Project Report

On

END TO END ANALYSIS OF MOBILE PHONE BASED COMMERCIAL ACTIVITIES

Submitted to

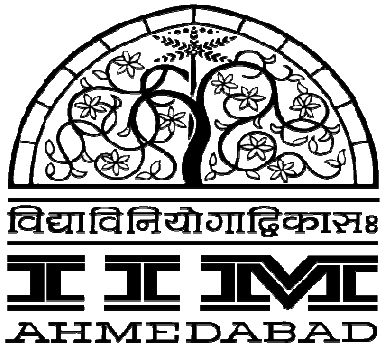
Professor Rekha Jain

Of

CISG Department

By

Prateek Sharma



Indian Institute of Management

Ahmedabad

Acknowledgements

This project has a been a great learning opportunity for me and it has been such an experience due to the immense support and encouragement provided by my project guide, Prof. (Mrs.) Rekha Jain (Faculty, CISG department IIM Ahmedabad; Executive Chairperson IITCOE). The project wouldn't have served its purpose sufficiently in the absence of her invaluable input. I would also like to express my gratitude towards Prof. B.H. Jajoo (Dean, IIM Ahmedabad) for giving me an opportunity to interact with Dr. (Mr.) R.B. Barman (Co-Chairman, Mobile Payment Forum of India – MPFI; Executive Director, RBI) whose inputs were an integral part towards building the basis of this project. I am highly grateful to Mr. Barman for his guidance as well. I would also like to thank Mr. Sashank Rajpurohit (PGP2 student, IIM Ahmedabad, Summer Intern at Airtel) for his contribution.

Last but not the least; I am grateful towards IIM Ahmedabad as an institution for providing such a learning platform for the students pursuing PGP course.

Summary

This report presents a snapshot description of the current financial activities as being undertaken by various entities in India by considering some examples. At the same time, it defines an ecosystem for discussing the m-commerce model. The ecosystem elaborates the roles of each and every significant stakeholder involved in the m-commerce process. Thereafter, the report proposes two models to be used in an m-commerce related system, namely, debit model and credit model. Each of these models is suitably explained and a comparison is done across the models. The debit model, essentially a model approved by the regulatory bodies in India is more or less similar to what has been proposed in various forums in India. However, the credit model is suitably explored and is subject to the prevalent regulatory norms. Thereafter, the report analyzes the role and responsibility of each and every stakeholder previously identified.

Using the analysis done so far, the report suggests a probable, non-traditional route for the growth of m-commerce, wherein various regulatory supports are assumed to sketch the future.

Contents

Project Details

Title of the Project

End to End Analysis of Mobile Phone based Commercial Activities

Student background

Prateek Sharma has completed his BE in Electronics and Telecommunications Engineering from Sardar Patel Institute of Technology, Mumbai University in 2009, with specialization in wireless networks and networks security. He has a keen interest in the telecommunications and associated fields. He interned at ITC, Foods Business Division.

Project Area

IITCOE, IIM A

Project Guide

Prof. Rekha Jain

Term

6 (Slot 11 and 12)

Introduction

The mobile subscription penetration is expected to increase in India at the rate of 75% with a total of 1.159 billion mobile phone users across the nation by 2013 (1). Currently, the estimated number of mobile phone (GSM) users (termed as Wireless Users by TRAI) has already reached nearly 556millions (2) or more than 730millions (2) over all mobile phone users, by the end of January 2011 with a growth rate of nearly 43.23% over December 2009 (3). If nothing at all, these statistics at least showcase one very important thing, i.e., the accessibility of mobile phones, or if it can be suitably reworded – reach-ability of mobile phones. This is one of the main reasons that RBI (Reserve Bank of India – *see footnote*[1]) has decided to push all the nationalized (Private and Public Sector Units) banking units in India towards adoption of mobile phone based and other similar wireless technologies in their banking services as a means to achieve financial inclusion across India. Even though there's a significant heterogeneity in terms of "reach-ability levels" of mobile phones in urban areas versus rural areas, it is a fair start to what may turn out be a revolutionary process of bringing banks and people together across India.

However, we must also remember that banking need not pick up unless there's a need to bank, i.e., a person enabled to access banking services through mobile services may not necessarily access banking services unless there's a need to do the same. It is absolutely essential for that person to have some sizeable cash to put to use for banking services (or suitable guarantees to avail loans), especially in rural areas. Thus, the whole setup of bringing about financial inclusion is also dependent on mobile technology being able to aggregate and service very small monetary amounts at profitable returns (for the major players who are affected directly per transaction - like banks and their customer). This brings into the picture the role of m-commerce, or usage of mobile technology not just for banking, but any and all kind of financial transactions as permitted by the legal authority.

[1] RBI – Reserve Bank of India: The central governing bank of India, committed to maintaining nation's monetary and financial stability, http://www.rbi.org.in/scripts/AboutusDisplay.aspx#

Currently, mobile phones not only act as a voice communication medium, it also acts an information node, through which generation, relay and reception of information can take place in a rapid and cost-effective manner. Hence, it is to no surprise that the value added services, which rely on exactly these features of mobile phones, have picked up the market recently. And most noticeably, one of the most interesting and most awaited services is that of commerce. However, due to the sheer number of transactions, regulations and operational nodes involved, there is a need to study the entire chain of mobile commerce, from the consumer end to the financial institutions involved.

There have already been some advances in the field of Mobile Banking largely due to the involvement of the private players. At the same time, the government has tried to regulate this domain from time to time by issuing various guidelines which may or may not have been followed, especially in the mobile banking practices, which have had a start as early as in 2000 whereas guidelines were being issued only by 2008, by RBI. Nonetheless, it is essential to get a brief a snapshot of the contemporary mobile banking practices as well as the future of it.

Current Practices

M-Commerce

M-commerce, a widely accepted term to quote any commercial/financial activity taking place through a mobile phone, is a rapidly gaining significance in India. One can also define m-commerce as any transaction of goods or services or transfer of information that may lead to such a transaction, through wireless devices like mobile phones. Thus, the scope of m-commerce extends beyond the initial one time exchange of information or just the fist transaction. (E.g., there can be small amounts in payment of micro-insurance premium through mobile phones or payment towards a purchase as small as INR 5).

With the success of models like m-Pesa in Kenya and Hal cash in Spain, the financial institutions and telecommunication service providers, including some of the consumer telecommunications equipment manufacturers are readying themselves to enter this field and are awaiting the conducive regulatory environment to support them. Already in India, banks like HDFC, ICICI, Citibank, SBI, etc have started provided financial transaction services to their clients. At the same time, telecommunication service providers like Airtel and Vodafone have also added these services as a part of their VAS. Recently, third party institutions (third party because they are directly not involved in transactions themselves, but provide a medium for the consumers and the financial institutions to interact with each other) like ngpays and IMT (empays) have developed a significant user base.

Currently in India, due to regulatory restrictions by RBI (no private institution allowed to create its own currency, whether physical or electronic; limited transactions allowed through mobile phones and only licensed institutions allowed to deposit cash), the m-commerce services being provided are merely mobile banking and its extensions. There still hasn't been a system in place to replace cash with electronic cash with complete synchronization across all the stake holders.

However, one can look at the models of services like Oxicash (m-wallet) or Airtel semi-closed wallet [4] which have attempted to develop a system wherein, cash is deposited in advance through bank accounts (with associated, partner banks) and then the user is provided with an access to the bank accounts (for Oxicash, the user gets points mapped proportionally to the amount registered for transaction whereas Airtel users get direct debit facility from the bank account itself), on her mobile phone which can redeemed for financial transactions across all partner sellers, including the ability to transfer points/money equivalent amount, and hence, cash from one individual to another using only the recipient's mobile number (the recipient needs to be an Oxigen user as well).

Thus, there have been ventures to widen the scope of m-commerce beyond m-banking through partnerships and associations across financial institutions, sellers and telecommunication service providers. These ventures have so far been restricted by the regulations of RBI, which are moving more and more into the direction of favoring m-commerce.

M-Banking as a means of M-commerce

There are broadly three categories of m-banking systems,

1. Bank driven

   Here, bank hires a vendor and provides the service to only its customers at negligible or no costs. Leaders – ICICI, Citibank, HDFC, SBI. The mode of payment is through account transfers from the customers' account to the sellers' accounts (usually through a third party secured transaction channel like VeriSign, etc)

2. Telecom service provider driven

   Here, the telecom service providers use their network and user connections to enable the users pay through partners' banks, either through an inbuilt portal on the phone or in the network applications. Leaders – Airtel, Vodafone, etc

3. Third party driven

In this model usually a third party vendor collaborates with multiple banks and provides services like account transfers across various services, to the customers, usually independent of the cellular service provider. Leaders – ngpays, empays, etc. recently, Nokia has decided to provide such a service through its vast operations in India.

