Managing Information Security Using New Mobile Banking Data Security Standard [MBDSS] Framework

Sudhakara
University of Mysore Computer Center,
Manasagangothri, Mysore-570 006
Email: sudhakara_am@yahoo.com

ABSTRACT

In this world of computer and communication, 60.6% of world populations are having mobile phones. With the rise in popularity of 3G mobile phones, banks has already started offering their facilities anywhere as user can get a phone signal irrespective of geographical location. Several countries are offering faster 4G Mobiles. Due to faster and reliable mobile phones, the users wants to use their mobile as all-in-one device with basic communication service along with entertainment and banking services. As far as the evolution of offerings and technology, one can see the future as an organic integration of mobile banking capabilities and channels that bring customers everything they could want or need to satisfy all their banking function from their mobile handset. Mobile phone is the first channel that allows a bank to proactively, economically and in a timely fashion reach out to customers, rather than relying on customers to initiate an online session, call, branch or ATM visit. This is a huge advantage that delivers customers more personal and timely information about their finances as well as exposure to new and relevant bank products.

Through the proactive communications channel Mobile banking also enables the bank to develop a deeper relationship with their customers. Unlike any other channel mobile banking allows you to have complete control and real-time understanding of personal finances. More and more bank customers are seeing these offerings as core to choosing and sticking with a financial institution. But due to lack of standards in mobile banking and security, the customers are reluctantly using mobile banking services offered by banks. To offer all the banking services- information based and transactions based services, security, confidentiality, integrity and non repudiation has to be bundled together, to facilitate the mobile users performing all the mobile banking services. This paper deals with the study of all information security standards and thus creating a framework for a highly secured and robust mobile banking standard in this world of computer and communications.

Keywords: Mobile banking, Security Standard, Information Security Standards, Mobile Banking architecture

INTRODUCTION

Mobile Banking has arrived. Banks are restructuring their infrastructure to adopt cost effective and faster mobile banking and extend all the possible financial services to its customer. Non banking people will be added to its database and hence can reach all the sections of the society. Mobile Banking presents an opportunity for banks to retain their existing, technology-savvy customer base by offering value-added, innovative services and to attract new customers from corresponding sections of the society . Due to new technology development and growth in telecommunications In India, the usage of mobile banking slowly catching up.

Many banks in India have come to regard Mobile Banking as a necessary tool to foster and retain an innovative image. This self-reinforcing dynamism is expected to gain currency in near-future so that Mobile Banking services could soon advance to a standard product – on the lines of Online Banking –

offered by more or less each and every bank.

As on December 2008, 60.6% of world population is using mobile phones. The % population mobile users in India (45%), China (56%), USA (89%) and UK (123%) and Russia (143%). These statistics throws the light on the potential and its usability in the world of banking where as of now the mobile are being used mainly for communication purpose. These mobile users also use their mobile for entertainment like playing music, seeing videos, taking pictures and storing their personal computer files for education too. Due to advent of new developments in information technology especially in data security few banks are contemplating to introduce all the financial services through mobiles and now they are offering selective financial services through mobile banking . This mobile banking is being offered in the banks all over the world. The customer apprehension about their data security and privacy, is the main hurdle in accepting this mobile banking. The customers are reluctant to use the mobile banking due to increase in financial frauds. The lack of security standards and use of not time-tested technology has a greater impact on mobile banking usage.

To remove apprehension about security, banks and service providers should come out with robust data security technology. The customers if convinced about data security and privacy of their transactions, one can surely expect exponential growth in the mobile banking in the world. Hence to build a robust security model one has to have standards in these security areas. Till date, no mobile banking standard exists in this banking sector for mobile banking operations. Unless there is security standard for financial transactions just like PCI-DSS for credit card and debit card transactions, due to increase in cyber frauds. the customers will hesitate to use their mobiles to do any financial transactions. The mobile banking standard has to be developed involving all the players in the financial transactions. As of now, the banks are offering only few transactions which are only information oriented and which does not require any robust security. These financial transactions are balance enquiry, accounting information, banks web services etc. Now these transactions are done based on the regulatory guidelines from central bank of the particular country. In building this mobile banking standard, various aspects of mobile banking, its operations, standards, security is briefly explained.

