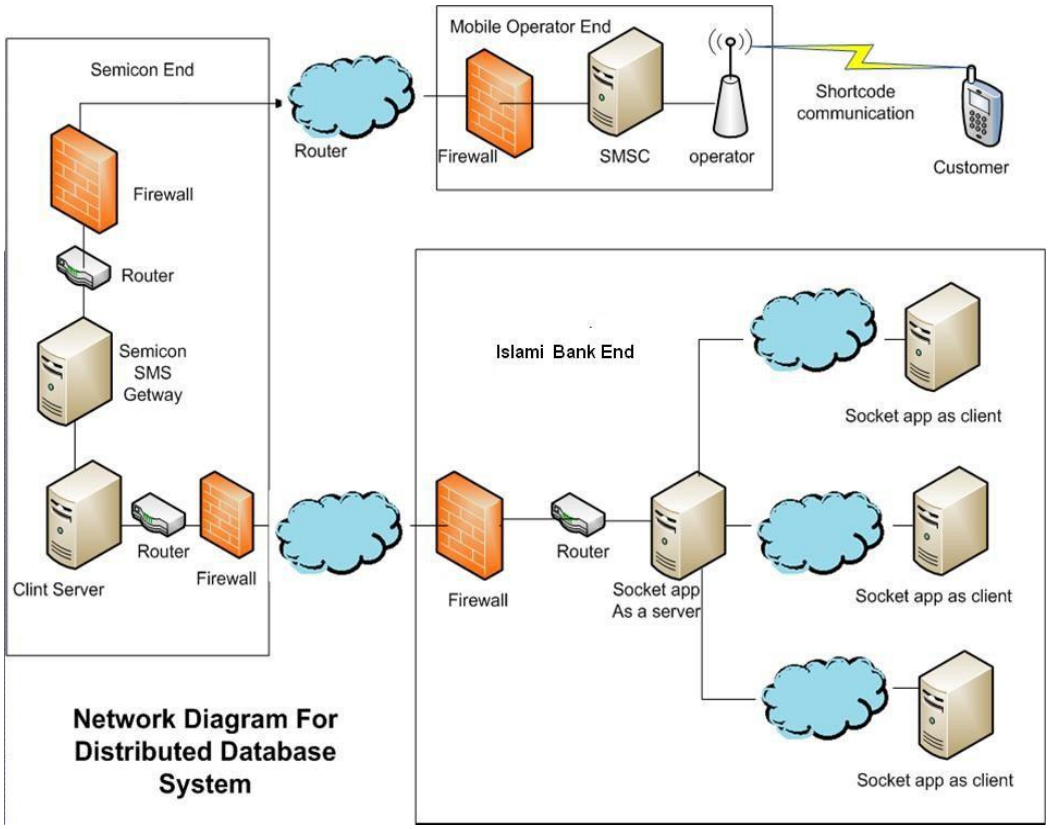


Fig 4.2: Network Diagram for Distributed Database System

1st step: Customers send the shortcut via his/her mobile phone and that code goes to operator like GP, ROBI etc. They pass the info thru SMSC and firewall for special security

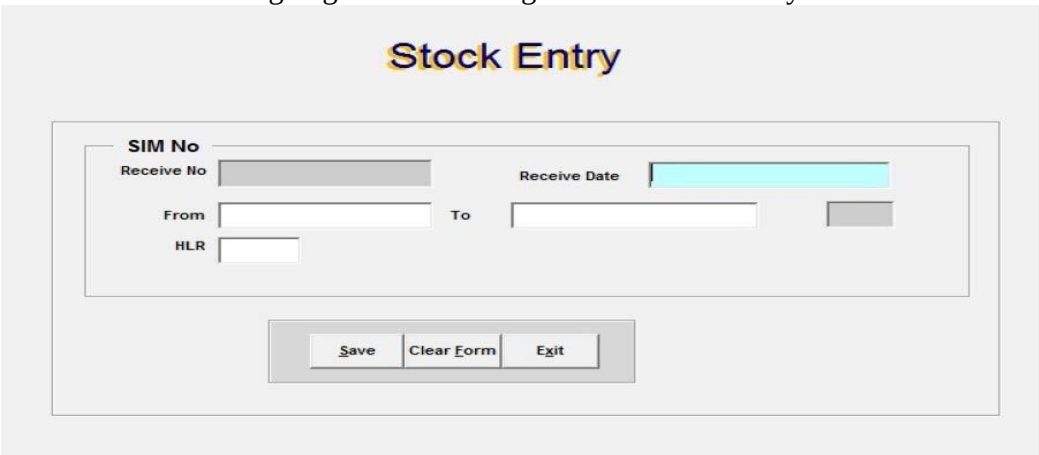
2nd step: Operators send the code to Semicon via router. After checking by firewalls the shortcut goes to Semicon SMS Gateway and assures the security of the sensitive information hidden in the code.

3rd step: Semicon sends the code to banks system via a router. The firewall and routers pass the code to the server then the socket app as a client.

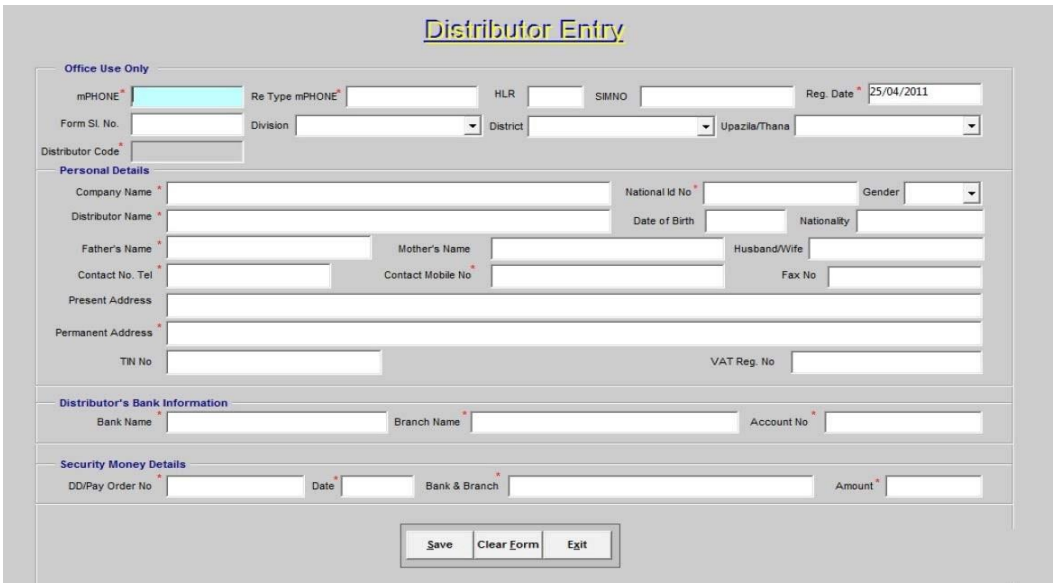
This is the way an SMS/short code goes to banks system where the funding is safe. The operator and Semicon system assures the security of the bridge between banks and customers here.

