Report of the Group on Enabling PKI in Payment System Applications

Reserve Bank of India

March 2014

Report of the Group on Enabling PKI in Payment System Applications

Reserve Bank of India

March 2014

Report of the Group on Enabling PKI in Payment System Applications

Dr Anil Kumar Sharma
(Convenor)

Shri P Ramachandran
(Member)

Shri Hemant Kumar
(Member)

Shri Sharad Saxena
(Member)

Shri D A Tambe
(Member)

Shri Pankaj Ekka
(Member)

Shri Pankaj Mishra
(Member)

Smt R. Jayalakshmi
(Member)

Shri Kalyan Chakravarthy
(Member)

INDEX

Abbreviations

ACID	Atomicity, Consistency, Isolation, Durability
AEPS	Aadhaar Enabled Payment Systems
ATM	Automated Teller Machine
BAH	Business Application Header
BIS	Bank for International Settlements
BOD	Begin-of-Day
BIN	Bank Identification Number
CA	Certifying Authority
CBLO	Collateralised Borrowing and Lending Obligation
CBS	Core Banking Solutions
CCA	Controller of Certifying Authorities
CCIL	Clearing Corporation of India Limited
CFCA	China Financial Certification Authority
CISO	Chief Information Security Officer
CMS	Cryptographic Message Syntax
CNP	Card Not Present
CP	Card Present
CRL	Certificate Revocation List
CTS	Cheque Truncation System
DGBA	Department of Government Banking and Accounts
DIT	Department of Information Technology
DPSS	Department of Payment and Settlement Systems
DSC	Digital Signature Certificate
DSS	Data Security Standard
ECS	Electronic Clearing Service
EOD	End-Of-Day
ESCB	European System of Central Banks
EU	European Union
EMV	Europay, MasterCard and Visa
FEMA	Foreign Exchange Management Act
FIPS	Federal Information Processing Standards
FSS	Financial Supervisory Service
HSRS	High Speed Reader Sorter System
HTTPS	Hypertext Transfer Protocol Secure
IDRBT	Institute for Development and Research in Banking Technology

IMPS	Immediate Payment Service
IP	Internet Protocol
ISO	International Organization for Standardization
IIN	Issuer Identification Number
ITSEC	Information Technology Security Evaluation Criteria
MAC	Message Authentication Code
MD5	Message Digest 5 Algorithm
MICR	Magnetic Ink Character Recognition
MITB	Man-in-the-browser attack
MITM	Man-in-the-middle attack
NDS	Negotiated Dealing System
NEFT	National Electronic Funds Transfer
NFS	National Financial Switch
NPCI	National Payments Corporation of India
NRT	Near Real Time
OTP	One Time Password
PA	Payment Application
PBF	Positive Balance File
PCI	Payment Card Industry
PIN	Personal Identification Number
PKC	Public Key Certificates
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
POS	Point of Sale
RBA	Risk-based Authentication
RBI	Reserve Bank of India
RECS	Regional Electronic Clearing Service
RTGS	Real Time Gross Settlement System
SHA	Secure Hash Algorithm
SHA-2	Secure Hashing Algorithm 2
SIPS	Systemically Important Payment Systems
SMS	Short Message Service
SSL	Secure Sockets Layer
STK	Standard Tool Kit
USIM	Universal Subscriber Identity Module
URN	Unique Reference Number
USB	Universal Serial Bus
VISA	Visa International Service Association

ACKNOWLEDGEMENTS

The members of the Group would like to place on record their gratitude to Shri Vijay Chugh, CGM, DPSS, RBI, Dr A.S. Ramasastri, CGM-in-C, DIT, RBI, Dr A.K. Hirve, CGM, DIT, RBI, Shri P. Parthasarthy, CGM, CISO, DIT, RBI, for giving valuable suggestions and guidance during the course of working of the Group.

The Group acknowledges the various inputs received from other participants of the Working Group Shri Shasi Sekhar Nishank, AGM (DIT, CO), RBI, Miss Rohini Daud, Assistant (DIT, CO), RBI, Shri Rushikant Shastri, Assistant Vice President, SBI, Shri N. C. Dash, AGM, SBI, Ms Sneha Suhas, DGM, ICICI Bank, Shri Dilip Gadekar, AM (DGBA, Core Banking Division, RBI).

The Group also acknowledges special invitees Shri Amitabh Tewary, Master Card; Shri Saiprasad Nabar, NPCI; Shri Shailesh Deshmukh, NPCI; Shri Sanjay Nazaret, VISA for their valuable contributions in providing inputs in preparation of the approach paper.

Executive Summary

1. The objectives of an effective payment system is to ensure a Safe, Secure, Efficient, Robust and Sound Payment System in the country. In order to secure electronic documents and transactions and to ensure legal compliance, digital technology is used.

2. Payment systems are subjected to various financial risks viz. Credit Risk, Liquidity Risk, Systemic Risk, Operational Risk and Legal Risk.

3. Electronic payments are based on Information security, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.). Two major aspects of information security are: IT Security and Information Assurance.

4. Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational.

5. Without security measures and controls in place, the data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

6. Network Attacks in Electronic Payment Systems include Eavesdropping, Data Modification, Identity Spoofing (IP Address Spoofing), Password-Based Attacks, Denial-of-Service Attack, Man-in-the-Middle Attack, Compromised-Key Attack, Sniffer Attack, and Application-Layer Attack.

7. The core principles of Information Security are Confidentiality, Integrity, Availability, Authenticity and Non-repudiation.

8. It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation. Thus it is important to adopt and review algorithms and key sizes from time to time in such a way that the electronic signature standards should not pose threat from contemporary computational power. For secure digital signature mentioned in the Information Technology Act , a storage medium which generates and retains the private key without it leaving the token, satisfy the exclusive control of private key is with subscriber. The generation and exclusive retention of private key on secure hardware crypto device should be as per well-established standards and such hardware crypto device is to be protected with secret code known only to subscriber. In the case of secure digital signature, the authenticity and integrity of the electronic record or any digital signature is presumed and the fact that such digital signature is the digital signature of the subscriber need not be proved. Apart from key storage requirements, secure signatures are required to be created and verified in accordance with security procedures (rule 2004).

9. Reserve Bank has been promoting use of Public Key Infrastructure (PKI) technology in the electronic payments systems to secure a transaction from non-repudiation angle. Various electronic payments systems introduced by RBI and other agencies viz. Real-Time Gross Settlement (RTGS) System, National Electronic Fund Transfer (NEFT), Collaterised Borrowing and Lending Obligation (CBLO), Forex Clearing, Government Securities Clearing, and Cheque Truncation System (CTS). In volume terms, these systems contributed 25.1 per cent whereas these systems contributed 93.7 per cent share to the total number of payment transactions carried out in the year 2012-13 (Table 2.2). Whereas

non-PKI enabled payment systems contributed 75 per cent in volume terms but only 6.3 per cent in value terms in the year 2012-13.

10. Of the non-PKI enabled payment systems, MICR Clearing and non-MICR clearing contributed 37 per cent and 10% per cent in volume terms (Chart 2.5) and 69 per cent and 25 per cent in value terms (Chart 2.6). However, with the implementation of CTS system across the country, the cheque clearing will also be PKI enabled. Of the remaining, debit cards and credit cards transactions contribute 21 per cent and 18 per cent in volume terms (Chart 2.5) and 1 per cent and 2 per cent in value terms respectively (Chart 2.6) and ECS debit constituted 8 per cent and ECS credit constituted 6 per cent in volume terms (Chart 2.5) and 1 per cent and 2 per cent respectively in value terms (Chart 2.6).

11. RBI had also issued guidelines on "Security and Risk Mitigation Measures for Electronic Payment Transactions" which are mentioned in Annex III (Security Measures already initiated by RBI for Electronic Payment systems). Accordingly, the issuing bank will need to convert the older cards (the ones with the traditional magstrip) into EMV chip and pin enabled ones (this will be done for users who have used their cards internationally at least once before).

12. Since most of the Internet Banking applications at bank's end interface with the PKI enabled payment systems, the payment transactions between originating bank and RBI are PKI enabled, however, the transaction leg between originating/ordering customer and the originating bank may not be PKI enabled. Various security features deployed by banks in their Internet Banking Applications is given in Annex I and II. This raises doubts in the end-to-end security and particularly in respect of non-repudiation of electronic payments transactions. In view of this, the Group recommends that customers should be informed of risks, existing security measures and also given a choice of different methods of authentication to be able to select a system that matches their security requirements.

13. All Banks' Internet Banking applications should mandatorily create authentication environment for password-based two-factor authentication as well

as PKI-based system for authentication and transaction verification in online Banking Transaction.

14. DBOD may review the KYC process in banks to meet the requirement of verification prior to issuance of Digital Signature Certificates (DSCs) by Banks.

~~15.~~ The major cost of the DSC is found to be the verification cost. Banks follow verification process of their customers, which is similar to the requirements of DSC application. CCA may examine to permit banks to act as Registration Authority (RA) for their customers for issue of DSCs.CCA to also examine exemption to all CAs from the circular/ guidelines issued by Government of India on physical verification of forms of subscriber as it is involved with banks regulated under Reserve Bank of India.