What is mobile Banking

"Mobile Banking is one of the banking services provided with the help of mobile telecommunication devices. The scope of offered services may include facilities to conduct bank and stock market transactions, to administer accounts and to access customized information.[9]

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. There is one more category which is based on the origin of transactions. If the customers wants information, he pulls the information from the bank for example balance enquiry. Banks sends/pushes certain information to its customers. It is called push technology for example Bill payment alerts.[10]

What is a standard?

The standard is a document with methods, processes, practices, is an agreed, repeatable way of doing something. [4]. It is a published document that contains a technical specification or other precise criteria designed to be used consistently as a rule, guideline, or definition. Standards help to make life simpler and to increase the reliability and the effectiveness of many goods and services we use.

Standards are created by bringing together the experience and expertise of all interested parties such as the producers, sellers, buyers, users and regulators of a particular material, product, process or service.

Standards are designed for voluntary use and do not impose any regulations. However, laws and regulations may refer to certain standards and make compliance with them compulsory. For example, the physical characteristics and format of credit cards is set out in standard number BS EN ISO/IEC 7810:1996. Adhering to this standard means that the cards can be used worldwide.

Any standard is a collective work. Committees of manufacturers, users, research organizations, government departments and consumers work together to draw up standards that evolve to meet the demands of society and technology.

What is information security?

Information security defines information as an asset, which adds value to an organization and consequently needs to be suitably protected [5]. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

INFORMATION SECURITY STANDARDS

" . . nearly 90% of those companies that had adopted BS 7799 said that formal certification had improved their business continuity; 85% said it had minimized damage from security incidents; and 53% said it had led to a higher return on investment said a report from Computer Weekly, May 2004."

This report tells us the importance of information security standards in this ever growing computerized information systems. As the technology developed, to have complete information security, more security standards were formulated. Several Security Standards were released from time to time to combat ever increasing cyber frauds globally. The complete list of different information security standards are as follows. [4]

- Basel II
- COBiT
- European Privacy Directive
- Gramm-Leach Bliley Act (GBLA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Financial Instruments and Exchange Law (JSOX)
- National Credit Union Administration (NCUA)
- Payment Application Data Security Standard (PA DSS)
- Payment Card Industry Data Security Standard (PCI DSS)
- Personal Information Protection and Electronic Documents (PIPEDA)
- U.S. State Breach Disclosure
- The ISO 27000 Series

Basel II

Basel II is the second of the Basel Accords, which are recommendations and regulations on banking laws issued by the Basel Committee on Banking Supervision. The intent of Basel II is to establish a set of regulations among large, internationally active banking organizations to protect against financial and operational risks specifically faced by the banking industry. Specific mention is made of operational risk and event loss types, including internal and external fraud from unauthorized activity, theft, and system security incidents, such as theft of information.

COBiT

COBiT is a framework that suggests an approach to Information Technology management with the objective of ensuring that the technology delivers the information that meet the business needs of the entity. COBiT is a business orientated framework that identifies 34 information technology processes, grouped in 4 domains, and is supported by 318 detailed control objectives. Each one of the 34 processes references IT resources, and the quality, fiduciary and security requirements for information. CobiT provides a generally applicable and accepted standard for good IT security and control practices to support management's needs in determining and monitoring the appropriate level of IT security and control for their organisations.

European Privacy Directive

This directive requires member countries of the European Union (EU) to adopt laws that protect personal information, and to disclose who is collecting the data and why, and who will ultimately have access to it. The directive also gives the person the right to access the data and make corrections to it. Countries affected by these regulations include Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden.