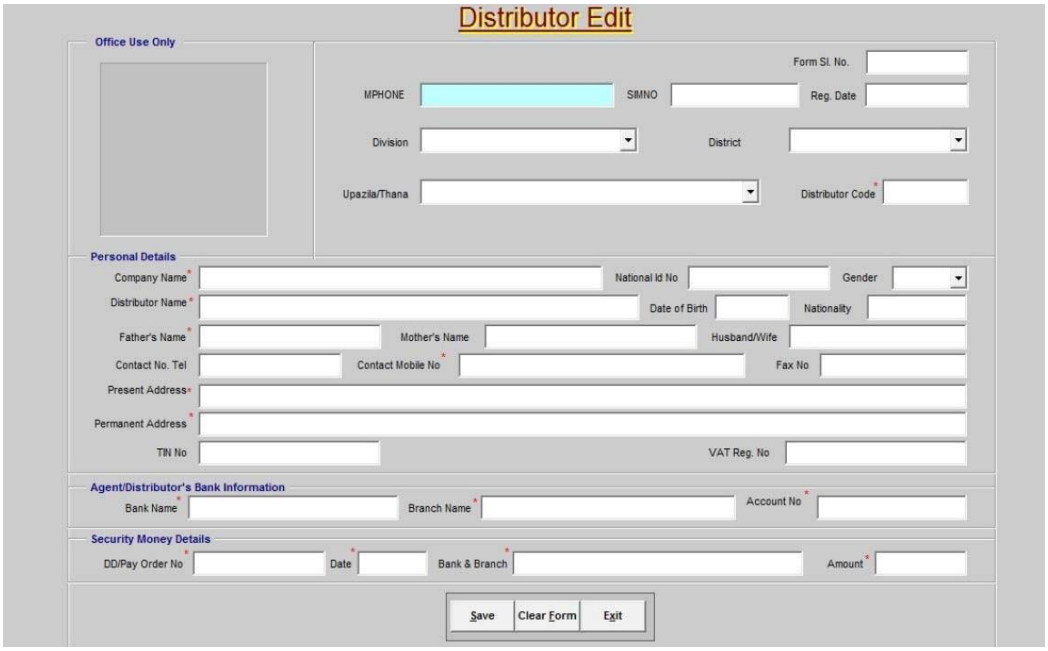
4.3 Software of Mobile Banking

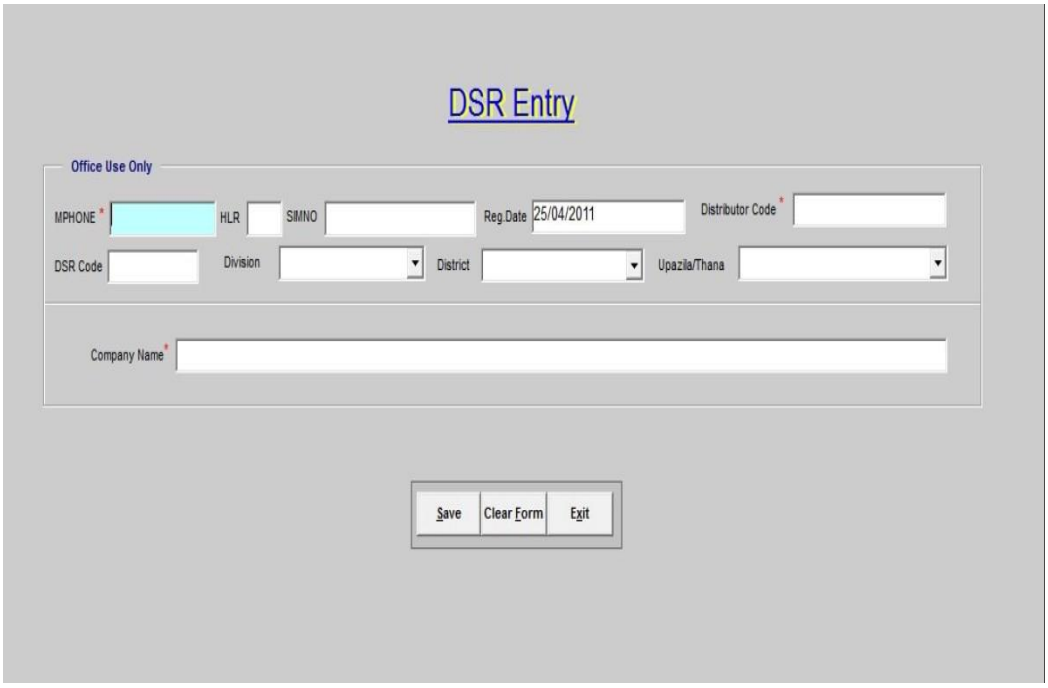
The name of software is m-pay. Here are some screen of m-pay software.
When the customer is going to start banking then this Stock Entry is stored to serve.

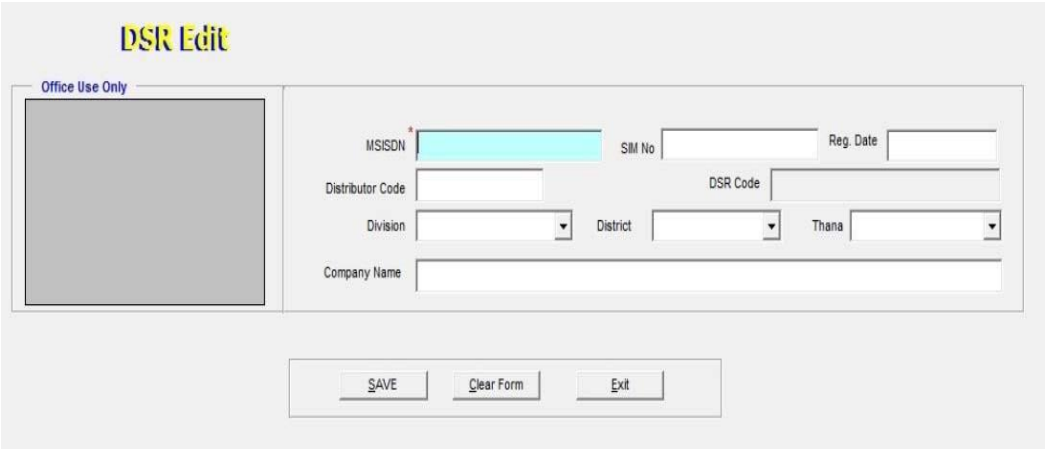


When a customer is starting to banking then distributor is filling this manually for mobile banking.