16. Physical form verification should rest at Registration Authority (RA) level.

17. The following points need to be considered for Digital Signature Certificate (DSCs) issued by CA

(a) Validity period for DSCs may be increased from 3 years to 5 years

(b) the cost of DSC to be brought down

(c) Renewal process for DSC to be made simple and same may be renewed with digitally signed message prior to expiry. If DSC is expired, physical verification may be followed

(d) CCA may examine issues of DSCs on various form factors.

18. A group under the aegis of IDRBT may be set-up to study and include alternative techniques/technologies used in Internet Banking Applications in Schedule 2 of the IT Act. Cloud-Hosted DSC, Trusted Execution Environment, Hardened “Soft” Signatures, Mobile PKI, Portable Security Transaction Protocol and Hybrid PKI Solution as alternative strategies may also be studied in detail keeping in view Indian context.

19. In Online banking transactions, banks should provide the option to its customers for enabling PKI for its online banking transactions as optional feature for all customers.

20. Implementation Strategy for PKI-based system environment for authentication and transaction verification by banks may be carried out in three phases:

- Short-Term Implementation Strategy (phase-I)
- Medium-Term Implementation Strategy (Phase-II)
- Long-Term Implementation Strategy (Phase-III)

Phase	Description	Remarks
I	Implementation of DSC as an optional feature for certain role holders in Corporate Internet Banking for login as additional authentication.	To be implemented by Banks within 6 months.
II	Implementation of DSC as an optional feature for Authorizers in Corporate Internet Banking for authorizing the transactions.	To be implemented by banks within 12 months.
III	Implementation of DSC as an optional feature for Personal Internet Banking Users for authorizing the transactions.	To be implemented by Banks within 18 months.

21. After PKI infrastructure is enabled in all the banks a review may be taken for mandating digital signature for large value payments.

Chapter I

Introduction

1.1 The objectives of an effective payment system is to ensure a Safe, Secure, Efficient, Robust and Sound Payment System in the country. In order to secure electronic documents and transactions and to ensure legal compliance, digital technology is used. However, in online banking transactions in India the account holder bears the liability of transactions in case of dispute. In view of this a Group comprising of members from banks (SBI and ICICI bank), IDRBT- CA, CCA (New Delhi) and RBI (DIT, DPSS, DGBA- CBS and CISO) was formed to prepare an approach paper for enabling PKI for the Payment Systems in India.

1.2 The Terms of reference for this group is as under:

(a) Feasibility of PKI implementation for different segments of payment Systems

(b) Approach of PKI implementation in each of the segments

(c) Methodology for issuance of certificates on a large scale and

(d) Strategy for preparing the entire financial system for such an implementation.

The Group has following members representing different RBI Departments and other Institutions/ Organisations:

Institution/ RBI Department	**Representatives**
RBI –Dept. of Information Technology	Dr Anil Kumar Sharma, GM, DIT
CCA, New Delhi	Shri P Ramachandran, Scientist 'D'
RBI – CISO	Shri Hemant Kumar, GM/CISO
State Bank of India (SBI)	1. Shri D A Tambe, GM, IT-Infrastructure
	2. Shri Pankaj Mishra, DM, IT-Payments
ICICI Bank	Shri Sharad Saxena, GM-IT

RBI – Dept. of Payment and Settlement Systems	Shri Pankaj Ekka, DGM
IDRBT, Hyderabad	Smt R. Jayalakshmi, AGM
RBI – Dept. of Govt. and Bank Accounts	Shri Kalyan Chakravarthy, AGM
RBI - Special Invitees	Shri P. Parthasarathi, CGM,CISO
Others - Special Invitees	1. Amitabh Tewary, Master Card
	2. Saiprasad Nabar, NPCI
	3. Shailesh Deshmukh, NPCI
	4. Sanjay Nazaret, VISA

The working group has held three meetings during November 11, 2013 to January 9, 2014 and finalized the report.

1.3 Payment systems are subjected to various financial risks which are under:

1.3.1 Credit Risk: It is the risk that participants in the transaction will not be paid for an outstanding claim. These participants include the counterparties themselves, the issuer of the settlement medium, and, if any, intermediaries involved in the delivery of goods, services, etc. Credit risks typically arises when one of the participants become insolvent.

1.3.2 Liquidity Risk: It is the risk that counterparty that owes funds will not be able to meet its payment obligation on time, thus adversely affecting the expected liquidity position of the recipient of funds at the time the funds are due.

1.3.3 Systemic Risk: It is the risk that credit or liquidity problems incurred by one institution, or a small number of institutions, lead to similar difficulties for others. It is the risk of collapse of an entire financial system or entire market. The risk imposed by inter-linkages and interdependencies in a system or market, where failure of single entity or cluster of entities can cause a cascading failure which could potentially bring down entire system or market.

1.3.4 Operational Risk: It is the risk arising from the people process and systems through which a company operates. It can also include other classes of risk, such as fraud, legal risks, physical or environmental risks.

1.3.4 Legal Risk: It is a subset of Operational Risk. Legal risk is the risk of suffering a loss as a consequence of unforeseen interpretation of the systems' contractual basis or the legislation on which the contracts between the parties are based, e.g. in connection with a court ruling meet non-contractual obligations.

1.4 As customers continue to increasingly adopt electronic payment products and delivery channels for their transactional needs, it is necessary to recognise that security and safety have to be robust. Any security related issues resulting in fraud have the potential to undermine public confidence in the use of electronic payment products which will impact their usage. Increased fraudulent activities, which include attacks on IT infrastructure and delivery channels (cyber attacks), also pose significant risks to payment system providers. Necessary measures to strengthen security have to be taken as such attacks are growing in scale and sophistication. This may also result in reputational risks to the payment system providers.

1.5 Electronic payments are based on Information security, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.). Two major aspects of information security are: IT Security and Information Assurance. Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

1.6 Without security measures and controls in place, payment data might be subjected to an attack. Some attacks are passive, meaning information is monitored;

others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

1.7 Communication networks and data are vulnerable to any of the following types of attacks in the absence of proper security plan in place.

1.8 Common Types of Network Attacks are as follows:

1.8.1 Eavesdropping : In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in the network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on the communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, the data can be read by others as it traverses the network.

1.8.2 Data Modification: After an attacker has read payment data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if the customers do not require confidentiality for all communications, the customers do not want any of the messages to be modified in transit. For example, if the customers are exchanging purchase requisitions, they do not want the items, amounts, or billing information to be modified. Any digitally signed data, if modified, could be detected easily.

1.8.3 Identity Spoofing (IP Address Spoofing): Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete customers data. The attacker can also conduct other types of attacks, as described in the following sections. Client-server authentication (TLS) should be in place to prevent this.

1.8.4 Password-Based Attacks: A common denominator of most operating system and network security plans is password-based access control. This means customers' access rights to a computer and network resources are determined by who he/she is, that is, his/her user name and his/her password. Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time. After gaining access to the payment network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete customers' data.

1.8.5 Denial-of-Service Attack: Unlike a password-based attack, the denial-of-service attack prevents normal use of the computer or network by valid users.

After gaining access to payment network, the attacker can do any of the following:

- Randomize the attention of internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behaviour of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

1.8.6 Man-in-the-Middle Attack: As the name indicates, a man-in-the-middle attack occurs when someone between the customer and the person with whom the customer is communicating is actively monitoring, capturing, and controlling the

communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming identity in order to read customer's message. The person on the other end might believe it is payer (Sending Customer) because the attacker might be actively replying as he/she likes to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

1.8.7 Compromised-Key Attack: A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key. An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack. With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

1.8.9 Sniffer Attack: A sniffer is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunnelled) packets can be broken open and read unless they are encrypted and the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze network and gain information to eventually cause the network to crash or to become corrupted.
- Read the communications.

1.8.10 Application-Layer Attack: An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of the application, system, or network, and can do any of the following:

- Read, add, delete, or modify the data or operating system.

- Introduce a virus program that uses computers and software applications to copy viruses throughout the network.
- Introduce a sniffer program to analyze the network and gain information that can eventually be used to crash or to corrupt the systems and network.
- Abnormally terminate data applications or operating systems.
- Disable other security controls to enable future attacks.

1.9 The core principles of Information Security are:

1.9.1 Confidentiality: Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary for maintaining the privacy of the people whose personal information is held in the system.

1.9.2 Integrity: In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of Consistency as understood in the classic ACID (Atomicity, Consistency, Isolation, Durability) model of transaction processing. Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

1.9.3 Availability: For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service

disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

1.9.4 Authenticity: In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

1.9.5 Non-repudiation: In law, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

1.10 Various foreign countries have either implemented or in the process of implementing PKI in their projects. The same is discussed in detail in Chapter II.