Gramm-Leach Bliley Act (GBLA)

The Gramm-Leach-Bliley Act, also known as the U.S. Financial Modernization Act, regulates the protection of consumer personal information held by financial institutions. The law provides consumers with limited control over how their personal data is used and shared by these institutions, and requires companies to establish safeguards that ensure the security and confidentiality of customer records.

Health Insurance Portability and Accountability Act (HIPAA)

The U.S. Health Insurance Portability and Accountability Act (HIPAA) mandates that all healthcare organizations comply with strict rules designed to protect the confidentiality and integrity of patient information. HIPAA requires entities to have safeguards in place to protect against any reasonably anticipated threats or hazards to the security, unauthorized use, or disclosure of the information, and sets severe civil and criminal penalties for non-compliance with these regulations.

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act (SOX) of 2002 regulates financial reporting and auditing of publicly traded companies. The law establishes strict requirements for reporting, disclosure, and internal controls, and defines penalties for non-compliance.

The SOX Act forms a new structure for corporate governance, establishing higher levels of fiscal accountability for U.S. businesses. Company officers could face criminal litigation and penalties if found in non-compliance.

Financial Instruments and Exchange Law (JSOX)

J-SOX, Japan's Financial Instruments and Exchange Law, is considered the Japanese version of Sarbanes-Oxley (SOX). The law introduces strict rules for the internal control of financial reporting in order to protect investors by improving the accuracy and reliability of corporate disclosures. Cost of non-compliance with J-SOX could involve criminal litigation, and penalties for company officers.

National Credit Union Administration (NCUA)

The National Credit Union Administration (NCUA) is an independent federal agency that requires U.S. federally-insured credit unions to establish a security program that addresses the privacy and protection of customer records and information. The NCUA mandates that credit unions must design and implement an information security program to control identified risks, commensurate with the sensitivity of the information. Among the considerations must be access controls on member information systems and encryption of electronic member information, including while in transit or in storage on networks or systems.

Payment Application Data Security Standard (PA DSS)

The Payment Application Data Security Standard (PA-DSS) is a subset of the Payment Card Industry Data Security Standard (PCI-DSS), which applies to software developers and integrators of payment applications that store, process, or transmit cardholder data as part of authorization and settlement. In order to ensure that all sensitive cardholder data is secure, PCI requires merchants, banks, and all other parties that decide to use a third-party application to select one that meets the PA-DSS standard.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) requires the protection of sensitive payment account data (such as primary account number (PAN), magnetic stripe data, CVV, and PIN) by any company that processes, stores, and transmits such data. The standard was developed by members of the PCI Security Standards Council, which includes VISA, MasterCard, and American Express, in response to increased credit card fraud. The focus of PCI DSS is the protection of sensitive cardholder account data that is collected and stored during credit card transactions. The standard consists of a core set of principles with 12 specific requirements for the protection of sensitive cardholder data in use, at rest, and in transit. One of the key challenges merchants, banks, and payment processors face is the implementation of data encryption to comply with the PCI security requirements—and to do so in an efficient and cost-effective manner.

Personal Information Protection and Electronic Documents (PIPEDA)

In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) establishes laws that regulate the collection, use, and disclosure of personal information by private sector organizations. The laws state that personal information must be protected by security safeguards appropriate to the sensitivity of the information, including technological measures, such as the use of passwords and encryption.

U.S. State Breach Disclosure

Modeled after California's S.B. 1386, the California Security Breach Notification Act, many states have adopted similar laws that require any person, business, or state agency that collects and stores personal customer information to notify individuals when their unencrypted personal information was, or is reasonably believed to have been, put at risk by a data security breach.

The ISO 27000 Series

This series will comprise a series of information security standards. This series will comprise an entire series of information security related standards. In the pipeline are ISO 27001, ISO 27002, ISO 27003, ISO 27004 and ISO 27005.

Specifically, these standards covered the following topics:

ISO 27001 – This is the revision of BS 7799 Part 2

ISO 27002 – renames ISO 17799

ISO 27003 – Implementation Guidance

ISO 27004 – Metrics and Measurement

ISO 27005 – Risk Management.