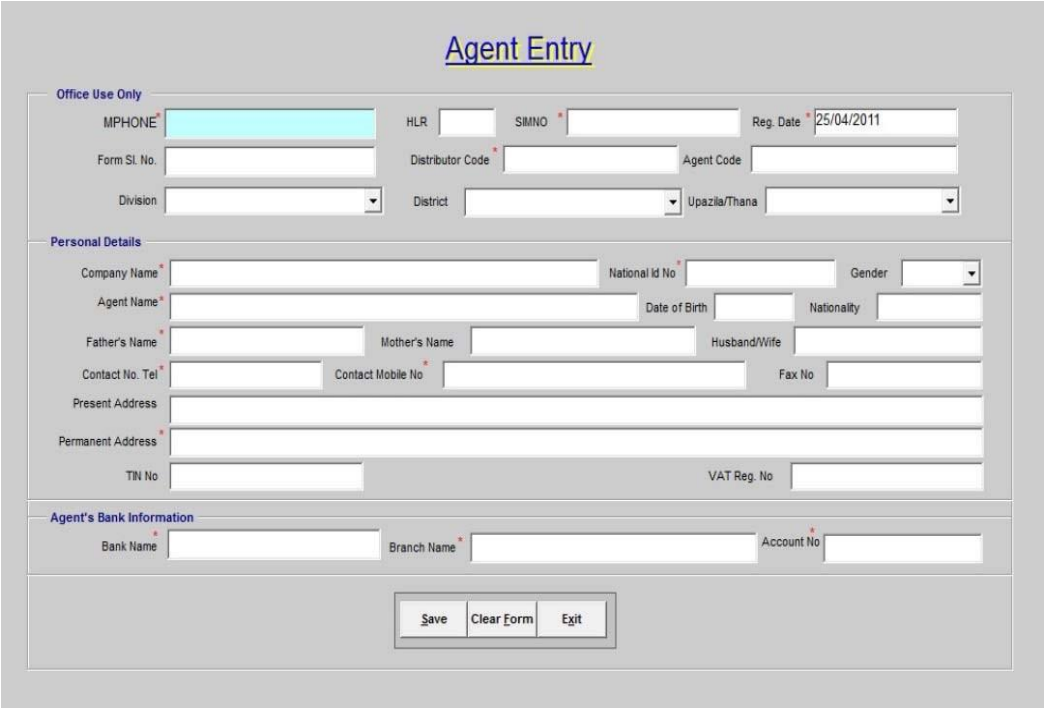


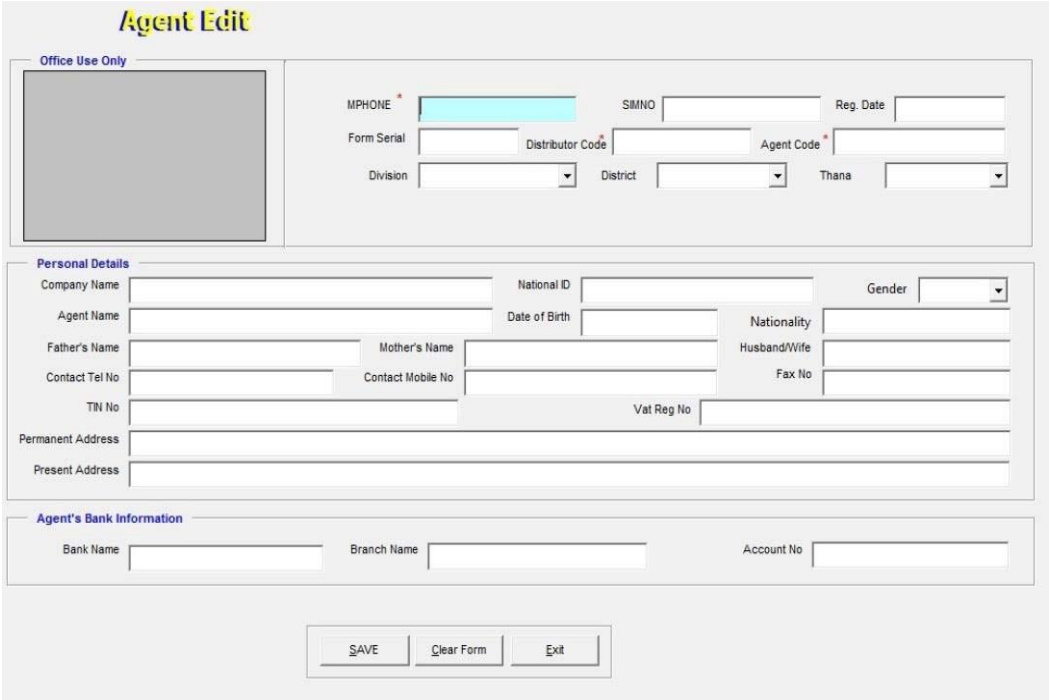




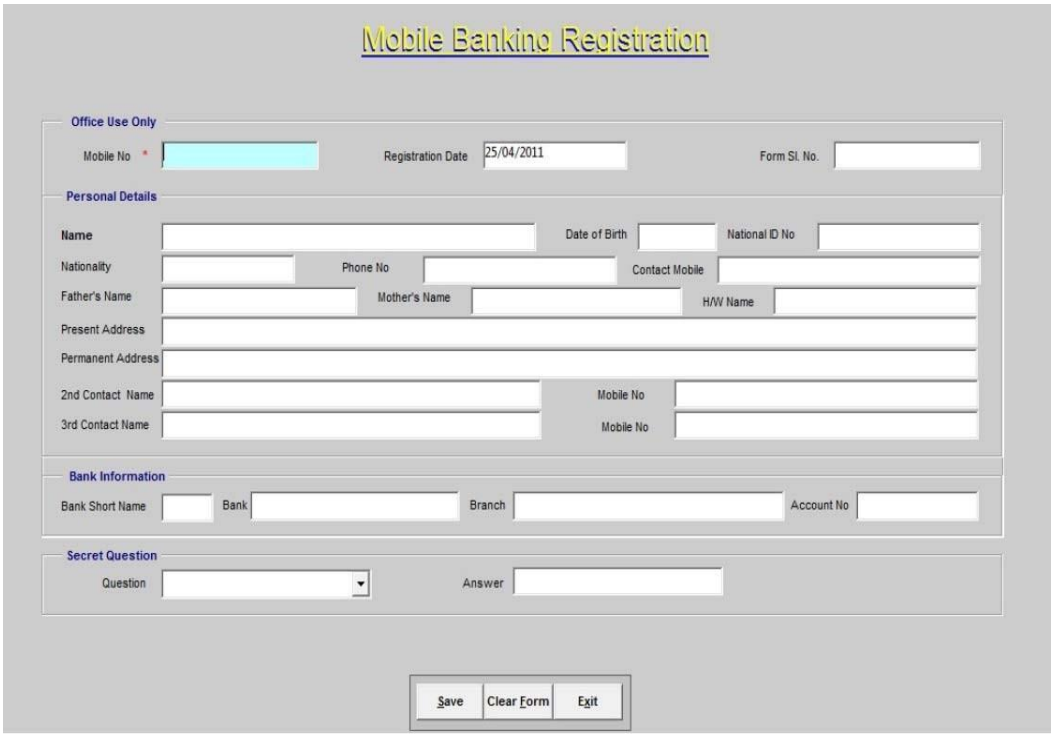


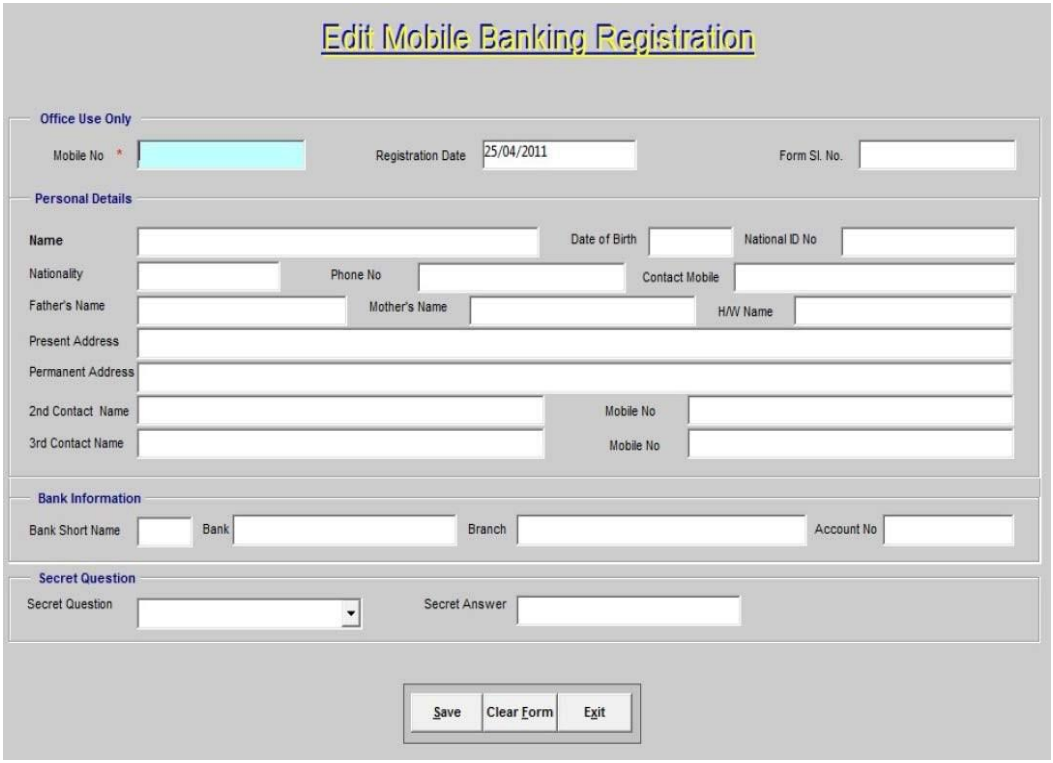
Agent Entry is also same as distributor entry.