Chapter II

Security Features in Existing Payment System Applications

2.1 There are various Indian Payment Systems which have emerged into Indian Financial Systems which may be classified as follows:

2.1.1 Paper Based Payment Systems: An important milestone in cheque clearing was mechanization of the clearing operations using Magnetic Ink Character Recognition (MICR) technology. Based on the recommendations of Damle Committee (1983), RBI introduced MICR-based clearing in the four metro cities of Chennai, Mumbai, Kolkata and New Delhi during 1986. Under the MICR technology the information necessary for mechanised processing is encoded, using special ink containing magnetisable particles, in the MICR band contained in the lower part of a cheque. Currently, cheque processing is carried out using MICR HSRS in 51 locations (MICR centres) in the country. With an objective to bring in further efficiency in the paper based clearing system, Cheque Truncation System (CTS), introduced by Reserve Bank of India in New Delhi in February 2008 which is PKI enabled. Under CTS, the physical movement of cheques is curtailed at the presenting bank level. The Clearing and settlement is done on the basis of images and MICR code line information (cheque number, MICR code, Short Account Number, Transaction Code). The payment processing is done by the drawee banks on the basis of images. The legal framework for cheque truncation was put in place by way of amendments to the Negotiable Instrument Act (Section 6 of the NI Act which defines a 'cheque' has been amended to include the "electronic image of a truncated cheque" and IT Act. It uses end-to-end Public Key Infrastructure (PKI) for security and non-repudiation.

2.1.2 Electronic Payments: The initiatives taken by RBI in the mid-eighties and early-nineties focused on technology-based solutions for the improvement of the payment and settlement system infrastructure, coupled with the introduction of new payment products by taking advantage of the technological advancements in banks. The continued increase in the volume of cheques added pressure on the existing set-up, thus necessitating a cost-effective alternative system.

(a) ECS Suite of products:

Electronic Clearing Service-Debit and Credit: The ECS Credit scheme was introduced in 1994 whereby electronic payment instructions are issued to replace paper instruments. The system works on the basis of one single debit transaction triggering a large number of credit entries and is useful for companies/governments making payments to a large number of beneficiaries. Under the scheme, the accounts of the investors/ beneficiaries are directly credited to their bank accounts without issue of paper instruments. The types of payments made include dividend payments, interest payments, salary, pensions, IPO Refund, IT refund etc. The ECS (Credit) offers certain advantages to customers as well as institutions. Customers are also benefited as it enables receipt of dividend/salary/other payment on due date itself, directly into the bank account without the need for visiting the bank for depositing the cheque/dividend/interest warrant etc.

Subsequently, the ECS (Debit) scheme was introduced in 1995 which facilitates payment of charges for utility services such as electricity, telephone companies, payment of insurance premia, credit card payments, loan installments, School/college/University/club fees etc. by customers overcoming certain deficiencies/problems faced by both the customers as well as user institutions. For instance, the need for customers to visit collection centres/authorized banks and stand in long queues for payment of bills/dues/fees, delays in collection of cheques, loss in transit, forgery, dishonor, fraud, etc. ECS (Debit) involves a large number of debits resulting in a single credit simultaneously and works on the principle of pre-authorised debit system under which the account holders' account is debited on the appointed date and the amounts are passed on to the beneficiary companies/user institutions. The system works on the strength of the mandate given by the account-holder/customer to the user institution whereby he/she authorizes the institutions to directly raise a debit to the bank account. The mandate also specifies the start and end date of the mandate, the frequency of payments under the mandate, the maximum permissible amount and so on, which need to be verified by the bank before debiting the customer’s account for the ECS amount. Both these facilities are available at all major cities across the country operated by RBI at some centre and by other banks at remaining centres. However, both these system works on decentralised model.

ECS (RECS) (Debit and Credit): To take care of pan-state / group of states payments from a location within the state itself and leveraging on CBS available in the banks, RECS was launched during the year 2009. The coverage is usually all the CBS enabled bank branches in a state / group of state. Under the system, the sponsor bank will upload the validated data through the Secured Web Server of RBI containing credit/debit instructions to the customers of CBS enabled bank branches spread across the Jurisdiction of the Regional office of RBI. The RECS centre will process the data, arrive at the settlement, generate destination bank wise data/reports and make available the data/reports through secured web-server to facilitate the destination bank branches to afford credit/debit to the accounts of beneficiaries by leveraging the CBS technology put in place by the bank. Presently RECS is available in 12 RBI centres (Ahmedabad, Bengaluru, Bhubaneswar, Chandigarh, Chennai, Guwahati, Hyderabad, Jaipur, Kolkata, Nagpur, New Delhi and Thiruvananthapuram.

National Electronic Clearing Service (NECS) Credit: To further leverage on technological development in the banking and leveraging on CBS in banks, RBI launched NECS in October 2008. The scheme is operated from National Clearing Cell (NCC), Mumbai. NECS (Credit) facilitates multiple credits to beneficiary accounts with destination branches across the country against a single debit of the account of the sponsor bank. This arrangement obviates multiple setups across country for facilitating ECS payments and saves a lot of resources for all the stakeholders. As of now, 76,310 bank branches spread across country are covered under the scheme and the same are growing every month.

(b) National Electronic Funds Transfer (NEFT) System: This retail electronic funds transfer system introduced in the late 1990s enabled an account holder of a bank to electronically transfer funds to another bank account holder with any other participating bank. EFT was available across 15 major centers in the country has been replaced by state of art, feature rich and more efficient system. NEFT launched in November 2005, is a more secure system introduced by Reserve Bank of India for facilitating one-to-one funds transfer requirements of individuals / corporate. NEFT is now the main electronic system for retail electronic payments operating in a near-real-time mode. Under NEFT, individuals, firms and corporate can electronically transfer funds from any branch to any individual, firm or corporate having an account

with any other bank branch in the country. NEFT system provides for batch settlements at hourly intervals, thus enabling near real-time transfer of funds. Certain other unique features viz. accepting cash for originating transactions, initiating transfer requests without any minimum or maximum amount limitations, facilitating one-way transfers to Nepal, receiving confirmation of the date / time of credit to the account of the beneficiaries, etc., are available in the system.

(c) Real Time Gross Settlement (RTGS) System: RTGS is an electronic funds transfer systems where transfer of money takes place from one bank to another on a "real time" and on "gross" basis. Settlement in "real time" means payment transaction is not subjected to any waiting period. "Gross settlement" means the transaction is settled on one to one basis without bunching or netting with any other transaction. Once processed, payments are final and irrevocable. This was introduced by Reserve Bank of India in 2004 and settles all inter-bank payments and customer transactions above Rs. 2 Lakhs. This payment system is one of the systemically important payment system applications. From 4 participants handling a few thousand transactions, RTGS has grown exponentially in terms of both the number of participants and the volume of transactions handled. Today RTGS caters to around 167 participants processing, on an average, 275,000 transactions a day. The Existing RTGS system was discontinued with effect from October 19, 2013. The new RTGS system was launched by the Governor on October 19, 2013 in RBI, Mumbai. There are more than 1,00,000 RTGS enabled branches in India. As on October 31, 2013, 3,53,665 number of RTGS transactions were settled in RTGS system.

(d) Collaterised Borrowing and Lending Obligation (CBLO): CBLO is another money market instrument operated by the Clearing Corporation of India Ltd. (CCIL), for the benefit of the entities who have either no access to the interbank call money market or have restricted access in terms of ceiling on call borrowing and lending transactions. It is a repo variant, permitted by RBI. CBLO is a discounted instrument available in electronic book entry form for the maturity period ranging from one day to ninety days (up to one year as per RBI guidelines). In order to enable the market participants to borrow and lend funds, CCIL provides the Dealing System through Indian Financial Network (INFINET), a closed user group to the Members of the Negotiated Dealing System (NDS) who maintain Current account with RBI and

through Internet for other entities who do not maintain Current account with RBI. Under CBLO, securities of borrower will be held in their constituent SGL account opened with CCIL and will not be transferred to lender. Membership to the CBLO segment is extended to entities who are RBI- NDS members, viz., Nationalized Banks, Private Banks, Foreign Banks, Co-operative Banks, Financial Institutions, Insurance Companies, Mutual Funds, Primary Dealers, etc. Associate Membership to CBLO segment is extended to entities who are not members of RBI- NDS, viz., Co-operative Banks, Mutual Funds, Insurance companies, NBFCs, Corporate, Provident/ Pension Funds, etc. By participating in the CBLO market, CCIL members can borrow or lend funds against the collateral of eligible securities. Eligible securities are Central Government securities including Treasury Bills, and such other securities as specified by CCIL from time to time. Borrowers in CBLO have to deposit the required amount of eligible securities with the CCIL based on which CCIL fixes the borrowing limits. CCIL matches the borrowing and lending orders submitted by the members and notifies them. While the securities held as collateral are in custody of the CCIL, the beneficial interest of the lender on the securities is recognized through proper documentation.

2.1.3 Other Payment Systems

(a) Pre-paid Payment Systems

Pre-paid instruments are payment instruments that facilitate purchase of goods and services against the value stored on these instruments. The value stored on such instruments represents the value paid for by the holders by cash, by debit to a bank account, or by credit card. The pre-paid payment instruments can be issued in the form of smart cards, magnetic stripe cards, internet accounts, internet wallets, mobile accounts, mobile wallets, paper vouchers, etc.

Subsequent to the notification of the PSS Act 2007, policy guidelines for issuance and operation of prepaid instruments in India were issued in April 2009 to regulate the issuance of prepaid payment instruments in the country. The guidelines have been revised many times in past to reflect the changing environment and technological developments. The use of pre-paid payment instruments for cross border transactions has not been permitted, except for the payment instruments approved under Foreign Exchange Management Act,1999 (FEMA).