The above standards framed from 1995 to till date was based on the technology prevailing during those periods. As the Technology developed, the security has to be increased to mitigate all the short comings while adopting the technology to existing systems. Based upon the experience and knowledge of the technology, standards were developed. In this world of broadband communication revolution, the mobile communications is playing a vital role in communications, entertainment and education. As the mobile phones reached the masses, the users needs increased and the new economically viable services to these users were developed. Thus the mobile banking services came into prominence due to easy accessibility and affordability of mobile phones throughout the world. To extend this facility to all the mobile phone users, a standard has to be in place. How this mobile banking operations is done and the architecture needed to give this mobile banking operations is briefly explained.

MOBILE BANKING OPERATIONS

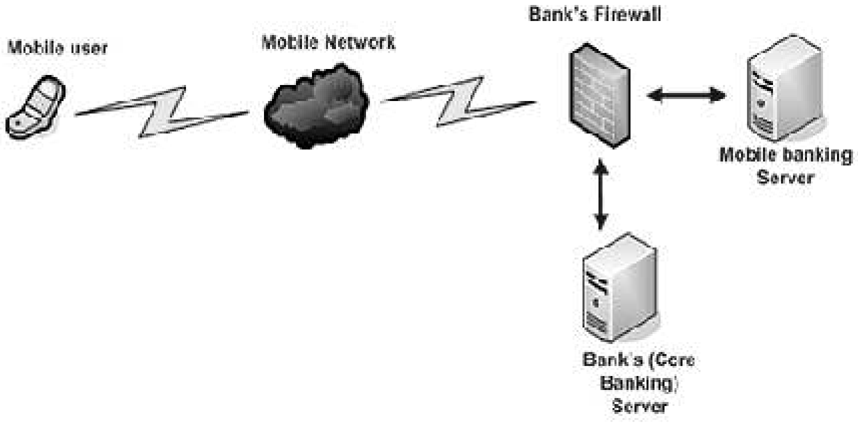
The Mobile Banking Operations consists of following step. They are :

- Maintains communication between the SIM card and the financial institution
- Routes mobile banking messages
- Manages mobile banking sessions
- Securely handles sensitive information
- Ensures the confidentiality and security of mobile transactions
- Manages user information
- Authenticates user
- Mobile Banking Architecture
- The two popular mobile banking architectures are
- The services which can be provided to customers directly by the bank

The services can be provided to customers through a 3rd party vendor

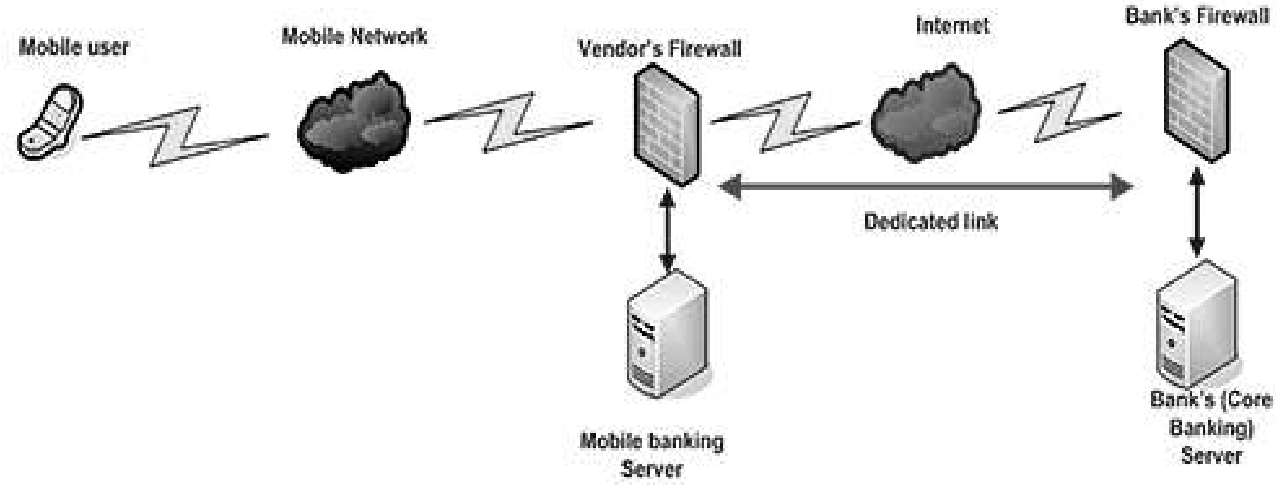
The architecture is based on the specific requirement that the facility is provided through GRPS, GSM, CDMA, EDGE, 3G and CSD enabled mobile phones. With Mobile banking, the following services can be availed of, but is not restricted to,