General m-banking practices:

1. Accounting (only for a fixed number of banks, those which are associated with the m-banking service providers or the banks themselves)
    - Cheque related operations
        i. Cheque book request
        ii. Cheque stopping
        iii. Cheque monitoring
        iv. Cheque status
    - Funds transfer
        i. Interbank funds transfer
        ii. Interbank funds transfer
        iii. RTGS
        iv. Account summary
        v. Transaction summary
    - DEMAT Account monitoring and transactions
    - Loan account operations
        i. Loan letters
        ii. Repayment
        iii. Reschedule, etc
    - Customer care operations (branch locator, ATM locator, etc)
2. Third party purchases
    - Movie tickets
    - FMCG purchases in association with big brands
    - Transport service providers
    - Utility bills
    - TV channel payments, etc

- Insurance payments
- Purchase of items from selected online shops and courier
- Travel ticket booking

Typical characteristics of services being provided so far:

1. Essentially Account Transfers from a consumer to a business
2. Through collaborations with banks as well as sellers, even service providers or app designers
3. Financial transactions essentially by a bank or a licensed financial institution only
4. Modes used – SMS, WAP, GPRS and now 3G based internet access supported by a secured, encrypted transaction service

Miscellaneous Services as a part of M-commerce

1. Entertainment
    a. Games
    b. Wall papers
    c. Ring tones
    d. Chat servers
    e. Caller tunes
    f. TV clips
    g. Voting for entertainment channel programs, etc
2. Business
    a. Stock market updates
    b. News updates
    c. Travel updates, etc
    d. Promotional
        i. Advertisements
        ii. Mobile coupons
        iii. “earn by viewing ad” promotions
        iv. Information about promotional events, etc

3. Education - Updates about admission procedure
4. Miscellaneous – SMS based social networking (interactive, and not static like other entertainment modes)

The above services are examples of service provider using the mobile phone usage charge (pre-paid – deposit or post-paid – billing) for providing commercial services. Here, the content may be through a third party, but billing is essentially taken care of by the telecommunications service provider.

M-Commerce Ecosystem

Mobile commerce has been a logical extension of e-commerce and a probable driving force to popularize m-banking, which would eventually contribute towards financial inclusion by popularizing mobile devices as a means of financial transaction. Some parallels can essentially be drawn from e-commerce (Electronic commerce – *see footnote*[2]) which most of the banking users (out of 60millions internet users in India, 6millions users use e-commerce to generate a business of nearly INR 100millions [(5)]). However, unlike e-commerce which mostly involved tools like credit cards, debit cards, online accounts, cash coupons, etc, m-commerce involves a completely different setup.

The most significant players in an e-commerce setup were banks which allowed usage of tools like credit cards et al, payment gateways like Billdesk, CCAvenue etc, and the end retailers that allowed the consumers to use such tools for making such purchases. This was further supported by RBI in the form of recognition of electronic receipts and invoices. The third party players, essentially the connectivity providers (internet connection service providers, website hosting service providers) had no active roles to play in any financial transaction so far. Effectively, this ecosystem consisted of only a basic bare bone structure. However, with the advent of mobile technology in the early 2000's and its adoption by private banking players in the later years, a new eco system started to develop where regulatory bodies had a larger role to play. At the same time, the infrastructure providers, i.e., telecom service providers were also expected to have an active role. For the purpose of this report, the focus will be mainly on the m-commerce aspects of this ecosystem and it will be referred to as the "m-commerce ecosystem" frequently.

[2] **Section 2.2.1** - … E-commerce involves individuals and business organizations exchanging business information and instructions over electronic media using computers, telephones and other telecommunication equipments…. RBI Report on Internet Banking, published on 22nd June, 2001. Copy at http://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=243

The m-commerce ecosystem consists of mainly four bodies performing various functions namely:

1. Regulatory Body such as RBI
2. Financial Institutions like Banks and NBFC's
3. Execution and operation Institutions
4. Direct users like mobile phone users and retailers

It is important to note that a major regulatory role will be played by RBI and not DoT (Department of Telecommunications, India: *see footnote*[3]) or TRAI (Telecom Regulatory Authority of India: *see footnote*[4]) as the primary operation being executed here is of a financial/monetary nature. However, the telecom providers are in no way exempt from any regulations as imposed by TRAI with or without collaboration from RBI. Thus, it's a tight rope walk for not just the financial institutions but also for the operations institutions in this ecosystem. This may not necessarily be the case in foreign nations where m-commerce has already amassed a huge business such as in Kenya.

Unlike other nations like Brazil, Mexico, Kenya, South Africa, Philippines, etc, the regulatory body for financial matters in India, Reserve Bank of India (RBI) has always maintained a strict control over merger of technology and financial transactions in an evolved and mature economy like India. However, with the advent of technology, RBI has progressively drafted guidelines towards adoption of various ICTs (Information and Communication Technology) by nationalized banks. In case of m-commerce, a significant step was made in drafting of the Mobile banking Guidelines [(6)] by RBI in September 2008 followed by modifications of the same subsequently in 2009, 2010 and most recently, January, 2011. As a matter of fact, RBI has centralized the entire process of mobile related financial transactions through the inception of IMPS (Interbank Mobile Payment Service). We may also see TRAI coming up with another set of guidelines as to which set of telecom service providers are certified to be an active part of the m-commerce ecosystem.

---

[3] **DoT or Department of Telecommunications -** Responsible for executing any Policy, Licensing and Coordination matters relating to telegraphs, telephones, wireless, data, facsimile and telemetric services and other like forms of communications in India. It is equivalent to the Ministry of Communications and Information technology. For further details, please visit - http://www.dot.gov.in/objective.htm

[4] **TRAI or Telecom Regulatory Authority of India** – Responsible for providing a fair and transparent policy environment which promotes a level playing field and facilitates fair competition. It has issued several directives, orders and regulations covering a wide range of subjects including tariffs, interconnection and quality of service as well as governance of authority. For further details, please visit - http://www.trai.gov.in/aboutus.asp

However, TRAI's involvement may not exceed beyond the technology stand point and may largely be an advisory role.

In terms of the significance of the roles, we can have the following structure of the m-commerce ecosystem:

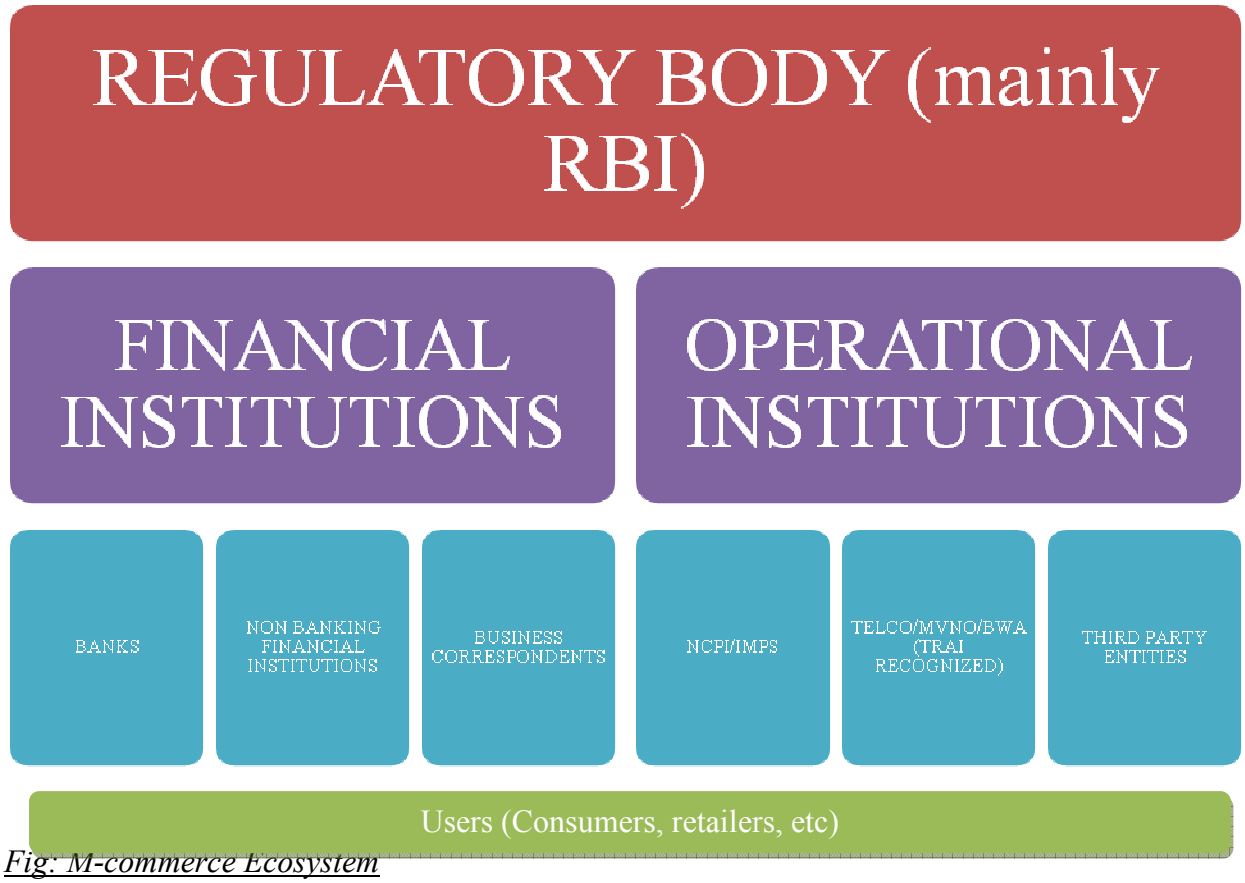


Fig: M-commerce Ecosystem

1. The financial institutions are at the helm of providing m-commerce; however, they lack the necessary technology setup. In fact, it is not their core competency to implement the necessary ICTs. Their expertise lies in the domain of financial transactions, and most importantly, experience of adhering to RBI's norms, especially the KYC [(7)] (Know your Customer) norms. Moreover, the banks are already aligned towards each other's business processes by the means of core-banking and inter-banking. It is for these reasons that RBI holds financial institutions like banks (or all those institutions that have retail banking license) responsible for delivering m-commerce services and it is for these reasons alone,

such institutions will like to collaborate/cooperate with players in the mobile phone industry.

2. The users of m-commerce (remitter and beneficiary) are necessarily current mobile phone users who have been authenticated by nationalized and registered (with RBI) banks under KYC [7] norms.

3. The most important players of this ecosystem from the technology point of view are execution and operation institutions. For the purpose of this report, following entities will be considered as a part of this system:
    a. Current as well as future mobile service operators holding telecom licenses in 23 circles on India, as recognized by DoT (Department of Telecommunications) and TRAI – Telecommunications Regulatory Authority of India (e.g. Airtel, Vodafone, etc)
    b. Mobile virtual network operators (MVNO) like Virgin Mobile
    c. Third party entities purchasing usage of telecom licenses (as defined by TRAI and DoT) for rendering m-commerce services to financial institutions (those holding a banking license)
    d. National Payments Corporation of India (NPCI [8]) along with its Interbank Mobile Payment Service (IMPS [9])
    e. Possible BWA (Broadband Wireless Access) entrants using BWA licenses to provide m-commerce/e-commerce services or their variations hereafter.

A few assumptions (in the absence of any written or visible instructions) from ecosystem are highlighted for the purpose of this report:

1. The overall governing authority (regulations) will be RBI
2. The financial institutions and operational institutions have to comply to RBI guidelines and at the face and at the same time, operational institutions like telecom service providers are expected to adhere to regulations as expected by DoT.
3. The IT (Information Technology) service providers have to comply to RBI guidelines as well.

4. The eventual purpose is to allow seamless transaction across any bank over any infrastructure using any personal hardware (mobile phone) for all registered users (KYC norms adherence – *see footnote*[5]).

[5] **KYC** [(7)] **or Know your Customer Norms:** Section 1.1 - The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. For further details, please visit - http://rbidocs.rbi.org.in/rdocs/notification/PDFs/MCKYCC010709.pdf

The Process for m-commerce

The process of m-commerce involves several entities such as mobile device, banks, mobile network operators, IMPS, etc. This report explores two different models which are sufficiently but not comprehensively analyzed in the forth coming sections. The models assume the various entities as a set of roles/responsibilities and distinguish between them on the basis of the functions they perform. There may be several other classifications via various combinations of the functions other than what have been proposed below.

Debit Model

Following is a preliminary flow of transactions between a remitter and a beneficiary using m-commerce, highlighting the flow of data and the various independent entities having partial or complete access to the data:

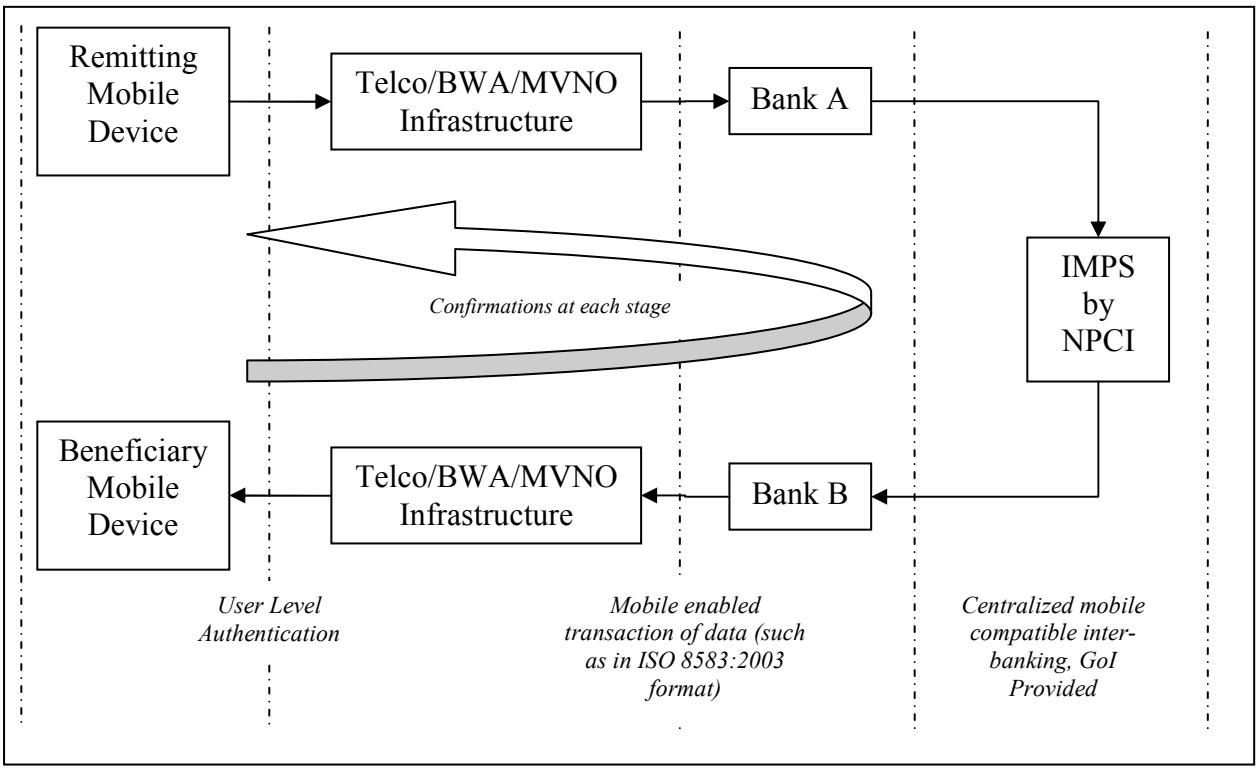


Fig: Flow diagram 1 for m-commerce in terms of flow of the data and the entities having access (partial or complete) access to the data

The above process flows as:

I. The remitter (who wants to credit some amount towards a purchase into the beneficiary's account) accesses the relevant m-commerce feature on his/her mobile phone. The mobile phone authenticates the remitter as the verified user of the account that is being accessed with that phone. The authorization session may last as long as a single transaction is over or till certain, pre-decided time limit is exceeded, whichever is earlier.

II. The remitter enters the unique mobile transaction ID of the beneficiary (to be referred to as MMID or Mobile Money ID, by NPCI) that is also associated with the account number of the beneficiary's bank account. The mobile device verifies whether the MMID is valid or not and only then the transaction proceeds further. There is a need to prevent transactions with a wrong person. This need is even more emphasized by the fact the unlike in a normal RTGS or NEFT transaction, m-commerce will follow a soft real time (*see footnote*[6]) procedure. The validation may be supplemented by entering the following details simultaneously:
    a. Beneficiary's registered name
    b. Account number
    c. MMID

III. Once the source and destination for the transaction are verified by Bank A (remitter's bank) and Bank B (beneficiary's bank), the remitter sends the details of the amount to be credited to Bank A.

IV. Bank A transfers the relevant amount to Bank B through IMPS. At the same time, it removes the said amount as well as transactional charges if any, from the remitter's account.