(b) Mobile Banking System

Mobile phones as a medium for providing banking services have been attaining increased importance. Reserve Bank brought out a set of operating guidelines on mobile banking for banks in October 2008, according to which only banks which are licensed and supervised in India and have a physical presence in India are permitted to offer mobile banking after obtaining necessary permission from Reserve Bank. The guidelines have clearly specified that the technology used for mobile banking must be secure and should ensure confidentiality, integrity, authenticity and non-repudiation. The limits placed on transactions amounts have since been removed and banks have been advised to set their own limit depending on the bank's risk perception, with the approval of their Board. Further, end to end encryption has been mandated for all the transaction above Rs 5,000/-.

(c) ATMs / Point of Sale (POS) Terminals / Online Transactions

Till October-end, the total number of ATMs stood at 1,04,500. Savings Bank customers can transact from any banks' ATM up to 5 times in a month without being charged for the same. To address the customer service issues arising out of failed ATM transactions where the customer's account gets debited without actual disbursal of cash, the Reserve Bank has mandated re-crediting of such failed transactions within 7 working day and mandated compensation for delays beyond the stipulated period. Furthermore, a standardized template has been prescribed for displaying at all ATM locations to facilitate lodging of complaints by customers.

There are around 10 lakh POS terminals in the country, which enable customers to make payments for purchases of goods and services by means of credit/debit cards. To facilitate customer convenience the Bank has also permitted cash withdrawal using debit cards/ prepaid cards issued by the banks at PoS terminals.

The PoS for accepting card payments also include online payment gateways. This facility is used for enabling online payments for goods and services. The online payments are enabled through own payment gateways or third party service providers called intermediaries. In payment transactions involving intermediaries, these intermediaries act as the initial recipient of payments and distribute the payment to merchants. In such transactions, the customers are exposed to the uncertainty of payment as most merchants treat the payments as final on receipt

from the intermediaries. In this regard to safeguard the interests of customers and to ensure that the payments made by them using Electronic/Online Payment modes are duly accounted for by intermediaries receiving such payments, directions were issued in November 2009 by RBI. Directions require that the funds received from customers for such transactions need to be maintained in an internal account of a bank and the intermediary should not have access to the same.

Further, to reduce the risks arising out of the use of credit/debit cards over internet/IVR (technically referred to as card not present (CNP) transactions), Reserve Bank mandated that all CNP transactions should be additionally authenticated based on information not available on the card and an online alert should be sent to the cardholders for such transactions.

(d) Immediate Payment Service (IMPS)

Immediate Payment Service (IMPS) is a payment service introduced by National Payments Corporation of India (NPCI). The service, launched as an instant mobile remittance solution in November, 2010 has today evolved as a multi-channel, multi-dimensional remittance platform. The IMPS platform today is capable of processing P2P (Person to Person), P2A (Person to Account) and P2M (Person to Merchant) remittance and transactions can be initiated from Mobile, Internet as well as ATM channel. In addition to banking customers, non-banking customers can also avail the IMPS facility through PPIs issued by non-bank issuer authorized by Reserve Bank of India.

IMPS offer an instant, 24X7, interbank electronic fund transfer service through multiple channels.

This facility is provided by NPCI through its existing NFS switch.

(e) Aadhaar Enabled Payment Systems (AEPS)

AEPS is a bank led model which allows online interoperable financial inclusion transaction at PoS (Micro ATM) through the Business correspondent of any bank using the Aadhaar authentication.

The four Aadhaar enabled basic types of banking transactions are as follows:-

- Balance Enquiry

- Cash Withdrawal
- Cash Deposit
- Aadhaar to Aadhaar Funds Transfer

The only inputs required for a customer to do a transaction under this scenario are:-

- IIN (Identifying the Bank to which the customer is associated)
- Aadhaar Number
- Fingerprint captured during their enrollment

(f) Credit cards and Debit cards

As mentioned above India is one of the fastest growing countries in the plastic money segment. Today there are close to 350 million debit cards and 19 million credit cards in India in circulation. According to MasterCard, 75% of all card payments are concentrated in the top 20 cities with Delhi, Mumbai and their sub-urban alone accounting for 43 per cent. Credit cards have a higher share in the discretionary category whereas debit cards dominate in routine expenses like utility payments. About 30 per cent of credit card spends are being done online. At least 10-15 per cent of customers use their cards only online, many from smaller cities. A Visa study reveals that people in the monthly income band of Rs 75,000-100,000 are the most prolific users of electronic cards.

Electronic payments dominate their expenses: rail/ airfare (71 per cent), durable goods (61 per cent), rent (49 per cent), tele/ mobile (47 per cent), medical institutions (46 per cent), clothing/ footwear (44 per cent), beverage and refreshments (35 per cent).Card payments form an integral part of e-payments in India because customers make many payments on their card-paying their bills, transferring funds and shopping.

Ever since Debit cards entered India, in 1998 they have been growing in number and today they consist of nearly 95 per cent of the total number of cards in circulation.

Credit cards have shown a relatively slower growth even though they entered the market one decade before debit cards. Majority of credit card purchases come from expenses on jewellery, dining and shopping.

2.2 Overall, during 2012-13the payment and settlement systems registered healthy growth, with volumes and value growing at 15.0 per cent and 29.7 per cent, respectively, on y-o-y basis compared with the growth of 9.0 per cent and 23.2 per cent, respectively during the previous year.

2.3 As can be seen from Table 2.1, it is observed that the use of debit cards is growing increasing over the period of last 3 years both in terms of number of transactions and value also. In the year 2012-13, number of transactions through credit cards and debit cards were 396.6 million and 469.1 million respectively.

Table 2.1: Payment System - Annual Turnover

Item	Volume (million)			Value (₹ billion)		
	2010-11	2011-12	2012-13	2010-11	2011-12	2012-13
1	2	3	4	5	6	7
Systemically Important Payment Systems (SIPS) through RTGS	**49.3**	**55.0**	**68.5**	**484872.3**	**539307.5**	**676841.0**
Total Financial Markets Clearing (1+2+3)	**1.7**	**1.9**	**2.26**	**383901.3**	**406071.2**	**501598.5**
1. CBLO	0.15	0.14	0.16	122597.4	111554.3	120480.4
2. Government Securities Clearing	0.36	0.44	0.70	69702.4	72520.8	119948.0
3. Forex Clearing.	1.20	1.30	1.40	191601.5	221996.1	261170.1
Others (4+5+6)	**1387.4**	**1341.9**	**1313.7**	**101341.3**	**99012.1**	**100181.8**
4. CTS	160.4	180.0	275.1	14391.2	15103.7	21779.5
5. MICR Clearing	994.6	934.9	823.3	68621.0	65093.2	57504.0
6. Non-MICR Clearing	232.3	227.0	215.3	18329.1	18815.1	20898.3
Total Retail Electronic Clearing (7+8+9)	**406.3**	**512.3**	**692.8**	**11944.9**	**20574.9**	**31876.8**
7. ECS DR	156.7	164.7	176.5	736.5	833.6	1083.1
8. ECS CR	117.3	121.5	122.2	1816.9	1837.8	1771.3
9. EFT/NEFT	132.3	226.1	394.1	9391.5	17903.5	29022.4
Total Cards (10+11)	**502.2**	**647.5**	**865.7**	**1142.1**	**1500.4**	**1972.9**
10.Credit Cards	265.1	320.0	396.6	755.2	966.1	1229.5
11.Debit Cards	237.1	327.5	469.1	386.9	534.3	743.4
Total Others (4 to 11)	**2295.9**	**2501.7**	**2872.2**	**114428.2**	**121087.4**	**134031.4**
Grand Total (1 to 11)	**2346.9**	**2558.6**	**2942.9**	**983201.8**	**1066466.1**	**1312470.9**

(Source: RBI Annual Report 2012-2013)

2.4 Share of electronic based payment transactions have been increasing both in volume and values terms. Whereas share of Paper based payments transactions are gradually decreasing both in terms of volume and value of transactions.

2.5 An overview on volume of transactions and their values in various payments system during the years is illustrated as shown below:

2.6 RTGS transactions have shown growth of 11.2 per cent in transaction value for the period 2011-2012 as compared with the period 2010-2011. Further the transaction value has increased by 25.5 per cent for the period 2012-13 as compared with the previous period 2011-2012. From both the charts, it may be concluded that share of RTGS transactions (in value terms) have increased from 51 per cent in 2011-12 to 52 per cent in 2012-13. Share of paper based payment system has declined significantly.