- Viewing A/C statement
- Viewing Cheque Status
- Stopping Cheque Payment
- Cheque Book Request
- Fixed Deposit Enquiry
- Bill Payment
- Shopping/ Purchasing items



Architecture 1: When the bank provides the service directly to the customer

The setup will have a web server, application server and the database at the bank's premises. The application will ensure what services are to be provided to the customer. Based on the banking services provided to the customer, the security of the infrastructure has to be built in. The database can be the same as the Core Banking database, having another table for mobile banking users. The customer uses his/her mobile phones to transact through the mobile network. The Mobile banking server in turn talks to the Core banking systems of the bank for user authentication, processing transactions, authorization, etc.



Architecture 2: When banks outsource this facility to 3rd party vendors

This is the more popular architecture as Banks can quickly roll out their mobile banking solutions by connecting to a 3rd party. This is also the architecture with more security issues as interconnection with a 3rd party is involved. In this architecture, the mobile banking servers are located at the 3rd party vendor's data centre. These servers will talk to the Core Banking servers of the bank through a secured channel (dedicated or shared link) for authentication, authorization and transaction processing. Due to the robust mobile banking architecture, mobile users are using banking services in their mobiles. The mobile users in different countries slowly accepting the mobile banking services based on the adoption of latest technology in their communication.

WORLD MOBILE BANKING SCENARIO

The mobile banking is being offered by most of the countries. All the banking services which were offered through online can be seen on mobile phones. Based upon the guidelines and recommendations of central banks of countries, the mobile banking services are on the upward trend. Let us study How these mobile banking services are offered and different methods used by banks by countries.

Mobile banking in US

The first option in mobile banking services is called Mobile web. Here all registered Bank Internet Banking customers can use this service. The customer can access the mobile banking services by logging via this web enabled browser with Internet banking login name and password.

The second option is called Mobile wallet- a downloadable application. Through this method, the customer can download mobile wallet from bank's website and it lets conveniently and securely access finances on wide variety of mobile devices. The customer can create own bank mobile PIN and Mobile wallet PIN and Download the mobile wallet onto mobile. After activating the mobile phone one can access the mobile banking services using wallet PIN. Both the options offer banking services freely.

The Bank will provide mobile banking services based upon mobile service provider and specific phone model at the beginning of the registration process. If the Mobile Wallet is not available for mobile service provider or particular device, the customer can access Mobile Banking at bank's website.Currently, about 100 devices are supported, including most smart phones.

According to Tower group report nearly 41 million US consumers will conduct some banking activity by mobile phone at least every 90 days by 2012. Most of the US banks started offering mobile banking in 2009.

Mobile Banking in Africa

It has been estimated that there are a billion people around the world who lack a bank account but own a mobile. Africa has the fastest-growing mobile phone market in the world and most of the operators are local firms.

In countries like South Africa, for example, mobile phones outnumber fixed lines by eight to one. In Kenya there were just 15,000 handsets in use a decade ago. Now that number tops 15 million. Setting up a bank account on your phone is straightforward. All you do is register with an approved agent, provide your phone, along with an ID card, and then deposit some cash onto your account. You can use it to pay for everything from beer to cattle - one Masai farmer told the BBC that when he sells cows in Nairobi, he puts the money on his phone to ensure that robbers can't get his cash. A Kenyan woman said she uses the technology to transfer money from her phone to that of her parents while a Nairobi businessman told us it was handy for settling customer accounts.

