Mobile Banking

Mobile banking is a system that allows customers of a financial institution to conduct a number of financial transactions through a mobile device such as a mobile phone or personal digital assistant.

FEATURES & BENEFITS OF MOBILE BANKING

a) **Simplicity :** The m-payment application must be user friendly with little or no learning curve to the customer. The customer must also be able to personalize the application to suit his or her convenience.

b) **Universality:** M-payments service must provide for transactions between one customer to another customer (C2C), or from a business to a customer (B2C) or between businesses (B2B). The coverage should include domestic, regional and global environments. Payments must be possible in terms of both low value micro-payments and high value macro payments.

c) **Security, Privacy and Trust:** A customer must be able to trust a mobile payment application provider that his or her credit or debit card information may not be misused. Secondly, when these transactions become recorded customer privacy should not be lost in the sense that the credit histories and spending patterns of the customer should not be openly available for public scrutiny. Mobile payments have to be as anonymous as cash transactions. Third, the system should be foolproof, resistant to attacks from hackers and terrorists. This may be provided using public key infrastructure security, biometrics and passwords integrated into the mobile payment solution architectures.

d) **Cost:** The m-payments should not be costlier than existing payment mechanisms to the extent possible. A m-payment solution should compete with other modes of payment in terms of cost and convenience.

e) **Speed:** The speed at which m-payments are executed must be acceptable to customers and merchants.

f) **Cross border payments:** To become widely accepted the m-payment application must be available globally, word-wide.

Advantages :

A very effective way of improving customer service could be to inform customers better. Credit card fraud is one such area. A bank could, through the use of mobile technology, inform owners each time purchases above a certain value have been made on their card. This way the owner is always informed when their card is used, and how much money was taken for each transaction.

Similarly, the bank could remind customers of outstanding loan repayment dates, dates for the payment of monthly installments or simply tell them that a bill has been presented and is up for payment. The customers can then check their balance on the phone and authorize the required amounts for payment.

The customers can also request for additional information. They can automatically view deposits and withdrawals as they occur and also pre- schedule payments to be made or cheques to be issued. Similarly, one could also request for services like stop cheque or issue of a cheque book over one's mobile phone.

There are number of reasons that should persuade banks in favor of mobile phones. They are set to become a crucial part of the total banking services experience for the customers. Also, they have the potential to bring down costs for the bank itself.

Through mobile messaging and other such interfaces, banks provide value added services to the customer at marginal costs.

Yet another benefit is the anywhere/anytime characteristics of mobile services. A mobile is almost always with the customer. As such it can be used over a vast geographical area. The customer does not have to visit the bank ATM or a branch to avail of the bank's services. Research indicates that the number of footfalls at a bank's branch has fallen down drastically after the installation of ATMs. As such with mobile services, a bank will need to hire even less employees as people will no longer need to visit bank branches apart from certain occasions. With Indian telecom operators working on offering services like money transaction over a mobile, it may soon be possible for a bank to offer phone

based credit systems. This will make credit cards redundant and also aid in checking credit card fraud apart from offering enhanced customer convenience.

The use of mobile technologies is thus a win-win proposition for both the banks and the bank's customers. The banks add to this personalized communication through the process of automation. For instance, if the customer asks for his account or card balance after conducting a transaction, the installed software can send him an automated reply informing of the same. These automated replies thus save the bank the need to hire additional employees for servicing customer needs.

Challenges for a mobile banking:

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) provide 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.

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 wireless network :

1. Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
2. 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 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 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 by the customer.

One-time password (OTPs) are 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 is expired once it has been used or once its scheduled life-cycle has expired.

Reliability

Another challenge for the banks is to scale-up the mobile banking infrastructure to handle 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 from 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 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.

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

Electronic Data Interchange

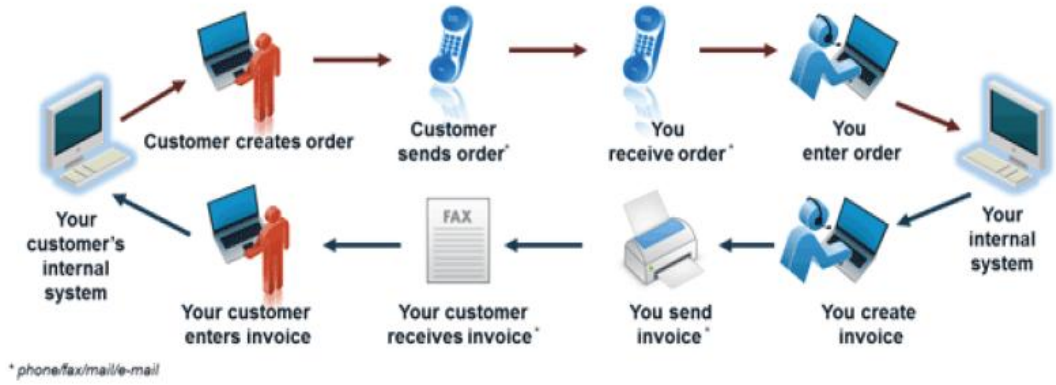
Electronic Data Interchange (EDI) is the *computer-to-computer* exchange of *business documents* in a *standard electronic format* between *business partners*.

By moving from a paper-based exchange of business document to one that is electronic, businesses enjoy major benefits such as reduced cost, increased processing speed, reduced errors and improved relationships with business partners.

Significance of each term:

Computer-to-computer– EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers. Having people involved slows down the processing of the documents and also introduces errors. Instead, EDI documents can f low straight through to the appropriate application on the receiver's computer (e.g. the Order Management System) and processing can begin immediately.

A typical manual process looks like this, with lots of paper and people involvement:



The EDI process looks like this – no paper, no people involved:

Business documents – These are any of the documents that are typically exchanged between businesses. The most common documents exchanged via EDI are purchase orders, invoices and Advance Ship Notices. But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents.

Standard format– Because EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents. A standard format describes what each piece of information is and in what format (e.g. integer, decimal, mmddyy). Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn't understand Japanese, the receiver's computer system doesn't understand the company-specific format of the sender's format. There are several EDI standards in use today, including ANSI, EDIFACT, TRADACOMS and XML. And, for each standard there are many different versions, e.g. ANSI 5010 or EDIFACT version D12, Release A. When two businesses decide to exchange EDI documents, they must agree on the specific EDI standard and version.

Businesses typically use an EDI translator – either as in-house software or via an EDI service provider – to translate the EDI format so the data can be used by their internal applications and thus enable straight through processing of documents.

Business partners – The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company B. Company A and Company B are business partners.