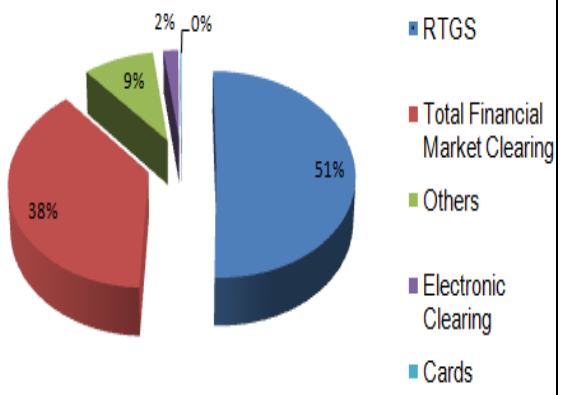
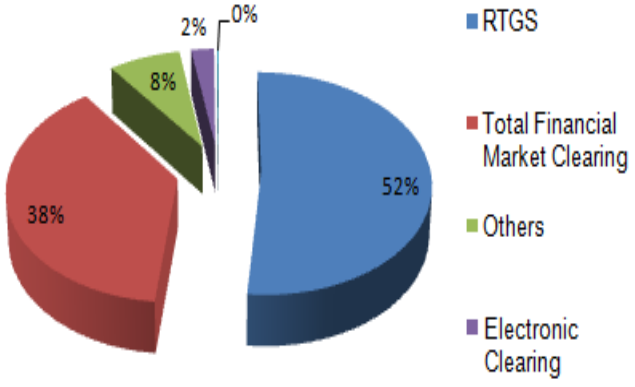
Chart 2.1: Value of Transaction for the period 2011-12 (Payment system wise)	**Chart 2.2: Value of Transaction for the period 2012-13 (Payment system wise)**
	

Table 2.2: PKI Vs Non-PKI Payment System - Annual Turnover

		2012-13	2012-13
Sr. No.	**Item**	**Volume (million)**	**Value (Rs. Billion)**
	PKI enabled Payment Systems		
1	SIPS through RTGS	68.5	6,76,841.0
2	CBLO	0.2	1,20,480.4
3	Government Securities Clearing	0.7	1,19,948.0
4	FOREX	1.4	2,61,170.1
5	CTS	275.1	21,779.5
6	NEFT	394.1	29,022.4
	Sub Total(1+2+3+4+5+6)	**740.0**	**12,29,241.4**
	Non-PKI		
7	MICR clearing	823.3	57,504.0
8	Non-MICR clearing	215.3	20,898.3
9	ECS DR	176.5	1,083.1
10	ECS CR	122.2	1,771.3
11	Credit Cards	396.6	1,229.5
12	Debit Cards	469.1	743.4
	Sub Total(7+8+9+10+11+12)	**2,203.0**	**83,229.6**
	Grand Total	**2,943.0**	**13,12,471.0**

(Source : RBI Annual Report 2012-2013)

Chart 2.3: PKI Enabled Payment Systems (Volume-wise) for the period 2012-2013.