Mobile banking in European countries

Orange UK and Barclaycard introduce a new mobile payment system which is claimed to be the biggest evolution in terms of payment after the introduction of plastic cards, 40 years ago. This new system will enable the customers to make payments through their handsets at the retailers by waving their handset against a reader. The two firms intend to widen their service to ticketing, transport and rewards.Deutsche Bank's Global Transaction Banking (GTB) division has announced that it is introducing mobile phone payments services to its clients in 80 countries across Europe, Middle East and Asia. Luup, a European-based mobile payment provider, will partner with Deutsche Bank to provide the service.

This new mobile payment service will allow the Bank's GTB clients to offer millions of consumers an instant and secure payments and money transfer service from any mobile device with any mobile network. It is the first time a major commercial bank has offered a cross-border mobile payments service to its banking and corporate customers.

Mobile banking in Asia

In different countries, Mobile Banking has already gained its popularity. For example, in the South Korean market LG Telecom teamed up with Kookmin Bank to provide their Mobile Banking services in 2004 and since then they have seen a nice and steady growth. In India, Reliance Infocomm has started providing Mobile banking services to ICICI Bank and HDFC Bank through their R-World environment. The number of mobile users in India rose to 471 millions and expected to reach 531 millions in 2010.

Mobile Banking transactions in India - Operative Guidelines for Banks

Mobile phones as a delivery channel for extending banking services have off-late been attaining greater significance. [1]. The rapid growth in users and wider coverage of mobile phone networks have made this channel an important platform for extending banking services to customers. With the rapid growth in the number of mobile phone subscribers in India (about 5.33 billion as at the end of March 2011 and growing at about 12 million a month), banks have been exploring the feasibility of using mobile phones as an alternative channel of delivery of banking services. Some banks have started offering information based services like balance enquiry, stop payment instruction of cheques, transactions enquiry, location of the nearest ATM/branch etc. Acceptance of transfer of funds instruction for credit to beneficiaries of same/or another bank in favor of pre-registered beneficiaries have also commenced in a few banks. In order to ensure a level playing field and considering that the technology is relatively new, Reserve Bank has brought out a set of operating guidelines for adoption by banks.

1. Mobile banking transactions
2. Regulatory & Supervisory Issues
3. Registration of customers for mobile service
4. Technology and Security Standards
5. Inter-operability
6. Clearing and Settlement for inter-bank funds transfer transactions
7. Customer Complaints and Grievance Redressal Mechanism
8. Transaction limit
9. Board approval .
10. Approval of Reserve Bank of India

The above regulations formulated by RBI from time to time has become guidelines to carry mobile banking services offered by several banks in India. Even though there is absolutely no mobile banking standard, based on guidelines, like Indian banks other foreign banks are offering transactional and enquiry based limited banking services through mobiles. Before creating standard, Let us study the challenges posed by this mobile banking.

Challenges for a Mobile Banking Solution [7]

Key challenges in developing a sophisticated mobile banking application are :

Handset operability

There are a large number of different mobile phone devices from top 15 mobile companies and it is a big challenge for banks to offer mobile banking solution on any type of device. Some of these devices support J2ME and others support SIM Application Toolkit, a WAP browser, or only SMS.

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.[15] 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 :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.

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.

Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.

User ID / Password authentication of bank's customer.

Encryption of the data being transmitted over the air.

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

Scalability & Reliability

Another challenge for the CIOs and CTOs of 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 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 :

Preferred Language

Date / Time format

Amount format

Default transactions

Standard Beneficiary list

Alerts

The observation and analysis of the security standards leads us to following considerations before embarking on new mobile banking standards

NEW MOBILE BANKING DATA SECURITY STANDARD (MBDSS)

Based on the existing information security standards and due to increase in the cyber frauds especially financial frauds in banks, it is apparent to have robust mobile banking standards. Before evolving mobile banking data security standard one should consider the various security aspects and guidelines released from time to time. Hence the following MBDSS framework.