[6] Soft Real Time – (quoted as it is)…Soft real time applications are those that would not suffer a catastrophic failure if some of their deadlines were not precisely met. They usually must satisfy a deadline, but if some percentage of deadlines is missed by a small interval, the results may still be considered to be acceptable. An example is the transmission of live audio and video content via a network; although violation of constraints may result in degraded sound or image quality, the system can continue to operate. Other examples include systems that maintain and update the flight plans for commercial airplanes, online banking systems and virtual reality systems. For further details, please visit - http://www.linfo.org/real_time.html

V. Bank B debits the amount into the beneficiary's account. It then sends a confirmation of the transfer of amount to the beneficiary and the Bank A. Bank A in turn closes the transaction and sends a confirmation to the remitter.

This method of using MMID's to identify an m-banking enabled mobile user has already been initiated and so far, nearly 6 million MMID's have been issued. However, this distribution has not met the intended purpose of promoting m-banking as there haven't been a significant number of transactions so far because nobody is paying through this method. One of the problems as identified during MPFI (MPFI – Mobile Payment Forum of India, *see footnote*[7]) meetings is the lack of ease in relevant mobile phone application installation and activation for using m-banking. It is believed that with adequate pricing and improvement in available technologies, m-banking through MMID's will flourish.

Credit Model

The same process can also be viewed in a different manner wherein, the payments are instantaneously done with or without the presence of a communication technology to connect to the respective banks. This model is specifically useful for areas with a low or intermittently available network/cellular infrastructure (such as rural areas in India which can't boast of a communication infrastructure as comparable to the urban areas). Following is a brief description of such a model (next page):

[7] MPFI – Mobile Payments Forum of India is a jointly launched forum by IDRBT (Institute for Development and Research in Banking Technology, India) and RTBI (Rural Technology Business Incubator, IIT Madras, India) that aims to enable mobile payments in India with secured and low cost transaction. For further details, please visit - http://www.mpf.org.in/

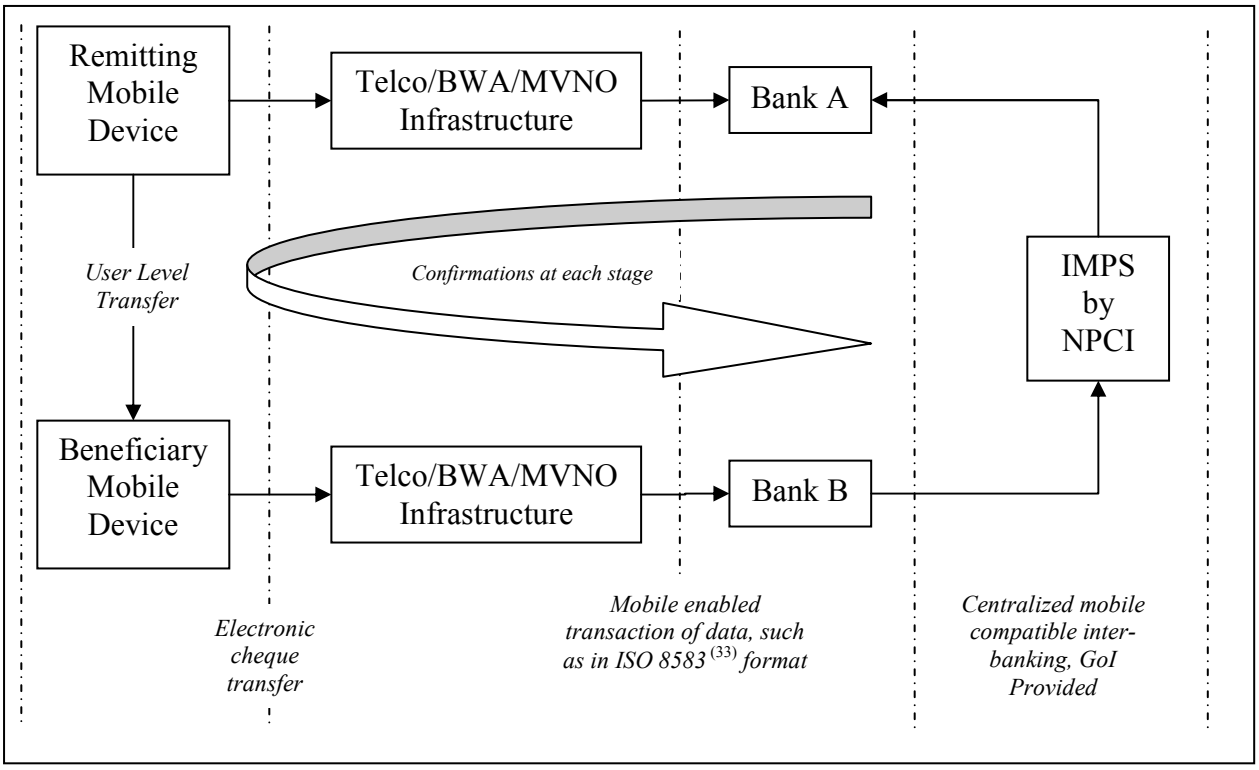


Fig: Flow diagram 2 for m-commerce in terms of flow of the data and the entities having access (partial or complete) access to the data

I. This model is very much similar to the system of a cheque. Here, the remitter sends an e-cheque to the beneficiary mobile device equivalent to the amount that needs to be transferred.

II. The e-cheque must consists of the following details:
   a. Remitter's MMID
   b. Remitted amount
   c. Remitter's bank ID

III. The Beneficiary's mobile device will add its own MMID and send the e-cheque to its own bank, Bank A. This transfer of data may or may not happen instantaneously if there's an issue in the connection system. Therefore, the transaction doesn't terminate and there's flexibility about the same. The users can terminate the transaction for their own convenience, leaving their mobile devices and the banks to sort out the details as and when the connection resumes. However, for such a model, following issues may be considered:

a. There has to be a limit to the number/volume/value of such transactions so as to limit the accumulation of the amount in the remitter's mobile device without any clearance with the banks. This will prevent any fraud from the remitter's side to some extent.

b. The MMID and other remitter details (the geographical location/time) and other such possible unique identifiers to identify the remitter in association with each and every such transaction must be unique and static. At the same time, the details should be backward traceable to identify the remitter, the associated bank and the communication services at any point of time post transaction.

c. This information should be easy to access by the enforcement authorities as well as audit agencies.

d. The MMID issuer should ensure that the remitter is always traceable through any address details and is verified as per KYC norms.

e. The mobile devices used in this kind of transaction should be completely tamper-proof and at no time should the transaction details lying on the remitter or the beneficiary's mobile devices be modifiable.

f. The network/cellular infrastructure though not needed in an "always available" manner, should be available such that there isn't a delay beyond a certain gap for the mobile devices to be able to communicate with the devices.

g. The security requirement of data are much more stringent across all channels (mobile device, MNO or Mobile Network Operator's equipments, bank's server) in this model as the data is to be protected for a longer duration than that in the previous model.

Since the duration is longer, it becomes easier, relatively speaking, to maliciously access the data in the absence of a sufficient security system.

IV. Whenever the remitter's or the beneficiary's mobile devices are able to communicate with their respective banks, bank A will temporarily close the transaction and will assume that the remitter has made all the payments to the beneficiary and will recognize it. At the same time, it will transfer the relevant amount to the beneficiary's account.

V. The remitter will indicate Bank A about the transfer of payments from the associated account to the beneficiary's account in Bank B as soon as the associated mobile device is able to connect to the bank.

VI. Bank B will confirm the transfer of accounts from the remitter to beneficiary by communicating the same from Bank A through NPCI's infrastructure.

VII. Only after this confirmation, the bank A will deduct the said amount from remitter's account and close the transaction at its end.

VIII. The entire transaction has the flexibility in terms of lesser need for an "always on" communication system and can still provide an "apparent" real time transaction.

Differences between the two models

1. In the previous model the transaction is considered complete only after a complete transfer and authorization of transaction by both the banks involved in the transaction. In a way, this system is very much similar to a Debit Card system and is based on the principles of accounts transfer, albeit in a real time manner.

2. In this model the transaction completes (for the users only) as soon as the beneficiary's mobile device receives the amount and sends the details to Bank B. The interbanking and associated confirmation of accounts need not happen in a real time manner. At the same time, the onus of maintaining the account of the remitter lies on the remitter's mobile

device. Thus, the transaction doesn't require a hard real time (instantaneous operations) action.

3. The debit model doesn't allow a mobile phone to behave a like a wallet whereas in the credit model, the mobile device acts like a wallet. Essentially, the temporary storage of e-cheques is in the form of a temporary storage of currency, which is being converted into the legally recognized currency by the banks. (The existence of an electronic currency has not yet been approved by RBI. Presently, RBI recognizes only Indian National Rupee as the legally recognized currency of India as the unit of financial transactions)

4. The Debit model can instantly detect any fraudulent transactions (such as transferring amounts from an account that's empty or is not authorized to transfer) by the virtue of its working model itself. However, the credit model, may, if at all, be susceptible to fraudulent transactions.