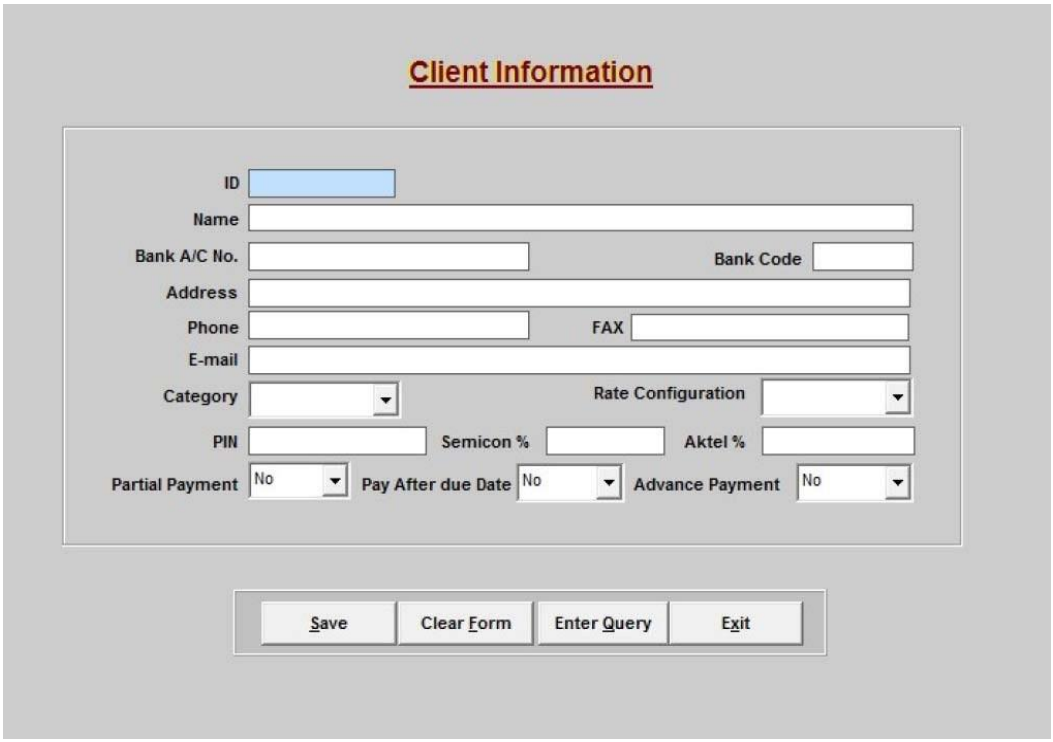


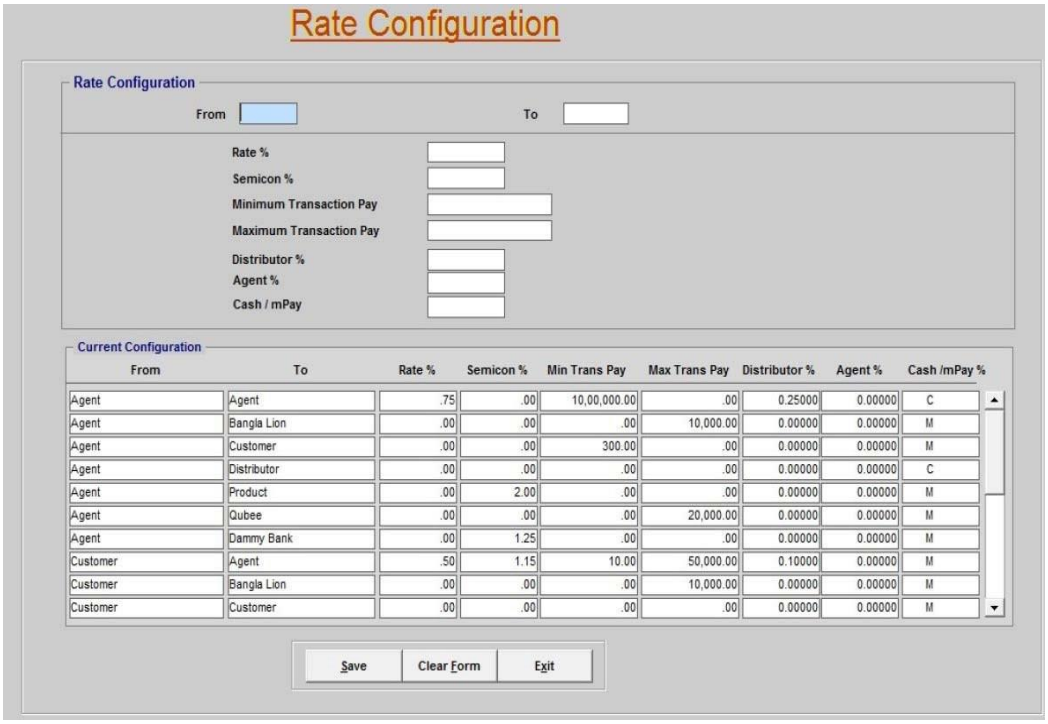
This is going to fill up by customer for mobile banking.

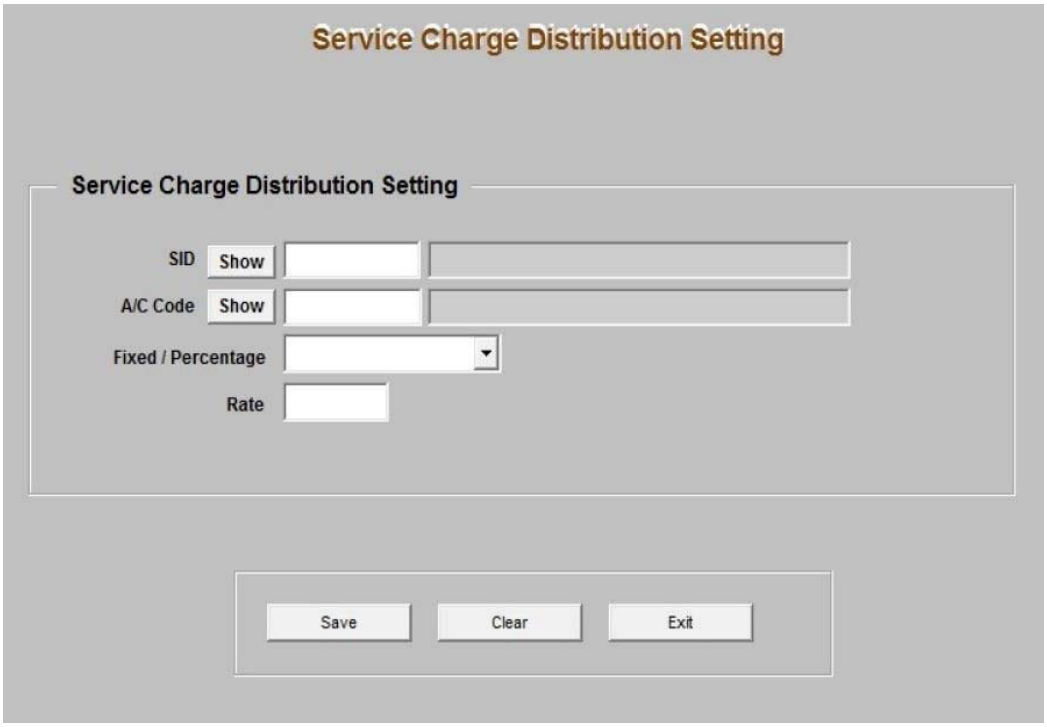




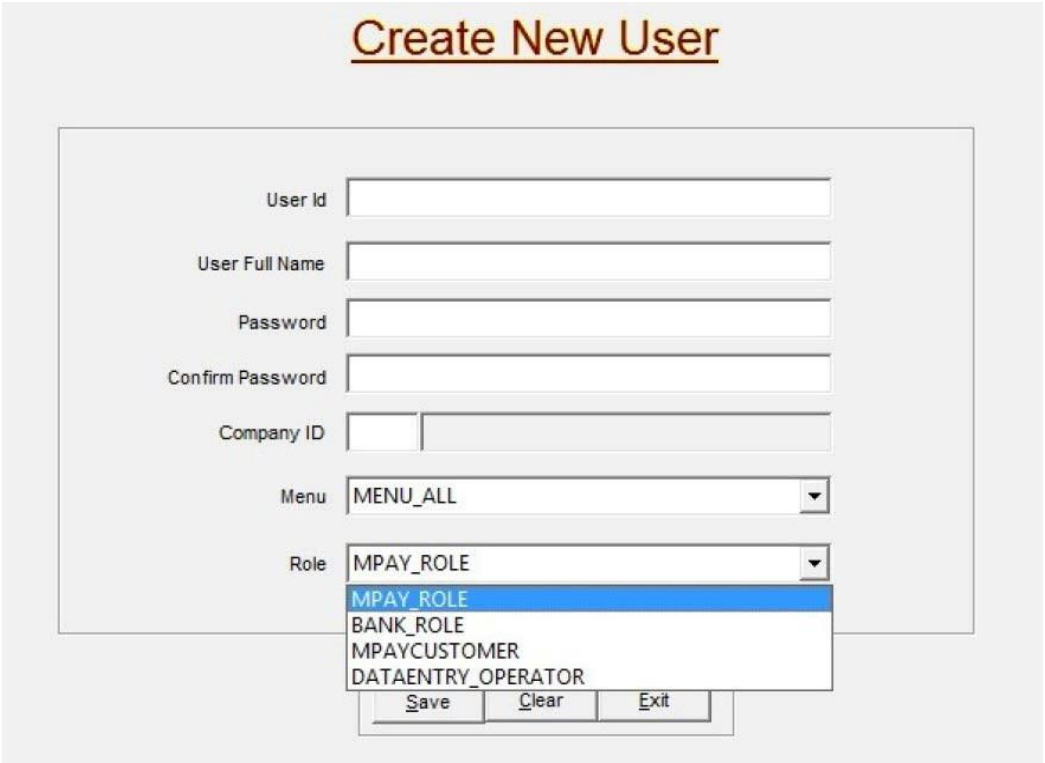
This is for client information.