1. Device dependent mobile banking- The Mobile providers should comply with standards set for mobiles like email/sms/browser for financial transactions prescribed by central bank of that country

2. Built in data security- use of IC chips or downloadable web browser

3. All banks should comply with PCI-DSS as it safeguards the customer data and will be first level in the data security.

4. The mobiles should be all weather/architectural neutral, secured and simple device.

5. It should support Unicode i.e to support all the existing languages in the world

6. Mobile device should support transactions Irrespective of time and place of transactions

7. Alerts should be voice/ text generated/video generated

8. Adherence to the compliance- bank, mobile provider and security provider

9. The mobile banking fraud should be detected by banks and mobile provider and intimated to the customers before the next fraudulent transaction

10. Mobile device with blue tooth and mobile device without blue tooth treat differently geographically based banks supervised by central bank of particular country.

11. Any dispute/claims/payments should be localized and the countries should have agreement to prosecute any cyber fraudsters if found guilty irrespective of country of origin

12. The financial transactions should be limited to account balances only

13. No big financial transaction is allowed in mobile banking

14. Registration of mobile devices is compulsory and in person

CONCLUSION

With 4G technology, faster mobile communication that is 50 times faster than 3G mobiles, any type of services could be given. The mobile users are increasing due to the reliability and secured digital communications. With broadband communications already users are availing the online banking services through their offices and homes. Now users wants all the banking services on the move through their mobile phones. As the technology promised the reliability, privacy and security for their data, users wants more facilities put into mobiles. Due to PCI-DSS[18] security standards developed jointly by VISA/MASTER/American Express /JCB/Discover, the credit card and debit cards usage increased phenomenally as it provides robust security to their financial transactions.The bank customers are moved from Branch to ATM for financial transactions. Also it has saved time and cost of transactions. But due to lack of mobile banking standard which is suppose to provide their data security and privacy, the mobile users are hesitantly using bank services partially. To give impetus to the growth of mobile banking services in the world, the mobile banking data security standard has to be evolved and implemented so as to get confidence in the customer to carry any banking services either through online or mobile or ATM or Branch. To increase the confidence and to provide data integrity, confidentiality and non-repudiation the need of mobile data security standard framework is envisaged.

REFERENCES

1. Code of books from Reserve Bank of India

2. en.wikipedia.org/.../List_of_countries_by_ number_of_mobile_phones_in_ use

3. http://en.wikipedia.org/wiki/Mobile_banking

4. http://kuriositaet.de/iso8583/introduction.html

5. http://news.cnet.com/river/?tag=hdr;snav

6. http://www.bsigroup.com/en/Standards-and-Publications

7. http://www.bsigroup.com/en/Standards-and-Publications/About-standards/What-is-a-standard/

8. http://www.howstuffworks.com/

9. http://www.rbi.org.in/Scripts/NotificationUser.aspx

10. http://www.wisegeek.com/what-is-information-security.htm

11. https://www.pcisecuritystandards.org/

12. Mobile Technology from 1G to 4G from L S Ashiho

13. Owens, John and Anna Bantug-Herrera (2006): [1] Catching the Technology Wave: Mobile Phone Banking and Text-A-Payment in the Philippines

14. Tiwari, Rajnish and Buse, Stephan(2007): The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector, Hamburg University Press (E-Book as PDF to be downloaded)

15. Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006): Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises, in: CEC/EEE 2006, Proceedings of The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, pp. 522–529.

16. Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006): Mobile Banking as Business Strategy: Impact of Mobile Technologies on Customer Behaviour and its Implications for Banks, in: Technology Management for the Global Future - Proceedings of PICMET '06.

17. Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2007): Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage, in: Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management, New Delhi, pp. 886–894.

18. www.cashcow.in