5. The debit model needs an all-time connectivity through the connectivity infrastructure whereas the credit model can work even if the connectivity infrastructure is intermittently live.

6. The credit model demands a completely tamper-proof mobile device that is capable of storing financial transaction details in a highly secured manner, without allowing anyone to modify the same at all, for theoretically an infinite amount of time, i.e., the data becomes static and non-modifiable. In the case of the debit model, the data need not be stored at all as it gets transmitted instantaneously across the banking network.

7. Apart from the major differences as mentioned above, there can be other differences in form of different legal implications and responsibilities of the stakeholders involved, role of encryption technology at the end user's end, nature of connectivity infrastructure being used, jurisdiction boundaries in case of any disputes, etc.

8. This model currently may present the mobile device of the remitter as a credit agency that is linked to the remitter's bank account as well. In other words, this model can also be explained as:

    a. The mobile device (or rather a specific application in the mobile device) behaves like a micro-credit agency, with one and only one debtor.
    b. The mobile device in turn, acts on the behalf of the bank in which the remitter has an account.
    c. For every transaction, the remitter directs the mobile device to transfer some amount to a beneficiary.
    d. The mobile device later on adjusts its accounts with the remitter's bank account.
    e. On the beneficiary's side, the mobile device acts like a deposit account that has one and only one depositor.
    f. The beneficiary's mobile device receives an amount from the remitter's mobile device and keeps a record of the same. (the record essentially contains at least the information about the remitter's bank account and the beneficiary's bank account)
    g. The mobile device adjusts the accounts with beneficiary's bank account as and when possible.
    h. Simply put the remitter's as well as the beneficiary's mobile devices behave like micro-banks themselves.
    i. Such an arrangement would require a highly secured mobile device that performs the above mentioned functions in an efficient manner. For the purpose of this report, such mobile device functionalities will together be referred to as "mobile-banks".

9. Mobile-banks functioning in this credit model are capable of any transaction, irrespective of the presence of a network. The mobile-bank may be run straight out of a modified SIM card, or any other device that is not directly accessible to the mobile phone user the way a phone memory is. In such a scenario, even the mobile phone will be able to access mobile-bank facilities in a restricted manner. For security reasons, the mobile bank

facility may have a hardware control in addition to the two-factor authentication for every session.

10. This model poses a lot of regulatory challenges as the complete onus of financial transaction falls on the device itself, and demands a high level of cooperation and unbiased support from the hardware/device manufacturer. To draw parallels with current RBI regulations, each of the mobile-banks is equivalent of a Business Correspondent (BC) [10] as defined by RBI. However, it is not a BC as it is not any of the entities who/which are allowed to assume the role of a BC.

11. At the same time, this method creates a device/system that takes the concept of banking to a whole new level wherein the entire concept of branchless banking transforms into mobile-device functionality.

12. With appropriate regulatory system in place and a secured environment, this model may be aptly modified and applied in regions still lacking always-on network connectivity. However, it will require a lot of standardization across hardware designs, network operations and above all, banking facilities (which are standardized to a great extent in India with the advent of Core banking Solutions) [11].

These two largely contrasting models in terms of nature of responsibilities of mobile devices have very similar security requirements (albeit with different intensities) which are explained in further sections.

RBI recommended technology system

For the purpose of this report, the role of technology will be explored at least to satisfy all the operational guidelines as published by RBI [12]. In order to briefly capture those guidelines so as to clearly reflect the role of technology, a description (illustrative but not comprehensive) of the same follows (reworded for the purpose of this report, with the addition of opinions of the authors of the report):

1. User Authentication
    a. At least two-factor authentication is required wherein; both the authentications of the user are not compromised at the same time. For example, if one of the authentication is in the form of a login username-password defined by the user, the other factor of authentication can be mPIN (a uniquely generated PIN decided by the bank for every transaction) provided by the Bank through a secured means like a encrypted number generator as used by banks like HSBC (refer Exhibit 1 for an example), SMS or IVRS channel.

    b. Currently, IVRS is more preferred as the communication of the secured PIN via IVRS is complete only when a human ear listens to it and responds appropriately. Also, IVRS is more securely transmitted from the bank to the user across the network as compared to SMS (or even Secured SMS as proposed in various forums). The encrypted number generator, though the most secured means, is not a portable and user friendly device as the user will always have to carry this device and the mobile device with her. These two devices can't even be combined as it will defeat the entire purpose of two-factor authentication itself.

    c. RBI encourages usage of higher level of authentication. (However, nowhere in the guidelines does the user level comfort is considered as RBI's prime requirement is to assure secured transactions).

d. One such mode of authentication can be the use of a fingerprint recognition/Iris recognition (database for the same can be based on the one created by Aadhar, UIDAI [13] system for India). This will help less educated people to avail the benefits of m-commerce.

e. However, this method is highly dependent on the hardware used in Mobile phones and will require a lot of standardization on the manufacturer's part to adhere to the norms specified by the UIDAI authority. At the same time, such a confirmation will only be a partial replacement to login name-password technique as the user himself/herself has to be pre-registered with the bank under KYC [7] norms.

2. Encryption to ensure confidentiality, integrity, non-repudiation and authenticity

   a. As shown in the diagram in the previous section, the data for the m-commerce transactions is flowing at least through 7 independent entities. Therefore there are several occasions during which the data can be manipulated, siphoned, phished, corrupted or rendered unclaimed-able for the sender. Even within the operations of individual entities, the data flow is open to such malpractices. Hence, there's a need to ensure the following:

      i. Secured Data encryption during transfer from mobile device to the Telco/BWA/MVNO infrastructure such that data integrity and secrecy is maintained during this entire transaction.

      ii. Prevention of intrusion by implementing Network Intrusion Prevention Systems (NIPS) across the passive telecomm network such that neither it is possible for anyone to capture/decrypt/modify/encrypt the data nor to prevent the flow of data across the infrastructure till it reaches the first level bank.

      iii. Assuming that NPCI is capable of providing a secured transaction across its network of banks.

b. It is essential to maintain proper digital signatures across transactions to avoid any fraudulent claims by remitters about foul-play transactions (non-repudiation)

3. Uniformity of data formats
    a. Since there are multiple entities involved in the data flow, there needs be a strict adherence to universal data format. It is not advisable to process and transform the data (excluding encapsulation) by each entity as it may lead to breach of data integrity or confidentiality. The universal data format may have the following characteristics:
        i. Uniform data format capable of being transported in both wireless and wired domain (may be using encapsulation, though not preferred), in such a manner that data can be securely transmitted from the user to the bank, without any additional security requirement across the MNO or internet channels
        ii. Easy and secured encryption/decryption, such that the encryption technology is hardware agnostic at the least
        iii. Open protocol design (not proprietary)
        iv. Agnostic to the mobile hardware
        v. Portable across any mobile phone OS ideally
        vi. Agnostic to the underlying Telecomm operator/BWA operator/MVNO operator

4. Adherence to the Information Technology Act, 2000, India [14]: Since this system is being identified keeping in mind the Indian regulations, it is essential that the IT Act of India is duly adhered to, especially in terms of encryption. Moreover, it is assumed that the entire system doesn't compromise any other law in India, at least by design.

Stakeholder's Analysis

In order to understand either of the models (credit model and debit model), the report will first assess individual entities in each model so as to determine their role in the m-commerce ecosystem.

The mobile Device User

For the purpose of this report, the role of mobile device user will be analyzed from the point of view of a remitter/beneficiary in a payment transaction with a recognized (recognized by RBI as a legal recipient/sender) third party and the associated scope of activities. The various m-banking practices that are more of an information transfer between the bank and the user will not be emphasized upon, unless directly involved in the process of the transaction. Also, activities in which the user is making a payment/receiving a payment to/from the home bank (the bank in which the user has an account) or the foreign bank (any other nationalized bank that holds a banking license) will not be considered.