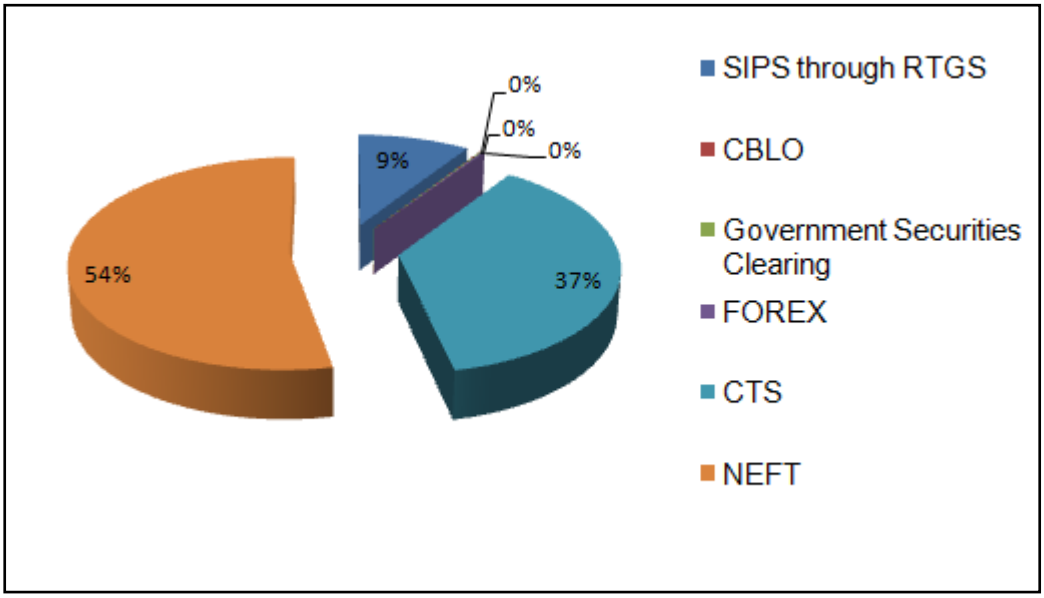


Chart 2.4: PKI Enabled Payment System (Value-wise) for the period 2012-2013

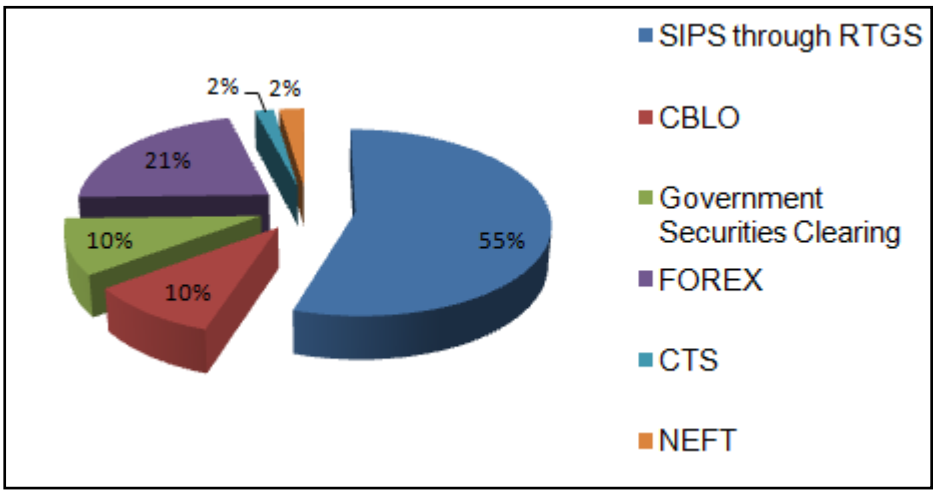


Chart 2.5: Non-PKI Enabled Payment System (Volume-wise) for the period 2012-2013

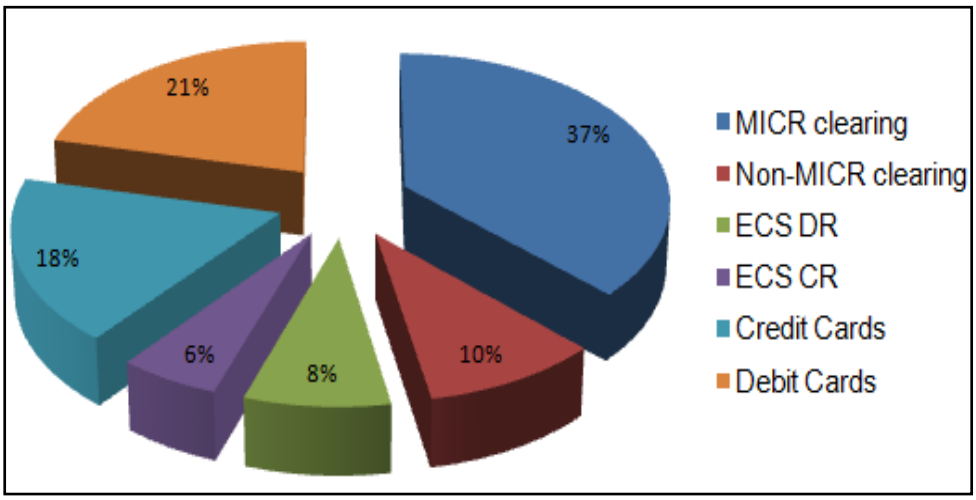


Chart 2.6: Non-PKI Enabled Payment System (Value-wise) for the period 2012-2013

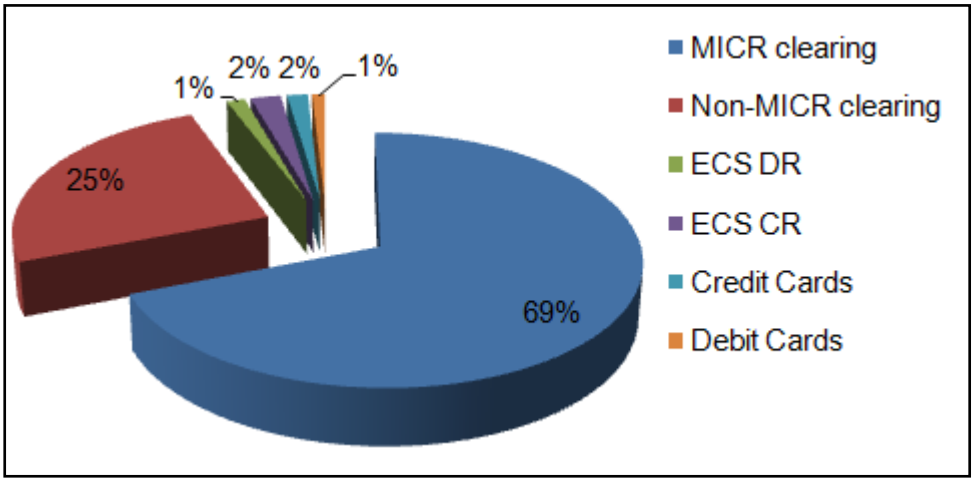
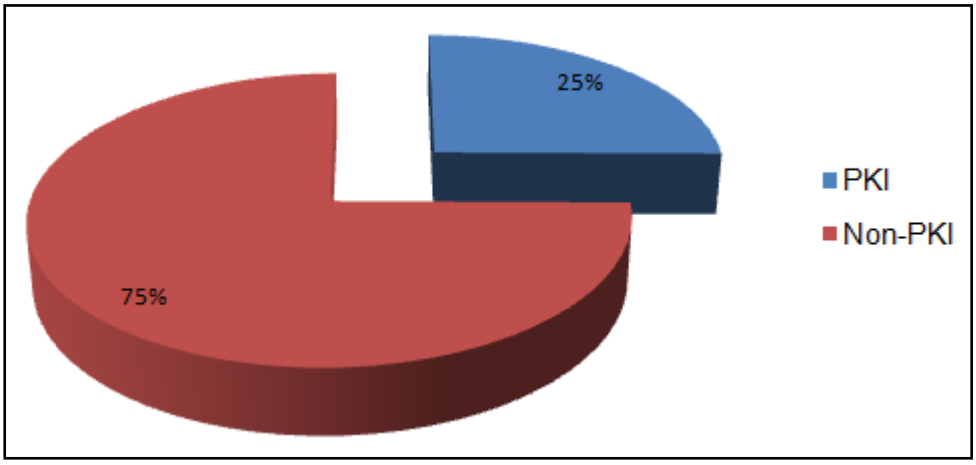
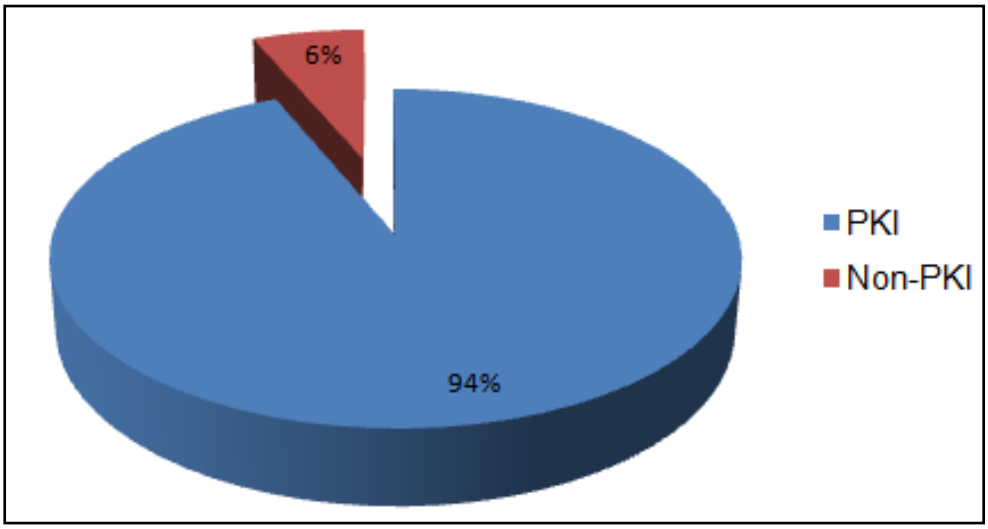


Chart 2.7: PKI Vs Non-PKI (Volume wise for the Period 2012-2013)



2.7 As seen from the Chart 2.7, non-PKI based transactions constitute 75 per cent of all the payments systems for the period 2012-2013. The PKI based transactions constitute 25 per cent of the total payment transaction during the same Period.

Chart 2.8: PKI Vs Non-PKI (Value wise for the Period 2012-2013)



2.8 As it may be seen from the Chart 2.8, value wise the PKI enabled payment systems constitute 94 per cent of the total value of payment systems.

2.9 Security Arrangements in Existing Payment Systems

2.9.1 Security and Risk Mitigation Measures for Card Present Transactions: In its endeavor to ensure that the payment systems operated in the country are safe, secure, sound and efficient, RBI has been taking proactive measures to contain the incidence of frauds in these systems. One such measure has been the move to secure Card Not Present (CNP) transactions, making it mandatory for banks to put in place additional authentication/validation for all on-line/ IVR/MOTO/recurring transactions etc. based on information not available on the credit/debit /prepaid cards.

Card Present (CP) Transactions (transactions at ATM and POS delivery channels) constitute the major proportion of card based transactions in the country. Although a PIN validation is necessary for cash withdrawal at ATMs, majority of the card transactions at POS were not enabled for any additional authentication (other than

signature). A majority of the cards issued by banks in India are Magstripe cards and the data stored on such cards are vulnerable to skimming and cloning.

The increased usage of credit/debit cards at various delivery channels also witnessed the increase in the frauds taking place due to the cards being lost / stolen, data being compromised and cards skimmed/counterfeited. To address this issue, RBI constituted a Working Group in March, 2011, with representations from various stake holders to examine these aspects and recommend an action plan which would foolproof the ecosystem. The Group submitted its report in June, 2011 and its recommendations, inter alia, include use of Aadhaar (an initiative of the Unique Identification Authority of India) based biometric authentication for all CP transactions in lieu of PIN with Magstripe cards continuing to be the form factor. The need for a complete migration to EMV Chip and PIN based cards could be considered based on the progress of Aadhaar in about 18 months. The Group has also recommended measures to secure the technology infrastructure, improve fraud risk management practices and strengthen merchant sourcing process within a period of 12-24 months. The report was examined and the recommendations therein have broadly been accepted by RBI.

Accordingly, it was advised that the banks not complying with the requirements shall compensate loss, if any, incurred by the card holder using card at POS terminals not adhering to the mandated standards.

Further, the banks have been mandated to issue EMV(card with chip and pin) to certain category of customers and for the other customers, banks have been given option to either issue EMV cards or adopt Aadhaar biometric authentication as additional factor of authentication. The banks have also been advised to enable acquiring infrastructure for both EMV and Aadhaar authentication.

2.9.2 Security Features in NEFT Application: NEFT application uses the Structured Financial Messaging System (SFMS) formats provided by Indian Financial Network (INFINET). Hence it uses the security features provided by SFMS.

SFMS uses X.509 Digital signatures for access control and authentication messages. Messages are encrypted with the receiving node's Public Key to protect confidentiality of the message while in transit. Access control and authentication procedures are different for different categories of users. There are four kinds of users in SFMS namely Creator, Verifier, Authorizer and Super Users.

- Creator: Creator users are only allowed to create, list and view messages.
- Verifier: Verifier users verify outgoing messages created by creator users.
- Authorizer: Authorizer users authorize messages verified by verifier users.
- Super Users: Super users create and maintain other user accounts.

Access control: Access Control for creator users is based on passwords. All other categories of users will have to sign the login message with their private keys stored in their smart cards/ tokens to gain access to any SFMS server (viz., Hub, CGBS, Gateway, Branch, or Off-line server).

Authentication: When a message is verified or authorized, the verifier/authorizer user has to digitally sign the message. The digital signature of the verifier user is stored in the local database and the authorizer user's signature is appended to the message and travels to the destination server. Even after the message is processed at the destination node, the signature is stored with the message when it is archived so that it is available even at a later date for verification and also to prevent altering of messages after archival.

Certification: Thus, all categories of users except Creator users will have to have legally valid Public Key Certificates (PKC) issued by a Certifying Authority licensed by the Controller of Certifying Authorities (CCA), Ministry of Communications and Information Technology, Government of India, New Delhi. Similarly, every server (viz., Hub, CGBS, Gateway, Branch, or Off-line Server), will have to be provided with a signing PKC and an encryption PKC. In addition, banks may opt for Secure Server (SSL) Certificates for allowing HTTPS access to those servers which are accessed by remote on-line terminals. Thus, the various PKCs required for SFMS operations will be as follows:

User PKCs: For Every User at Gateway or CGBS, For Every Verifier, Authoriser or Super User at Branches

Server Signing PKC: For Every SFMS Server (viz., Hub, CGBS, Gateway, Branch, or Off-line Server)

Server Encryption PKCs: For Every SFMS Server (viz., Hub, CGBS, Gateway, Branch, or Off-line Server)

Secure Server PKCs: For any server where the Bank feels it is necessary to restrict access to HTTPS mode.

2.9.3 Security Features in RTGS System:

(a) Security for RTGS clients

There are three different classes of client systems which will interact with the RTGS application for the settlement of payment instructions. Below is an overview of the security requirements for each of the said options.

(b) Thick Clients Security: The messages received by the RTGS from the thick clients connected to the INFINET network are digitally signed using the certificates issued by IDRBT to the respective Participants. The signature is included in the business application header (BAH) of the message and it covers the actual ISO message, excluding the BAH. The RTGS verifies the signature of each message before it accepts the settlements. Then the signature is copied verbatim by the RTGS to the outgoing message delivered to the receiving Participant after the settlement takes place so that the receiving institution can verify the authenticity of the payment.

The RTGS application will ensure that the owner of the certificate used to sign the incoming message is also the debited party indicated within the message's details.

(c) Web-service API Clients Security: The client applications that will implement the Web-service API provided by the RTGS system will have to comply with the following security requirements:

- The client application must connect to the RTGS using HTTPS protocol only. For this, the client application must have access to a digital certificate issued by IDRBT and recognized by the RTGS.
- The messages submitted by the client application must have the same message format (i.e. ISO 20022) as the messages received from the Message hub. This includes the signature requirements as presented above.
- The certificate used to secure the connection plus the certificate used to sign the message must be issued to the same Participant which must be identified as the debit party within the payment message.