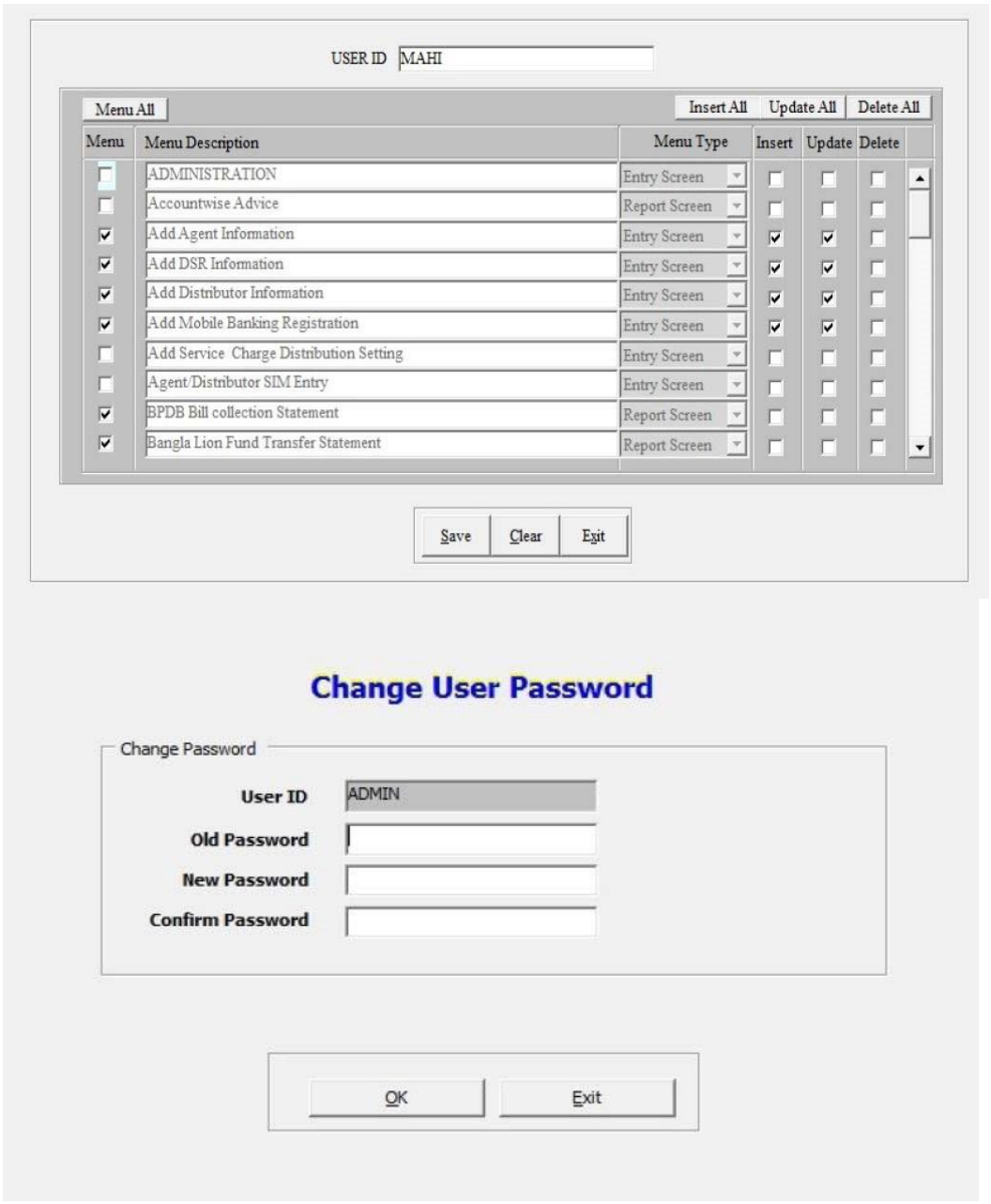


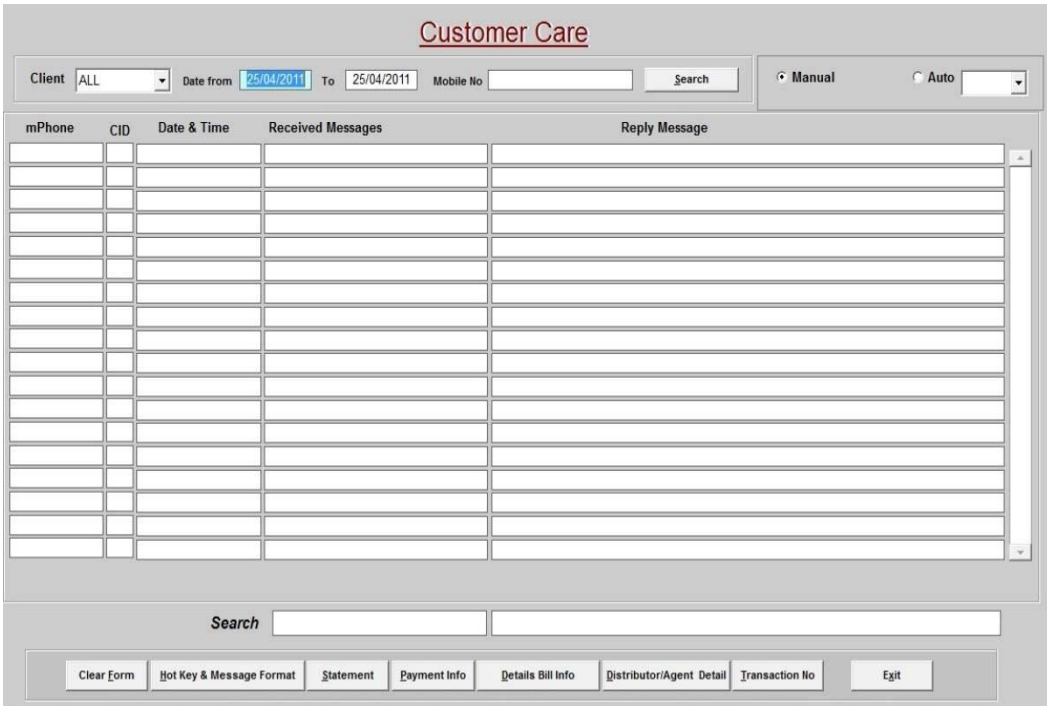


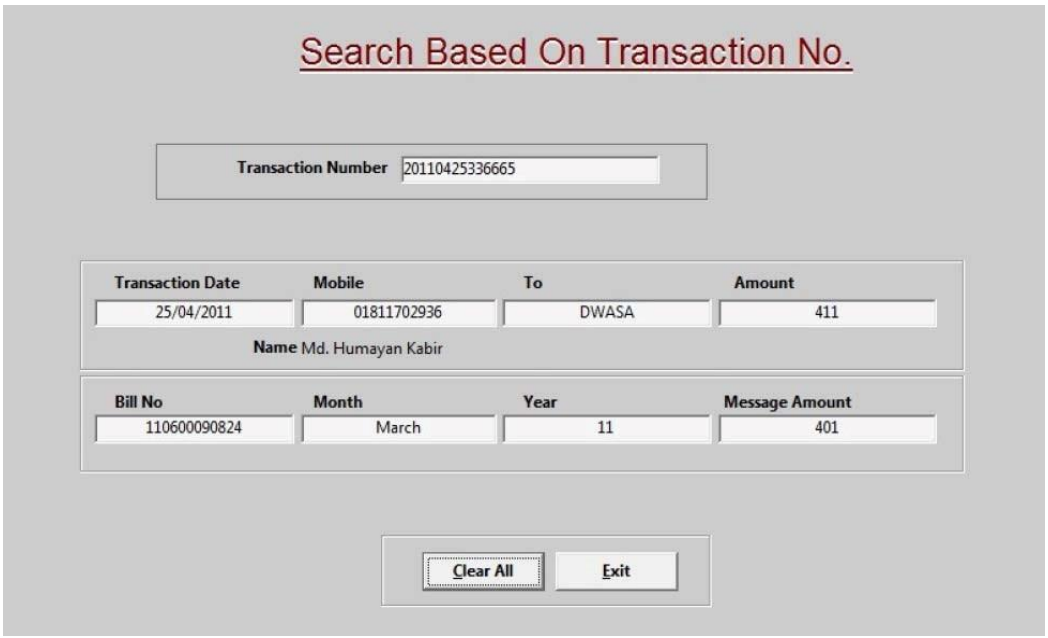


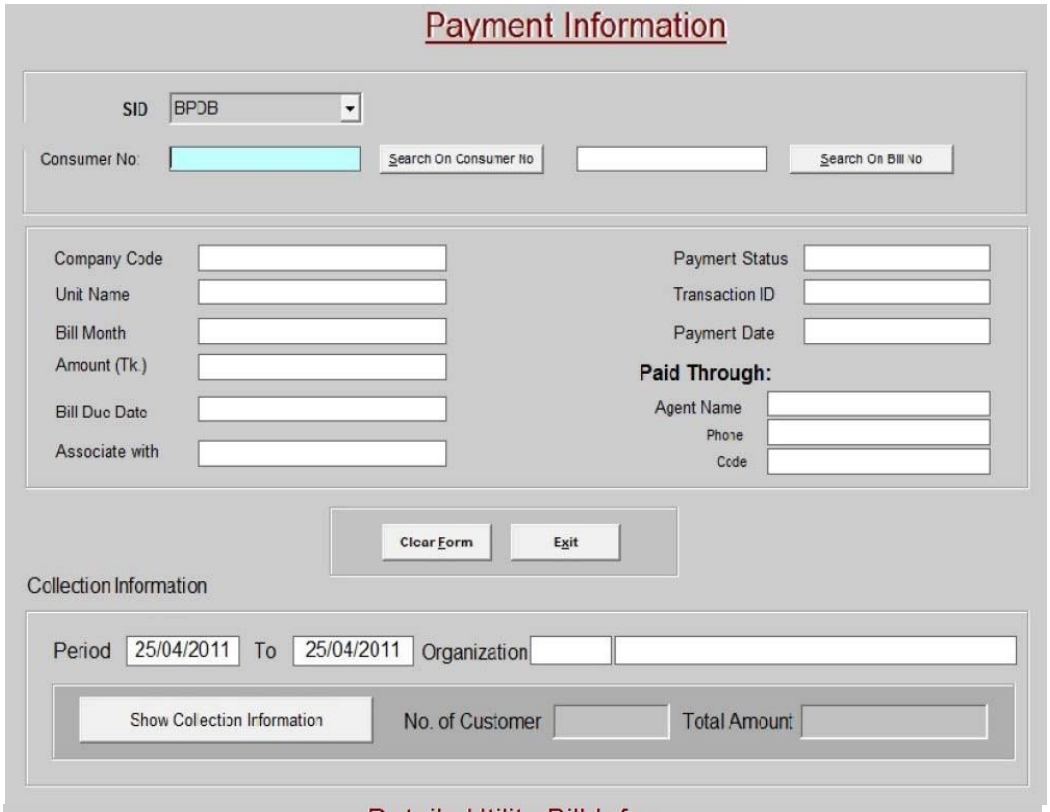
For new user this is the information bank need.

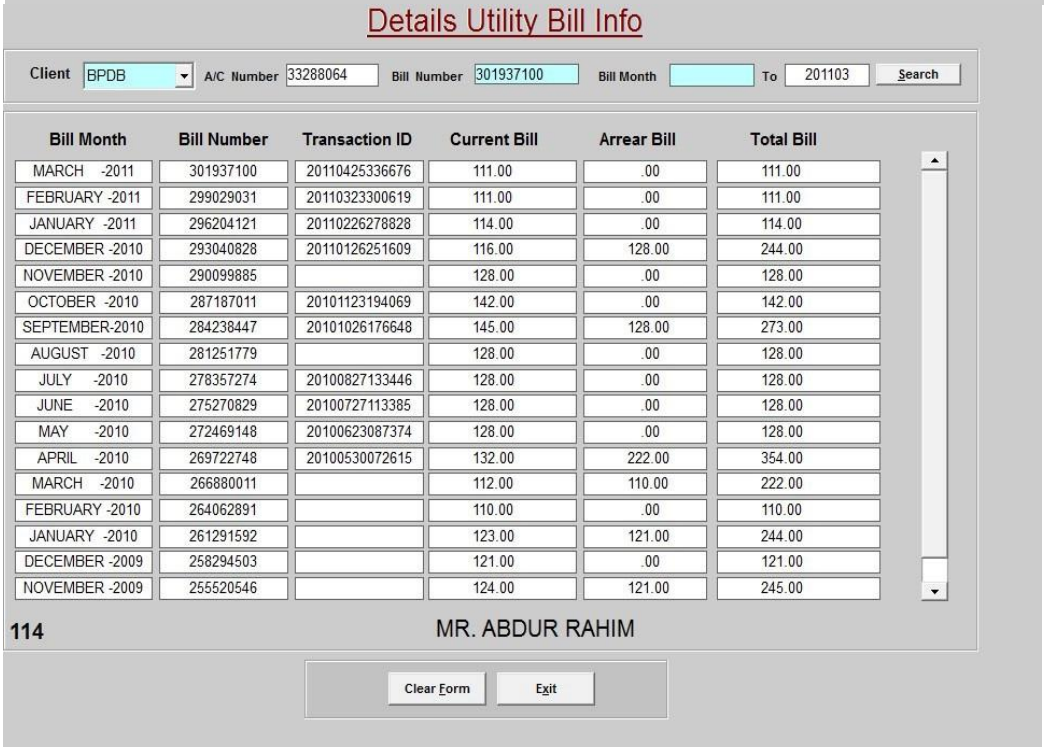




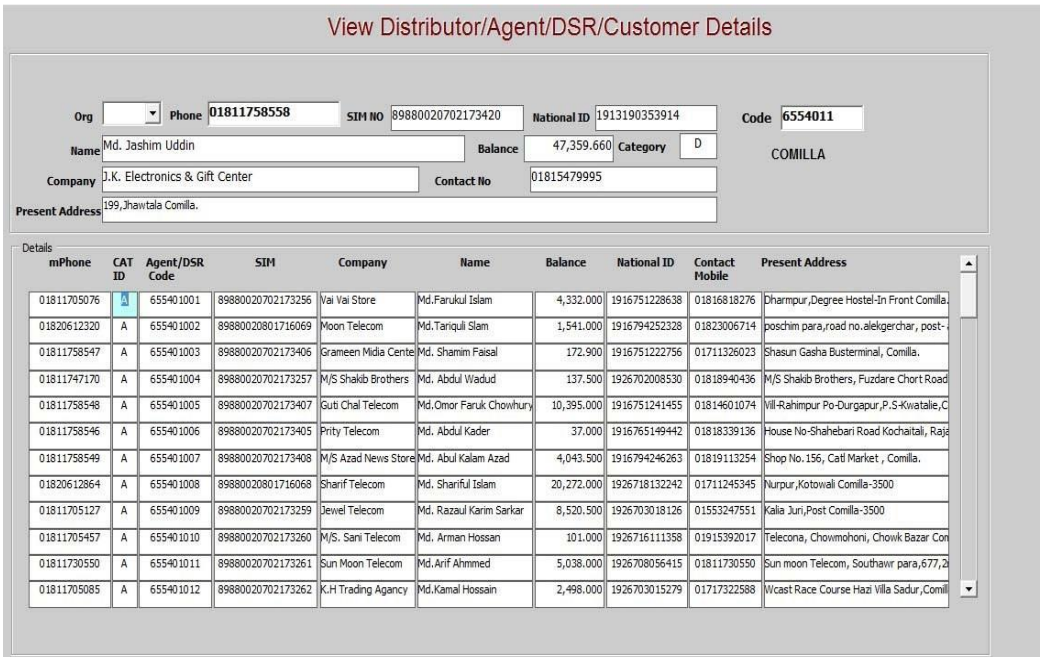








Bill Month	Bill Number	Transaction ID	Current Bill	Arrear Bill	Total Bill
MARCH -2011	301937100	20110425336676	111.00	.00	111.00
FEBRUARY -2011	299029031	20110323300619	111.00	.00	111.00
JANUARY -2011	296204121	20110226278828	114.00	.00	114.00
DECEMBER -2010	293040828	20110126251609	116.00	128.00	244.00
NOVEMBER -2010	290099885		128.00	.00	128.00
OCTOBER -2010	287187011	20101123194069	142.00	.00	142.00
SEPTEMBER-2010	284238447	20101026176648	145.00	128.00	273.00
AUGUST -2010	281251779		128.00	.00	128.00
JULY -2010	278357274	20100827133446	128.00	.00	128.00
JUNE -2010	275270829	20100727113385	128.00	.00	128.00
MAY -2010	272469148	20100623087374	128.00	.00	128.00
APRIL -2010	269722748	20100530072615	132.00	222.00	354.00
MARCH -2010	266880011		112.00	110.00	222.00
FEBRUARY -2010	264062891		110.00	.00	110.00
JANUARY -2010	261291592		123.00	121.00	244.00
DECEMBER -2009	258294503		121.00	.00	121.00
NOVEMBER -2009	255520546		124.00	121.00	245.00



View Distributor/Agent/DSR/Customer Details

Org | Phone 01811758558 | SIM NO 89880020702173420 | National ID 1913190353914 | Code 6554011