Needs and Usage

1. Payments
    a. Remittance of amount for a real time purchase. E.g. shopping an article from a retail outlet, buying vegetables from the grocery store, tea from a road side tea vendor, purchase from a tourist spot seller, etc
        i. Ideal real time transaction would relate to an instantaneous, zero delay in the transfer of relevant amounts
        ii. Ideal universality of payments would relate to being able to make payments to each and every legal entity with an MMID as far as the scope of this report is concerned

b. Transfer of amounts from the user to another individual person, whether in person or remotely
    i. Ideal situation would be a transfer to any person associated with an MMID

c. Payments towards bills, insurance amounts, etc (especially for concepts like micro insurances, toll charge bills, local transport tickets and other such services)
    i. Ideal situation would be to automatically, periodically complete these payments on a single click of a button
    ii. Ideal payment process would be consolidation of all such bills in a single list with minimum views required to get into the details

d. Payment towards digital purchases like ticket (travelling, movies) booking, music download, e-book downloads, OTA (over the air) installations, etc

2. Receipts
    a. Receipts towards any sale (authorized by RBI) of an object, service, etc (such as reception of an amount by a porter on a railway station)
        i. Ideal situation would be to complete these transactions for any amount
        ii. Ideal situation would be to complete them in real time, instantaneously

    b. Receipt of cash in lieu of a cash-coupon or similar activities
        i. Ideal situation would not require any physical cash to be involved and all transactions would be done through electronic means

    c. Receipts of any other monetary amount from a legitimate source that may be directed to a dedicated bank account associated or alien to the user's mobile payment identity

3. Costs
    a. Minimum fee for availing m-commerce services

    b. Uniform fee structure across any bank, any MNO or any device as far as m-commerce activities are concerned

    c. Minimum/negligible fee per transaction

4. Quality of Service requirements
    a. Instantaneous, 24x7 operation

    b. Ability to transact seamlessly whether in roaming or home network

    c. To reiterate again and again just to emphasize, complete confidentiality, privacy and security for every transaction attempted, and guarantee that every such transaction completes in an expected fashion

Threats, Risks and Difficulties

1. Monetary loss due to
    a. Incomplete or faultily registered transactions wherein, transaction details either don't reach the correct recipient or reach the wrong recipient. Possible means are
        i. Compromised or non-functional mobile device
        ii. Non-unique MMIDs
        iii. Modification of MMIDs and other authentication details during data transfer
        iv. Modification of transaction details while being translated from one protocol into other during the process of transmission from the mobile device to the banks

b. fraudulent transactions by means of
    i. identity theft
    ii. identity duplication or identity masquerading (permanent and/or temporary), at any point of m-commerce transaction (e.g. via BSS)
    iii. unsolicited transfer of amounts during a legitimate payment/receipt transaction
    iv. multiple transactions during a session authorized for only a single transaction
    v. any other means of transfer of monetary amounts unauthorized by the user and/or the associated mobile banking account's administrator bank

2. Unauthorized (or illegal as per governing law) archiving of the transactions (current and/or past)

3. Unauthorized (or illegal as per the governing law) eavesdropping over the transactions (current and/or past)

4. Difficulty in initiating/sustaining/completing any transaction/information update/notifications pertaining to m-commerce due to
    a. any delays/interruptions/network unavailability/service denial or any other technology related event

    b. administrative issues regarding user's rights over the transaction as recognized by the associated bank/infrastructure provider/IMPS/RBI

    c. any other such issue within the ambit of the governing law

5. Difficulty in using m-commerce due to mobile device restrictions (uncomfortable with the device itself) or with the user interface system being used

6. Inconvenience with the design of the entire m-commerce system

The Telecom Infrastructure

For the purpose of this report, it will be assumed that

1. The Mobile Network Operators (MNO's) are solely responsible for providing the connectivity from a mobile device to a bank

2. The MNO's are only those entities which have been given the license by TRAI for using spectrum to provide GSM, CDMA, 3G, 4G, LTE or BWA based services and are recognized by TRAI as the legal users of this spectrum license

3. The MNO's are providing a complete path for the data to flow from a mobile device to the bank, and may or may not be responsible for aggregating this data internally or through out-sourcing to a third party IT service provider.

4. The MNO's infrastructure services will be available for such a commercial use only if it is allowed by (in the descending order of authority)

    a. TRAI
    b. RBI

Role and responsibilities

The MNO's use the following model to allow transmission of data across the network

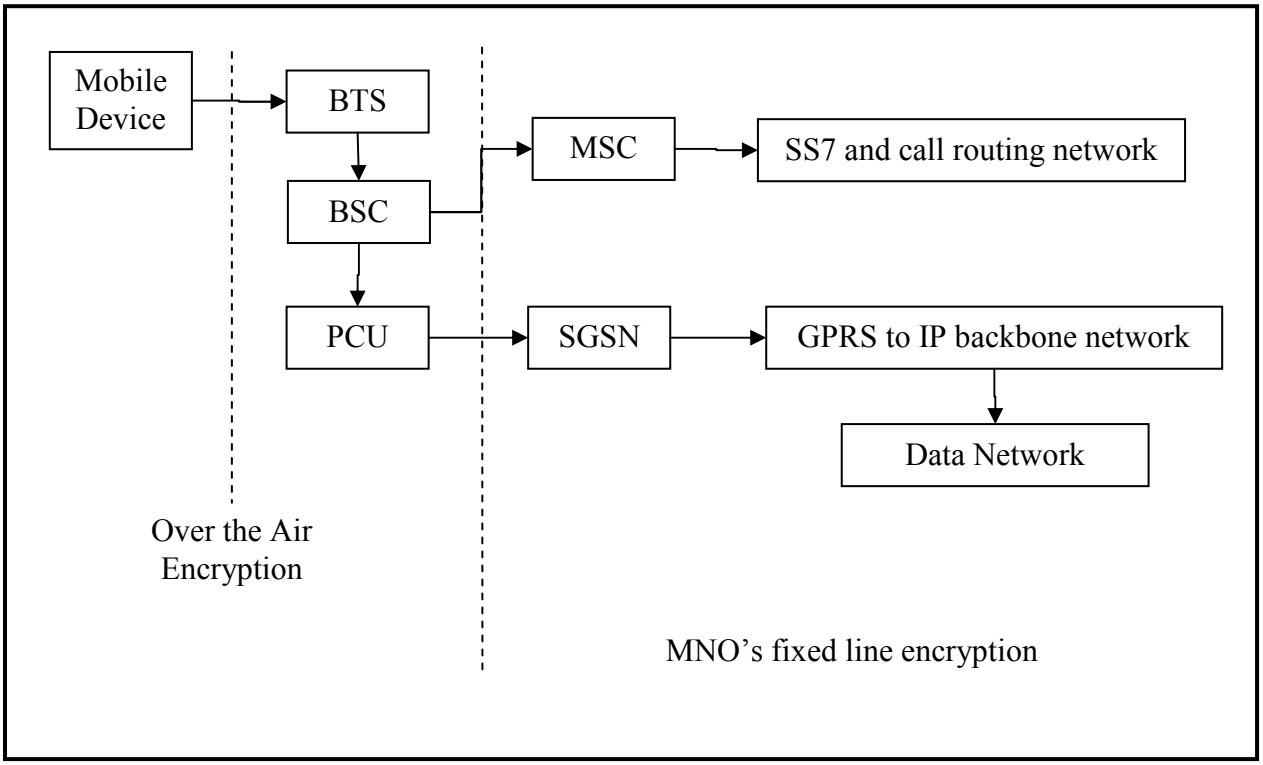


Fig: Flow of data in a GSM network [15] *(only a representative model to assess the security involved in the flow of data)*

Data flow:

1. The data from Mobile device flows to the Base Transceiver Station (BTS) over the air. This data transfer is encrypted using A5 algorithm.
2. Data flows from BTS to Base Station Controller (BSC) over operator's fixed line network or through microwave transmission.
3. The data packets flow through a Packet Control Unit (PCU) whereas the voice is carried over to Mobile Switching Center (MSC) to SS7 Protocol and other call routing protocol handlers.
4. The data packets continue to flow through the fixed lines to SGSN (Serving GPRS Support node) to GPRS management devices where the data is converted into IP suitable formats and hereafter, the data is carried over in IP format in a Data Network.

Key roles:

1. An MNO is responsible for ensuring that any data leaving from a mobile device reaches the associated bank servers without any security issues.

2. MNO is also responsible to ensure security over the air as well through its physical network. Therefore, no external entity should be able to access the m-commerce data being transferred in an unauthorized manner.

3. The MNO itself is not able to access the data reaching the bank, unless it is acting as a BC for the bank and hence, authorized to access the data.

4. It is important to realize that over the air security provided through A5 algorithm can be compromised and the data can be captured there itself. Also, since the data travels like a plaintext data over the physical network of the MNO, it can easily be tapped into during this entire process. Nonetheless, it will be most desirable if the data leaving the mobile device itself is encrypted independent of the MNO and can be decrypted only by the bank. Such a manner of data transfer would essentially be termed as end to end secured data transfer.