(d) Browser-based Clients Security: The users that will submit and receive payments to and from the RTGS using the Internet browsers must comply with the following security constraints:

- Each user must have an individual certificate issued by IDRBT specifically for the RTGS activity. This certificate must be securely stored on an e-Token device protected by a secret pin or password. Each user will have a profile defined in the RTGS that will describe the system functions the user is able to access to. These functions will be set by a security officer of RBI or of the respective Participant.
- To access the PO application that provides the user input function for messages, the user must also provide a username and a password. The password must be regularly changed and has to meet the RBI's complexity requirements for passwords.

The browser-based clients will be used by the Participants but also by the RBI, for the command and control operations that maintain and coordinate the RTGS application. So the above security measures apply to both categories of users.

(e) User security Management: All users of RTGS and PO will be authenticated based on a digital certificate issued by RBI's Certifying Authority or IDRBT, a username and a secret password and user certificate serial number. The certificate will be stored securely on token device along with the private and public keys. The user account definitions along with their passwords and certificate serial numbers will be stored in the application main database. The passwords are stored only in an encrypted format. A password policy (i.e. minimum length, minimum complexity etc.) will be enforced to all users according to RBI internal regulations. The system will also force the users to periodically update their passwords, without reusing the same values. User Management will be the responsibility of the admin of respective participants.

(f) PKI-based Digital Signatures: Files imported by the PO function of RTGS will have to be digitally signed using a certificate issued by RBI's Certifying Authority. Details are provided in the Security User Guide regarding certificates and their use.

RBI's Certifying Authority will issue for each registered user a digital signing certificate on security device i.e. E-Token) containing a pair of keys (private and public key). At the central location of the RBI's Certifying Authority, a Certificate Revocation List (CRL) will be maintained to manage the revoked certificates. If RBI

deploys several CA servers and root certificates to handle the certificate issuance process, the RTGS application will support multiple Certificate Revocation List (CRL) files. RBI's Certifying Authority will also provide a digital certificate for each subcomponent of RTGS (one for RTGS and one for PO). These certificates are stored on crypto devices.

It is important to note that the certificate containing the public key of the signer will be embedded in the signer information of the digital signature, so that there is no need to distribute public keys separately.

RTGS uses Class III Signing and Encryption certificates with SHA2/RSA 2048 bits key for both SFMS-MI (Thick Client) and Web-API. However, for PO, it uses Class-II signing User Certificate with SHA2/RSA 2048 bits key.

2.9.4 Security Features in Internet Banking: Security mechanism/ features which are available in Net Banking platform of large banks such as SBI and ICICI banks are mentioned in Annex I. Various security mechanism/ features deployed by Banks in their Internet Banking applications are given in Annex II. For various Security Measures proposed by RBI, please refer to Annex III.

2.9.5 Security Features in EMV Cards: The security features available in EMV Cards are mentioned in Annex IV.

Chapter III

Cross Country Experience in Implementing PKI

3.1 Various foreign countries have either implemented or in the process of implementing PKI in their various projects. The list of countries which have enabled PKI in their payment systems is given in Annex V.

3.2 Use of PKI in e-Banking Applications of other Countries

Electronic signature Laws in the U.S., Canada, U.K., Ireland, Australia, and New Zealand are technology neutral and allow for multiple technological solutions to provide the fundamental properties of integrity, authenticity and non-repudiation. In general, Laws in Latin American countries and Asia tend to favor digital signatures. Laws in European countries have favored digital signatures as well, however other types of e-signatures have also been implemented within European countries. Countries such as Germany have held tightly to the need for "Qualified Electronic Signatures". This requires digital signatures created using smart tokens, and with certificates issued from a qualified CA. The European Commission has recognized the issues that have been created with regard to cross-border interoperability. Distinct digital signature implementations and country specific certification regimes and politics pose interoperability issues. Authentication and electronic signature are two basic requirements in the Internet Banking. The Internet Banking scenarios of few countries are given below:

3.2.1 Sweden and Norway: A group of banks introduced an electronic identification based on PKI standard which is known as Bank ID. BankID is an unique electronic ID for secure identification and digital signatures. With BankID, individual can sign documents electronically, authenticate to a service or perform online payment transactions. This BankID consortium includes Danske Bank, Ikano Bank, Länsförsäkringar Bank, SEB, Skandiabanken, Sparbanken oresund, Sparbanken Syd, Svenska Handelsbanken, Swedbank and Nordea. BankID has been managed by a number of large banks for use by members of the public, authorities and companies. (Banks have introduced this option but it is not mandatory for the customers to use BankID).Banks act as Certification Authorities and at present there

are ten such banks. BankIDs have been issued to more than 7.6 million online banking customers. Out of this more than 4 million are active users. BankID is available on smart card, soft certificate as well as mobile phones, Ipads and other tablet computers.

In Sweden, BankID is a national solution for electronic identification and signing. The main objective of BankID was to meet requirements from the Swedish authorities to enable e-government and also meet security requirements for Internet banking. Majority of the Swedish banks are connected to BankID. Many services in the government, authorities, private companies and banks use BankID for electronic identification and signing. The services like online banking, e-trade, tax declaration, etc. are provided by the government, municipality, banks and companies using BankID. The BankID based digital identification in Sweden has a market share of 75 per cent. Sweden expects 250 - 300 million BankID transactions to be made during 2013. Since Bank IDs satisfy the requirements of advanced signature mentioned in the directives of European Union (EU) and Swedish law, BankIDs are legally binding.

In Norway, apart from a national ID or on smart cards, BankID is employed as an alternative authentication system. The Norwegian banking community adopted BankID for securing their e-commerce. The banks follow rigorous system for verifying customer's identity, enrolling users and issue them a BankID. The responsibility of issuing certificates lies with individual Banks. BankID certificates issued are stored either in central servers or in the SIM Card of individual. The BankID is stored on the customer’s mobile phone and can be used for online banking, Internet bill payments, and for obtaining online services from companies or government agencies. In Norway the mobile BankID uses PKI SIM cards, not soft certificates as is the case in Sweden. There are currently 3 million BankID users, out of which 3,50,000 users have registered for mobile version. In order to register user log in to online bank service using the BankId OTP authentication token and completes the Mobile PKI registeration as self service. BankID CA issues the qualified certificates for the user after the SIM application has generated the PKI key pairs (2048 bit RSA). The service is available from all five Mobile Network Operators in Norway. Service provider (almost 300) relying on BANKID include banks, financial, government and Municipal services and others. Other countries which have Mobile PKI services include Finland, Iceland, Estonia, Turkey and Moldova to name a few.

There are numerous countries with pilot services and some of which are now entering commercial phase.

In Norway and Sweden, individuals are having choice between a passwords-based solution and a PKI implementation for online transactions. The BankIDs in these countries are successful especially because the individuals were already used to log into their online banking environment and to make online payments.

3.2.2 China: China recognizes the privileged status of the digital signature in the variety of electronic signatures. Since 2005, PKI digital certificates have become the most effective security means for online transactions in China**.** Realizing the need for the issuance of e-signatures, the banking industry was proactive and created a joint venture of twelve banks, calling itself the China Financial Certification Authority ("CFCA"). The members issue digital signature certificate to the following for the use in the following categories

- bank-to-bank transactions;
- business-to-business transactions; and
- business-to-consumer transactions.

The underlying technologies involve three major components (1) asymmetric cryptography; (2) Public Key Iinfrastructure ("PKI"); and (3) a Certification Authority ("CA"). A CA should mandatorily be licensed by Government. The Ministry of Information Industry ("MII") is the body designated for the regulation of CAs in China. Prior to the issuance of certificate, the CA must inform the applicant about

- The conditions for the usage of the e-signature and the e-signature certificate
- Fees
- Subscriber liability to protect the private key and confidential information
- CA's responsibilities
- Other necessary Information.

To enforce the duties and liabilities of both parties, CA and subscriber should have a contract.

CAs are responsible for

1. creation, issuance, and management of e-signature certificates

2. confirmation of authenticity of e-signature certificates that the CA has issued;
3. Providing an online information search service pertaining to the current status of e-signature certificates the CA has issued.
4. CA must ensure that the certificate issued by them to a subscriber should contain
    - the name of the CA company
    - the name of the subscriber;
    - a serial number
    - the effective date and
    - the expiration date;
    - the e-signature verification data of the subscriber;
    - the CA's e-signature;
    - Other information that the Ministry of Information Industry may require.

Internet Banking transactions are authenticated and secured by Digital Signature enabled security in China. For detail, please see Annex V. In all these cases, the banks are acting as Registration Authority. USB Crypto Token is used for the storage of cryptographic credentials. The banking software is PKI enabled to use Digital Signature authentication and transaction signing. Such signatures are also legally valid in a court of law. PKI based Internet Banking is optional for the customers.

Established certificate

CFCA (China Financial Certification Authority) is responsible for issuance of certificates to users; these certificates are called Established Certificate. Established Certificate is a digital certificate generated and embedded by a CA organization in a secure storage medium such as Crypto Token. When a user applies for the certificate, a RA organization approves the identification of the user, associates the DN information of the certificate with the identification of the user, and sets up relationship with application systems database of the RA organization. The Established Certificate becomes effective when the identification of the user and the binding of the embedded certificate are both confirmed by the RA and CA organizations.