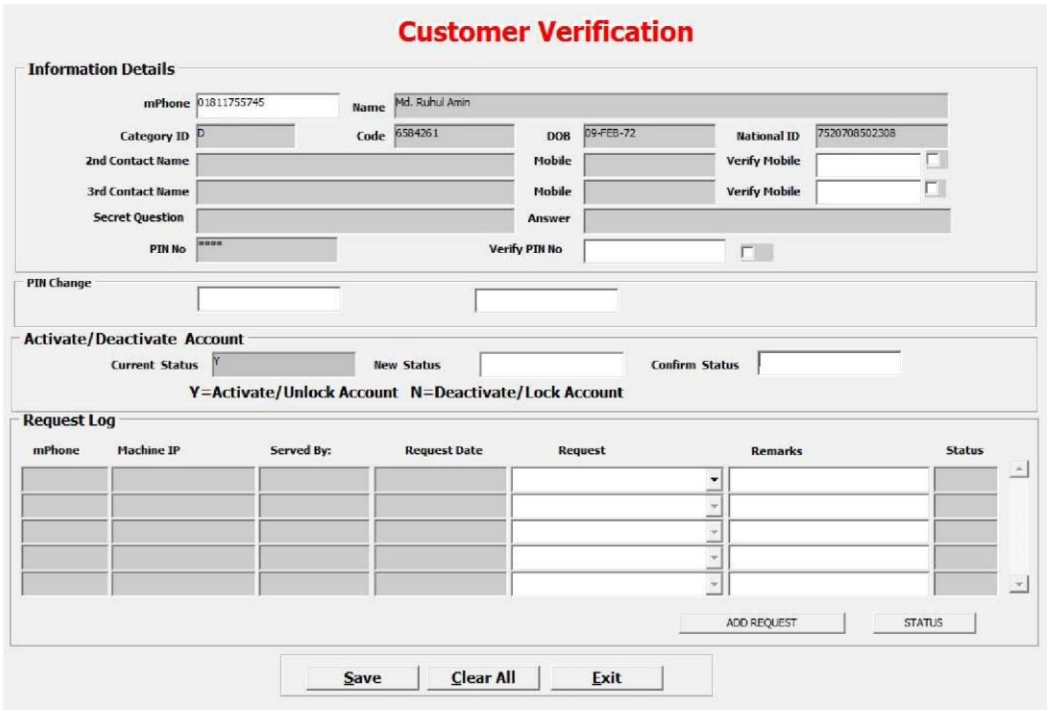
Name Md. Jashim Uddin | Balance 47,359.660 | Category D | COMILLA

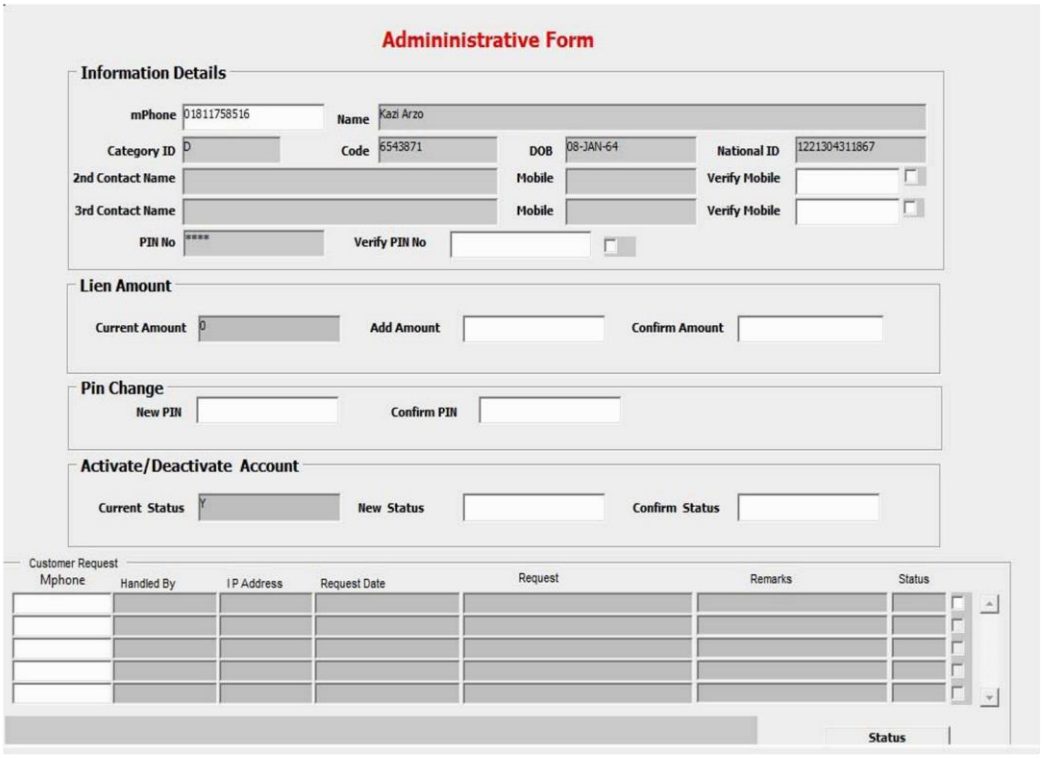
Company J.K. Electronics & Gift Center | Contact No 01815479995

Present Address 199,Jhawtala Comilla.