Contribution

The MNO can play a passive role in the m-commerce system by providing only the infrastructure and leave the role of a payment service to either the bank or a third party. Alternatively, the MNO can itself act as a payment service by acting as a BC. For the purpose of this report, all such payment service providers will be termed as Mobile Payment Service Providers (as denoted in the MPFI's documentations) or MPSP. The contribution of an MPSP will be as follows:

1. Maintaining full details of each and every transaction for both the banks as well as the mobile device users
2. Enabling the mobile device with suitable applications/programs/services so as to be able to use m-commerce

3. Maintaining such services independent of the bank
4. Ensuring end to end encryption of data when it flows between the bank and the mobile device
5. Providing customer services
6. Allowing the banks to concentrate only on the payment settlements and payment authorization
7. Bringing together different remitters and beneficiaries under a single roof for seamless transactions and usage of m-commerce

Benefits

Following are the benefits as perceived by an MNO:

1. Leveraging the data transfer capabilities towards revenue generation via an increase in the data flow across its network for the purpose of m-commerce

2. Increase in the revenue via addition of more customers to the customer base who want to avail m-commerce services

3. Leveraging the widespread distribution system for the purpose of providing additional banking facilities other than those accessible via m-commerce services and hence generate additional revenue

Besides these revenue sources, an MNO can earn through providing access to its customer base to various retailers. In short, an MNO can leverage its customer base, distribution system and mobility of data capabilities to earn revenue.

4.

The Banking Institution

The banking institutions perform the function of facilitating m-commerce transactions, validation each and every individual transaction, archiving the transactions and at the least, complete banking customer level traceability for every transaction (capabilities of tracing back a transaction to the remitter and/or the beneficiary along with every node through which the transaction has taken place), and avoid any administrative fraudulent activities. Following are some of the characteristics of this entity vis-à-vis m-commerce.

Needs

1. A bank needs to extend its banking facilities at the minimum possible operation/capital expenditure. It needs to increase its reach-ability across geographies and across time (i.e. - independent of the time of the day). This issue can partly be resolved by automating the banking operations as much as possible and at the same time, using a channel that's wide spread. A mobile device based system fits into both these criteria.

2. A bank needs to increase the total profit generated per transaction as performed by each of its customers as these transactions also form a major source of its revenue other than lending activities. This can be achieved by easing the process of transaction to the customer and making each transaction as less costly as possible for the customer. This again can be achieved using a mobile phone which not only provides mobility and hence reduced transportation cost to reach a bank branch for the customer, but also a means to have a very low ratio of transaction cost to transaction value.

3. The banks incur a significant cost in handling the physical cash assets (currency notes, coins, etc). In an ideal environment, a bank would like to completely do way with physical currency. By using more and more electronic devices, including mobile devices, banks can reduce the currency based operations and thus save expenses.

4. The banks need to retain customer loyalty to increase its account holders' quantity.

Requirements

1. One of the prime concerns for a bank is the security of the transactions it is facilitating through a mobile device. In an ideal situation, only the mobile device and the associated bank should be able to process the data transacting between them.

2. A bank would prefer to have communicate with the mobile device agnostic to the underlying MNO‘s infrastructure. Ideally, the entire communication channel between a bank and a mobile device should appear like a single line irrespective of the various technologies present midway.

3. A bank would require high level of customer service to ensure customer loyalty. It would ideally want full visibility of the data being transferred between it and the remitter, beneficiary and the beneficiary’s bank; and vice versa, minus the authentication details. This will ensure an ease of traceability across the entire cycle.

Roles and Responsibilities

General duties

1. The bank will be responsible for distributing the MMID’s across the nation.
2. The bank would have to ensure that each of MMID’s are issued only to those users who have adhered to KYC norms and are duly verified to be fit for m-commerce, and essentially for m-banking
3. The bank will be responsible for mapping the MMID’s to the user’s account and vice versa.
4. The bank will be responsible for monitoring the credit ratings of the users, especially in case of those involved with the earlier proposed credit model.

Remitter Specific

1. The bank is responsible for monitoring the credit limits of the remitter and the balance sheet of the remitter.

2. The bank will be responsible for authorizing a remitter for the transaction and maintaining that authorization and validating the same throughout the transaction.
3. It's the bank's duty to adhere to RBI's norms about number of transactions a day, value of each transaction and nature of the transaction before allowing a remitter to initiate a transaction.
4. The bank is also expected to manage all its customers simultaneously, without any error from its systems.
5. It's the bank's utmost responsibility to prevent any money laundering activity by facilitating perfect traceability for every transaction.
6. It's the bank's duty to complete a transaction such that money is transferred from the correct account, to the correct account, in the correct amount and within the preset time limit.
7. It's the bank's duty to communicate with the beneficiary's bank through NPCI under all circumstances and maintain perfect transparency for all transactions
8. A bank is responsible to maintain and share all accounting logs with the remitter and generate real time alert by whatever means possible if it detects any fraudulent transactions. In the first place, a bank must prevent any fraudulent activity.

Beneficiary Specific

1. The beneficiary's bank is responsible to accept and transfer all the receipt amounts to the relevant account as soon as possible and notify the beneficiary about the same.
2. The beneficiary's bank must inform the remitter's bank about receipt of the amount.
3. In case the beneficiary's bank identifies that a transaction is against the rules laid down by RBI, it must decline the transaction and notify the remitter's bank about the same.
4. The beneficiary's bank is also responsible for ensuring all the limitations pertaining to a transaction as decided by RBI.
5. It is also responsible for preventing any money laundering activities.
6. It should be able to service all of its consumers at the same time and in real time manner.
7. It should archive all the transactions and maintain perfect transparency with the remitter's bank as well the concerned authorities.
8. It is required to inform the beneficiary about any updates with her bank account.

The Government Agencies

The government agencies involved in the proposed (and only suggestive, not probable) models in the previous sections are mainly restricted towards policy formulation and monitoring the operations of the entire system. As such, RBI and by RBI's mandate – NPCI fall into this category along with TRAI, with a certain responsibility from the point of view of the telecom service providers (i.e., referred to as the operational service providers in the text). **Besides the responsibilities of these institutions as already listed in their respective mandate, additional roles and responsibilities with respect to m-commerce only, are explored below**. They are only suggestive and may or may not relate to all the possible cases.

Roles and Responsibilities

1. To provide an equally competitive environment to all the participating private players in the banking or infrastructure role
2. To design a system that above all, provides a fluid means of transfer of monetary amounts and/or associated information for the purpose of m-commerce in a real time manner
3. To design a system completely agnostic to any participating player in any role (banking and/or infrastructure services), homogenous to any technology, whether current or useful, that may be decided upon by the entities directly using those technologies and no other apparent benefactor
4. To design a system where any and every monetary transaction is traceable to
    a. The recipient
    b. The recipient's bank
    c. The sender
    d. The sender's bank
    e. Any infrastructural node (passive or active) involved in the entire system
5. To provide an electronic currency system that is transferable to and transferable from INR (physical form) and any other recognized international currency. (Such an electronic currency denomination may ease the processing of transactions at the user level itself and may not require the presence of a bank for any small transaction)

Possible risks to look out for

1. Money laundering operations across national/international border using the mobile devices, via any system whether or not recognized as m-commerce
2. Illegal access to the system by entities that may indulge in fraudulent activities by means of hacking (or by exploiting legal/technological loopholes within the system)
3. Customer grievances not being addressed by the banks/customers being discriminated on the basis of their choices of infrastructure operator/types of transactions/amount of transactions
4. Monopoly of a single entity in any of the stake-holding position by virtue of its assets (such as a telecom operator leveraging its telecom licenses to usurp competition in various circles)

The Road Ahead

So far, the models used for m-commerce across various nations (models like Airtel Semi wallet, Bank of Ethen's Wizzit services in South Africa, m-Pesa in Kenya, etc) are essentially debit systems which transfer money from one account to another in real time. Such systems have flourished due to supports by regulatory bodies across various nations who were very skeptical about using credit model in the m-commerce system. However, with the advent of highly secured SIM tool kits, Near Field Communication (NFC) [(16)] systems and real time network transmissions; there's a possibility that a mobile device may assume the role of a bank's branch and perform the credit/debit services independently of the bank itself.

Another possibility would be the presence of a complete debit model wherein, the MNO's serve the role of an MPSP, bank and IMPS if the regulations allow such a scenario.

Nonetheless, the RBI's push to promote m-banking for financial inclusion, and thus inherently m-commerce; MNO's push to mobile services in financial transactions to leverage their data services and the user's desire to simplify all the operations into a single click on a mobile device will be the key drivers that will decide the future of how fast m-commerce can spread across the masses. There will always be an inherent need to ensure a secured and fraud-proof environment and it will be possible only when all the stakeholders come together with this common purpose.