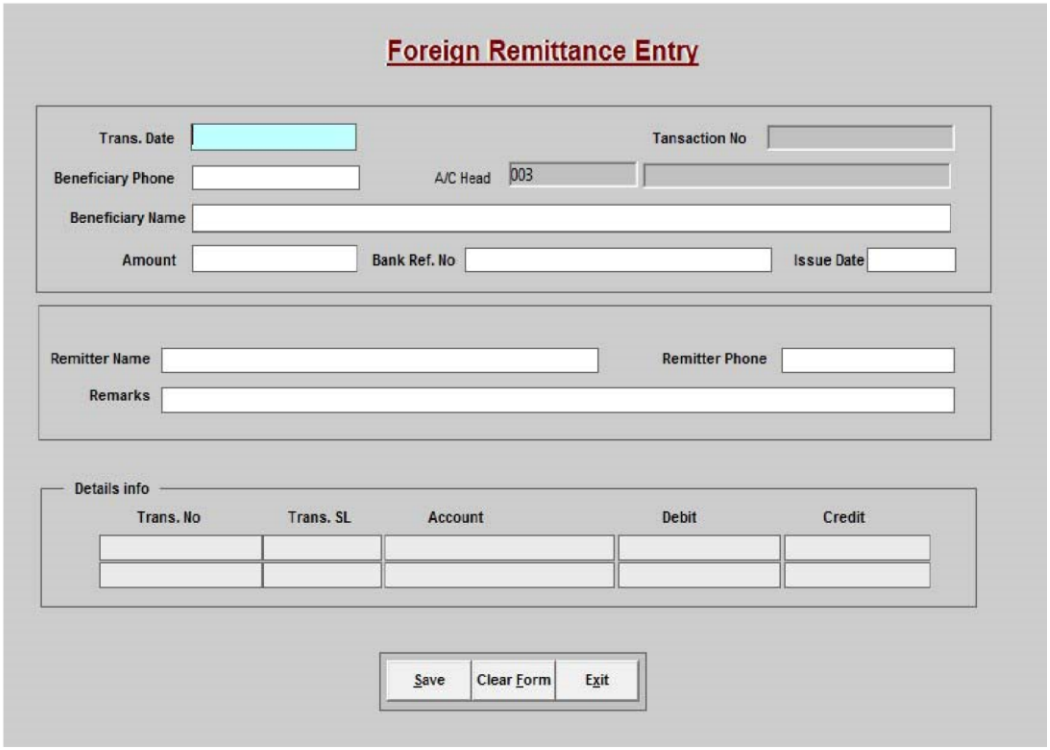
Details

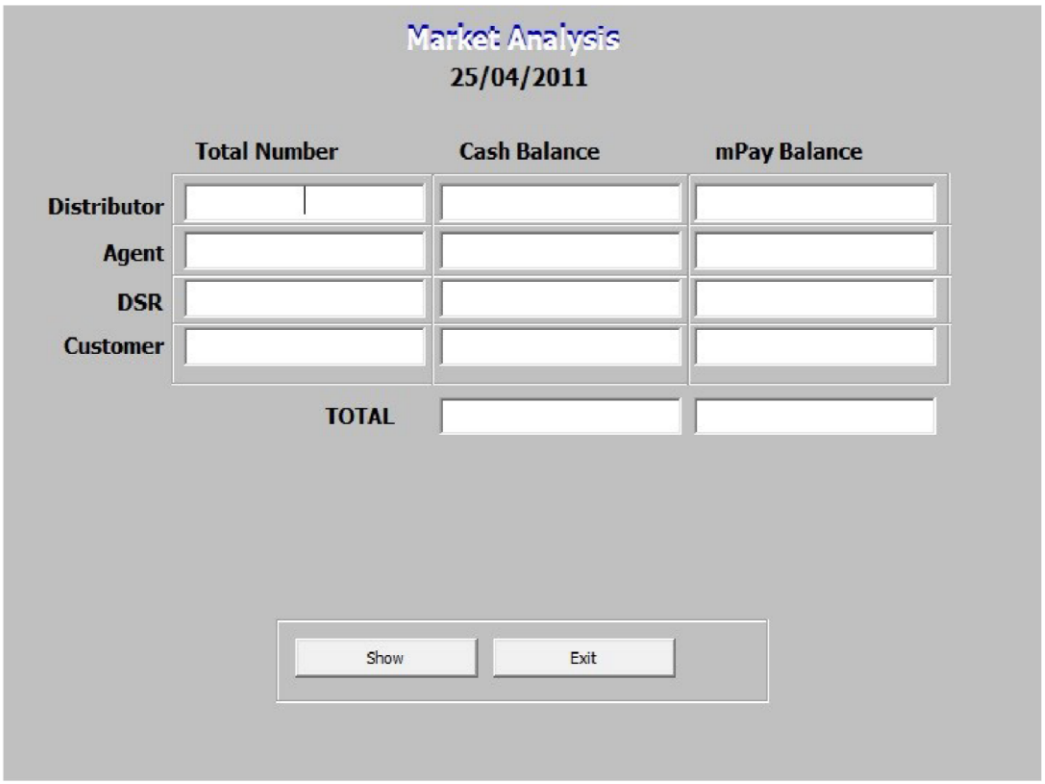
mPhone	CAT ID	Agent/DSR Code	SIM	Company	Name	Balance	National ID	Contact Mobile	Present Address
01811705076	A	655401001	89880020702173256	Vai Vai Store	Md.Farukul Islam	4,332.000	1916751228638	01816818276	Dharmpur,Degree Hostel-In Front Comilla.
01820612320	A	655401002	89880020801716069	Moon Telecom	Md.Tariquli Slam	1,541.000	1916794252328	01823006714	poschim para,road no.alekgerchar, post-
01811758547	A	655401003	89880020702173406	Grameen Midia Cente	Md. Shamim Faisal	172.900	1916751222756	01711326023	Shasun Gasha Busterminal, Comilla.
01811747170	A	655401004	89880020702173257	M/S Shakib Brothers	Md. Abdul Wadud	137.500	1926702008530	01818940436	M/S Shakib Brothers, Fuzdare Chort Road
01811758548	A	655401005	89880020702173407	Guti Chal Telecom	Md.Omor Faruk Chowhury	10,395.000	1916751241455	01814601074	Vill-Rahimpur Po-Durgapur,P.S-Kwatalie,C
01811758546	A	655401006	89880020702173405	Prity Telecom	Md. Abdul Kader	37.000	1916765149442	01818339136	House No-Shahebari Road Kochaitali, Raja
01811758549	A	655401007	89880020702173408	M/S Azad News Store	Md. Abul Kalam Azad	4,043.500	1916794246263	01819113254	Shop No.156, Catl Market , Comilla.
01820612864	A	655401008	89880020801716068	Sharif Telecom	Md. Shariful Islam	20,272.000	1926718132242	01711245345	Nurpur,Kotowali Comilla-3500
01811705127	A	655401009	89880020702173259	Jewel Telecom	Md. Razaul Karim Sarkar	8,520.500	1926703018126	01553247551	Kalia Juri,Post Comilla-3500
01811705457	A	655401010	89880020702173260	M/S. Sani Telecom	Md. Arman Hossan	101.000	1926716111358	01915392017	Telecona, Chowmohoni, Chowk Bazar Con
01811730550	A	655401011	89880020702173261	Sun Moon Telecom	Md.Arif Ahmmed	5,038.000	1926708056415	01811730550	Sun moon Telecom, Southawr para,677,2
01811705085	A	655401012	89880020702173262	K.H Trading Agancy	Md.Kamal Hossain	2,498.000	1926703015279	01717322588	Wcast Race Course Hazi Villa Sadur,Comill





This entry is for Foreign Remittance.





Chapter-5

Need for mobile banking security

5.1 The Need for Mobile Application Security

2014 will witness over 3 billion mobile users worldwide, according to Gartner's research. Mobile phones will become the preferred and most commonly used web device globally by 2013. They will be considered the most convenient device for almost everything that PCs are doing today. As a result, a large number of mobile applications will be built for multiple platforms (Android, J2ME, Symbian, etc.) and domains (mobile payments, mobile commerce, mobile Value Added Services, etc.).

As more and more transactions are made over mobile phones, hackers are perpetrating more fraud and attacks. Experts believe most security breaches are inevitable as mobile usage grows. What makes mobile phones vulnerable is the speed and advancement of technology, along with continued business demand for newer mobile products and services. Proper security controls must become an intrinsic part of mobile phones and mobile applications.

Major business impacts in case of mobile application security breach are:

- Fraudulent transactions (Revenue Loss) through mobile applications
- Confidentiality (Users sensitive data- Credit/Debit Card Data, PIN , user credentials)
- Revenue loss through communications services misuse

- Brand value degradation through SIM card cloning and related attacks
- Misuse of Enterprises Data through personal handheld devices
- Fraudulent transactions through USSD (Unstructured Supplementary Service Data) and DSTK (Dynamic SIM Toolkit) Applications

While telecoms and the rest of the service chain are becoming more motivated to deploy secure, reliable and robust products, the task is challenging. There are multiple mobile operating systems platforms, various telecom providers; banking service dependencies, and a complex network infrastructure to consider.

CONCLUSION

By working with the core IT team of Southeast Bank I have learned to deal with little big errors about the project of Mobile Banking practically. In this large and very sensitive information technology field a small flaw or security hole can bring down the whole system. The mobile banking concept of Southeast Bank is new and the system is still under construction. But I am glad that I was able to be with the team while they were making the structure, experimenting the flaws and solutions, building up a solid fraud proof mobile banking system for every Bangladeshi. Having a rare opportunity to use the knowledge and skills that I had acquired. The internship program gave me a chance not only to work with Southeast Bank Limited but also a chance to learn from the good experts. This would reflect much onto my experience to complete this project successfully.

APPENDIX

ATM- Automatic Teller Machines
BB- Bangladesh Bank
ITU- International Telecommunication Union
IVR- Interactive Voice Response
KYC- Known Your Customer
MPIN- Master Personal Identification Number
POS- point-of-sale terminal
PSO- payment system operators
PSP- payment service providers
PDA- Personal Digital Assistant
SMS- Short Message Service
STK- SIM Application Toolkit
SIM- Subscriber Identity Module
Telco- Telecommunication Company
USSD- Unstructured Supplementary Service Data
WAP- Wireless Application Protocol

REFERENCE

[1] Mobile Banking, Cited: 3 April, 2012 at 10.30 am available at: http://en.wikipedia.org/wiki/Mobile_banking

[2] STK menu, Cited: 3 April, 2012 at 11.00 am available at: http://en.wikipedia.org/wiki/SIM_Application_Toolkit

[3] Advantages and disadvantages of USSD menu, Cited: 15 May, 2012 at 12.00 pm available at: http://www.quirk.biz/resources/mobile101/285/1/Mobile-TechnologiesSMS-MMS-USSD-and-Bluetooth-Wireless-Infrared

[4] Current SMS Banking Services in South Africa, Cited: 20 May, 2012 at 8.00 pm available at: http://pubs.cs.uct.ac.za/archive/00000347/01/Security_of_Mobile_Banking_paper.pdf

[5] Advantages and disadvantages of Text SMS, Cited: 25 July, 2012 at 3.00 pm available at: https://www.itcu.org/online/virtual-branch/mobile-banking/text-sms

[6] STK, USSD, IVR, WAP, Cited: 2 June, 2012 at 1.00 pm available at: http://s3.amazonaws.com/zanran_storage/216.239.213.7/ContentPages/1000137448.pdf

[7] Text sms, Cited: 25 April, 2012 at 4.00 pm available at: http://en.wikipedia.org/wiki/Text_messaging

[8] Security threats and mitigating security risks of USSD, Cited: 5 May, 2012 at 11.45 am available at: http://blog.aujasnetworks.com/mitigating-security-risks-inussd-based-mobile-payment-applications.html

[9] STK, USSD, J2ME, SMS, WAP, IVR data security, Cited: 10 June, 2012 at 4.00 pm available at: http://www.google.com/url?sa=t&rct=j&q= &esrc=s&source=web&cd=4&cad=rja&ved=0CDUQFjAD&url=http%3A%2F%2Fs3.amazonaws.com%2Fzanran_storage%2F216.239.213.7%2 FContentPages%2F1000137448.pdf&ei=Iz9GUJzvGs3OrQeX3IGoBg&usg=AFQjCNF7czEyD_FK3iy1DPkTOMu3DyGHIw

[10] STK, USSD, WAP, IVR, Message structure, Cited: 25 June, 2012 at 3.00 pm available at: http://www.enggjournals.com/ijet/docs/IJET11-03-06-29.pdf

[11] Table 3.2, 3.3, Cited: 20 June, 2012 at 9.45 am available at:
http://www.oecd.org/dev/europemiddleeastandafrica/41837245.pdf

[12] Example of USSD Menu, Cited: 21 April at 3.30 pm available at:
http://www.dialogic.com/~/media/products/docs/appnotes/*11038*_USSD_an.pdf