Bibliography

1. **Chillibreeze Solutions Pvt. Ltd.** Mobile Commerce in India - An Overview. *India Reports: Reports and PPTs on India and Indian Business.* [Online] 2010. [Cited: October 18, 2010.] http://india-reports.in/internet-advantage/mobile-commerce-in-india-%E2%80%93-an-overview/.

2. **COAI.** *COAI :: Cellular Operators Association of India.* [Online] January 2011. [Cited: January 22, 2011.] http://coai.com/Sub%20Figs/GSM%202011/All%20india%20GSM%20sub%20figures%20Jan%202011.xls.

3. **TRAI.** Press Release: Telecom Subscription Data as on 31st December 2010. *Telecom Regulatory Authority of India.* [Online] February 9, 2011. [Cited: February 10, 2011.] http://www.trai.gov.in/WriteReadData/trai/upload/PressReleases/798/prerdiv9feb11.pdf.

4. **India News Top Info.** India Listed; Blog Archive; Airtel Mobile Payment Service Airtel Money: India's first Mobile Payment Service Prepaid Cash On Mobile launched 2011 Charges, Transaction Limits. [Online] february 1, 2011. [Cited: February 22, 2011.] http://indialist.0fees.net/airtel-mobile-payment-service-airtel-money-indias-first-mobile-payment-service-prepaid-cash-on-mobile-launched-2011-charges-transaction-limits/.

5. **Economic Times.** India Slowly gets to grip with e-commerce. *The Economic Times.* [Online] May 16, 2010. [Cited: 02 06, 2011.] http://economictimes.indiatimes.com/infotech/internet/India-slowly-gets-to-grips-with-e-commerce/articleshow/5936822.cms.

6. **Reserve Bank of India.** Mobile Payment in India - Operative Guidelines for Banks. *Reserve Bank of India.* [Online] 2010. [Cited: October 17, 2010.] http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365.

7. —. Know Your Customer (KYC) norms. *Reserve Bank of India.* [Online] June 30, 2009. [Cited: February 12, 2011.] http://rbidocs.rbi.org.in/rdocs/notification/PDFs/MCKYCC010709.pdf.

8. **National Payments Corporation of India.** National Payments Corporation of India. [Online] November 22, 2010. [Cited: February 05, 2011.] http://www.npci.org.in/aboutimps.aspx.

9. **Zee Biz News.** Mobile Money. *Latest Business News - Indian Stock Market, Sensex News, Nifty, BSE, Financial Advice: Zee Business.* [Online] February 6, 2011. [Cited: February 7, 2011.] http://biz.zeenews.com/interviews/story.aspx?newsid=259.

10. **Reserve Bank of India.** Reserve Bank of India. *Reserve Bank of India.* [Online] January 25, 2006. [Cited: February 22, 2011.] http://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=2718.

11. **Reserve bank of India.** RBI DOCS. [Online] June 2007. [Cited: February 22, 2011.] http://rbidocs.rbi.org.in/rdocs/Content/PDFs/80799.pdf.

12. **Reserve Bank of India.** Mobile Payment in India - Operative Guidelines for Banks. *Reserve Bank of India.* [Online] 2008. [Cited: February 07, 2011.] http://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=1365.

13. **UIDAI.** Unique Identification Authority of India. *UIDAI.* [Online] 2011. [Cited: February 6, 2011.] http://uidai.gov.in/.

14. **Ministry of Law, Justice and Company Affairs.** IT Bill 2000. [Online] 2000. [Cited: February 6, 2011.] http://cbi.nic.in/cybercrime/itbill2000.pdf.

15. **why telecom.com.** why telecom.com. *Hacking a GSM Mobile Fone - GSM HACKER | WhyTelecom.* [Online] [Cited: February 22, 2011.] http://whytelecom.com/content/hacking-gsm-mobile-fone-gsm-hacker.

16. **Cyber Media.** NFC Is To Be. *Voice&Data Online - Resource Center on Indian Telecom.* [Online] CIOL Networks, February 22, 2011. [Cited: February 22, 2011.] http://voicendata.ciol.com/content/news/111022201.asp.

17. **ICICI Bank.** ICICI Bank - iMobile. *Personal Banking | NRI Banking | Corporate and Business Banking | Rural Banking | ICICI Bank.* [Online] October 17, 2010. [Cited: October 17, 2010.] http://www.icicibank.com/campaigns/imobile/newuser.html.

18. Mobile Banking, Mobile Banking Services, Mobile Banking in India, Bank Mobile Banking - Citibank India. *Credit Card, Loans, Investments, Insurance, NRI and Online Banking Services | Citibank India.* [Online] 2010. [Cited: October 17, 2010.] http://www.online.citibank.co.in/products-services/online-services/citi-mobile.htm?eOfferCode=INHWAIMB.

19. **HDFC Bank.** Mobile Banking India | HDFC Bank - Mobile Banking Application, Mobile Banking Service. *HDFC Bank: Personal Banking Services.* [Online] 2010. [Cited: October 17, 2010.] http://www.hdfcbank.com/personal/access/mobilebanking/overview.htm.
20. **SBI.** STATE BANK OF INDIA :: INDIA's LARGEST BANK. *STATE BANK OF INDIA :: INDIA's LARGEST BANK.* [Online] 2010. [Cited: October 17, 2010.] http://www.statebankofindia.com/user.htm?action=viewsection&lang=0&id=0,1,21,691.
21. **Bharti Airtel.** M-Commerce - Mobile Commerce, Pay Bill Online, Book Tickets Online with Airtel. *Airtel India – Mobile Prepaid, Postpaid, DTH Services, Broadband Services.* [Online] 2010. [Cited: October 17, 2010.] http://www.airtel.in/m-commerce.
22. **Vodafone India.** Mobile Banking Services | Vodafone India. *Vodafone Gujarat - Prepaid | Postpaid | Caller Tunes | Vodafone Mobile Services.* [Online] 2010. [Cited: October 17, 2010.] http://www.vodafone.in/existingusers/services/pages/mobilebanking.aspx.
23. **ngpay.** Welcome to ngpay - India's Largest Mall on Mobile. *Welcome to ngpay - India's Largest Mall on Mobile.* [Online] 2010. [Cited: October 17, 2010.] http://www.ngpay.com/site/faqs.html.
24. **Empays Payment Systems India Pvt Ltd.** How It Works. *IMT is Instant Money Transfer.* [Online] 2010. [Cited: October 17, 2010.] http://www.empays.com/hows_work.php.
25. **Guha-Khasnobis, Rajeev Ahuja and Basudeb.** WORKING PAPER. *MICRO-INSURANCE IN INDIA:TRENDS AND STRATEGIES FOR FURTHER EXTENSION.* New Delhi, India : INDIAN COUNCIL FOR RESEARCH ON INTERNATIONAL ECONOMIC RELATIONS, June 2005.
26. **Thakkar, Pooja.** Mobile Banking in India - Business Review India. *Indian Business Magazine: Business News, Finance News Headlines, India Stock News - News and Information for Indian Business Executives.* [Online] August 20, 2010. [Cited: October 17, 2010.] http://www.businessreviewindia.in/blogs/economics/mobile-banking-india.
27. **Banzal, Sanjiv.** *World Wide Web Foundation.* [Online] 2010. [Cited: October 18, 2010.] http://public.webfoundation.org/2010/04/trai_compendium/25.Mobile_banking_M-commerce_15.03.pdf.
28. **Oxigen.** Oxicash Wallet | Mobile Recharge | TV Recharge | Rail Air Bus Movie Tickets | Bills | Toll Tax payments. *Oxicash Wallet | Mobile Recharge | TV Recharge | Rail Air Bus Movie Tickets | Bills | Toll Tax payments.* [Online] 2010. [Cited: October 18, 2010.] http://oxicash.in/.

29. **National Payments Corporation of India.** *National Payments Corporation of India.* [Online] 2010. [Cited: February 6, 2011.] http://www.npci.org.in/bankmember.aspx.

30. **Karnouskos.** IEEE Communications Society. *IEEE Communications Surveys and Tutorials.* [Online] 2004. [Cited: February 6, 2011.] http://www.comsoc.org/livepubs/surveys/public/2004/oct/pdf/KARNOUSKOS.pdf.

31. **Raju, Prabu, et al.** *Analysis of Mobile Infrastructure for Secure Mobile Payments.* India : Mobile Payments Forum, 2008.

32. **Bankable Frontier Associates LLC.** MANAGING THE RISK OF MOBILE BANKING TECHNOLOGIES. [Online] March 24, 2008. BFA-080324.

33. **ISO.** ISO 8583-1:2003. *International Standards for Business, Government and Society.* [Online] International Organization for Standardization, October 21, 2008. [Cited: February 12, 2011.] http://www.iso.org/iso/catalogue_detail.htm?csnumber=31628.