The binding refers to the establishment of corresponding relationship in a database between the DN information of the certificate and the identification of the user

(including but not limited to the name, type of ID, and number of the ID), so that the certificate can correspond to the user. The association refers to the establishment of corresponding relationship in a database between the DN information and the information of the RA organization, so that the certificate can be used in a specific RA organization.

These certificates are used by users for online transaction, authentication, confidentiality, integrity, and non-repudiation. CA generates and embeds established certificates in crypto Tokens and issue them to users through RA organizations.

CFCA has sold more than 5 million established certificates to more than 48 financial organizations, such as Bank of China, Huaxia Bank, etc. since 2009.

3.2.3 European System of Central Banks (ESCB-PKI): In Europe, as per the Directive 1999/93/EC of 13 December 1999 on a Community framework, electronic signatures framework has been established in several countries for digital authentication systems, promoting the free movement of electronic signatures and supporting services and products. This was mainly introduced to exchanges of information between beneficiaries of member states. Implementation of these requirements at national level has considered the three typologies of electronic signature defined in the Directive:

- Electronic signature;
- “Advanced electronic signature";
- **“**Advanced electronic signature" based on a qualified certificate and created by a secure signature-creation device.

Among EU member states, in respect of Authentication and Electronic Signature schemes, 17 of them deploy password-based solutions, 26 have implemented Public Key Infrastructures and one uses an Attribute Based Credentials solution. Seven European countries (the Czech Republic, Denmark, Estonia, Finland, Lithuania, Norway and Sweden) give their citizens the choice between a passwords-based solution and a PKI implementation.

The European System of Central Banks (ESCB) is composed of the European Central Bank (ECB) and the national central banks (NCBs) of 28 European Union (EU) Member States. European System of Central Banks (ESCB-PKI) follows and complies with the Decision of the European Central Bank laying down the framework for a public key infrastructure for the European System of Central Banks. The implementation conforms to the EU specification for an "advanced electronic

signature and are making use of security provided by PKI credentials on PC-connected smart tokens.

In order to counter the threats posed to the businesses, the ESCB-PKI delivers PKI services to the European System of Central Banks (ESCB) community such as strong authentication, digital signature and encryption. The beneficiaries includes ESCB shared applications and services meant for users of the ESCB and also for those of commercial banks and other external organizations that deal with the ESCB.

The ESCB-PKI complements the services provided by other Certification Authorities accepted by the ESCB. The main functionalities of the ESCB-PKI services can be summarised as follows:

- Verify the identity of a subject prior to the issuance of a certificate
- Create and sign certificates
- Process requests and reports related to the revocation status in order to determine the necessary actions to be taken
- Provide certificate revocation status to relying parties
- Recover private keys associated with encryption key usage certificates (only for internal users)
- Manage and distribute cryptographic tokens (e.g. smart cards)

3.2.4 HONG KONG: In Hong Kong, under the Electronic Transactions Ordinance (Cap. 553) (ETO), electronic or digital signatures have the same legal status as paper-based signatures. A signature requirement under the law can be satisfied by a digital signature supported by a recognized digital certificate for Government entities. For Non-Government entities, a signature requirement under the law can be met by any form of electronic signature including digital signature so long as it is reliable, appropriate and agreed by the recipient. The storage medium for Digital certificates can be Hong Kong ID Cards, user PCs or any other devices. The password protected user authentication credentials are widely used for online transactions.

Digital certificates are issued by certification authorities. Hong Kong Post Certification Authority is a recognized certification authority. Other commercially-run certification authority can also become a recognized certification authority on a voluntary basis, with the permission of Government Chief Information Officer. The Digital Signature Certificates issued by government recognized CAs are acceptable to the Government.

Several Government online services require the use of digital certificates. Digital certificates are accepted by banks, securities trading houses, e-merchants and other

services also. Hong Kong Post e-Cert is used in services such as secure e-mail, online government services, and online banking services. The information related to e-banking is given below.

BANK	USAGE OF CERTIFICATE ON ONLINE APPLICATION
Bank of Communications (Hong Kong Branch) www.bankcomm.com.hk	Net-Banking- services includes account details and electronic statement enquiry, foreign currency trading, time deposit management, online overseas fund transfer, CHATS, etc. Use e-Cert as a two-factor authentication tool for fund transfer to unregistered third parties and the online services
The Bank of East Asia, www.hkbea.com	Use e-Cert as two-factor authentication, online banking transactions, fund transfers to third-party accounts and designated bill payments.
Dah Sing Bank, www.dahsing.com	Use e-cert for online banking services, e-Deposit, fund transfer and bill payment services.
Shanghai Commercial Bank,www.shacombank.com.hk	Using e-Cert enabled fund transfer, remittance, bill payment, foreign exchange, fixed deposit placement and other transactions in a more secure way. Allow fund transfer and remittance to non-registered third-party accounts. Registration is not needed for bill payment to high-risk merchants. By using e-cert, one can avail fee discount on remittance, transferring of funds to other local banks

3.2.5 Korea: In Korea, 5 Accredited CA's have issued a total of around 20 million accredited certificates to users. Major PKI Applications are Internet Banking, Online Stock, Internet Shopping, Procurement, e-Gov Service. Electronic signature Act ensures the security and reliability of electronic documents. The usage of Digital signature certificates was made mandatory for the banking and trading systems, where security breaches occurred frequently in the process of identity verification. Efficient verification of identity was realized with the use of verification tools.

Government consults with Financial Supervisory Service (FSS) about using the certificates in the financial transactions. In 2002, the FSS made it mandatory to use

certificates in online internet banking. In 2003, FSS announced the mandatory use of Online Shopping and online trading. To promote use of accredited certificates, services were provided free of charge initially. Accredited certificates were provided free of charge and later on chargeable basis. The corporate certificates are now being charged. The requirements to be met by subscriber in respect of storage medium are as given below:

- A hardware protected secure storage with hardware cryptographic accelerator to generate and store private keys
- Digital signing and generation of a private key should be done inside the Token
- Private keys cannot be exported

Elsewhere in the world, more and more services providers are gradually recognizing, relying, and implementing PKI based authentication as the most reliable mechanism for authentication and signing of transaction with the additional benefit of legal binding. Recognizing the fact those customers of banks should not be the only ones to carry the burden of the consequences of criminal acts related to online banking, banks should provide robust security measures to protect their own interest and those of customers. Considering the increasing threats in online banking, the first criteria should be to provide effective protection to banks and its customers. Customers should be informed of risks, existing security measures and also given a choice of different methods of authentication to be able to select a system that matches their security requirements.

From the above, it is evident that Korea has made it mandatory to use PKI-based Digital Signatures in the online banking transactions for the purpose of authentication and transaction verification. However, countries like China, Sweden, Norway, European Union, Hong Kong etc have provided the user with the option to choose either the password-based two-factor authentication or PKI-based system for authentication and transaction verification.

In our case too, it would be important to make it mandatory for all the banks to create dual environment of password-based two-factor authentication and PKI-based system for authentication and transaction verification. High value transactions are

likely to be very vulnerable in the Internet environment. Therefore, it would be in the best interest for the banking sector as well as for the user to mandatorily use PKI-based solutions. It may be noted that the corporate sector already uses PKI-based submissions to various Government institutions like MCA and Income-tax.

The hurdle appears to be the verification of the user before the issuance of Digital Signature. Banks follow rigorous verification procedure prior to accepting the application for opening a bank account. It is recognized that the KYC process, which is very similar to verification process prior to issuance of the Digital Signature Certificate (DSC), is in practice in every Bank and our studies gives us confidence that this KYC process can be slightly reengineered to meet the requirement of verification prior to issuance of DSC. In view of this, DSC issuance can also be simplified.

Chapter IV

Feasibility in implementing PKI in all Payments System Applications

4.1 Current Scenario

The payment system applications RTGS, SFMS, NEFT, NDS and CTS are PKI enabled. This facilitates the banks to process and receive transactions using Digital Certificates that enhances the security of data travelling through network.

4.2 Present and Future Requirements

Most of the banks facilitate their customers to carry out financial transactions through online banking with the help of Internet. Online banking is presently authenticated through user id and password. The security and integrity of data, especially pertaining to financial transactions, travelling over the internet is critical. Banks have been adopting various approaches to facilitate the customers with one time password, SMS, Transaction specific passwords and grid card as Second Factor Authentication or combinations of these to add one more layer of security to critical online financial transactions. All these methods are prone to risk and cannot be used for establishing Non-repudiation and for assurance of data integrity and authenticity.

4.3 Digital Signatures for secure online transactions

The concept of non-repudiation is particularly important for financial or e-commerce applications.

4.3.1 Advantages of Digital Signatures

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable and cannot be imitated by someone else; A digital signature can be used with any kind of message, whether it is encrypted or plaintext. Digital signature can provide Transaction authentication, Transaction Verification and fraud detection in online banking application environment. The

implementation of PKI credentials (private, public keys) using secure hardware crypto tokens is capable of withstanding trojan attacks apart from other type of vulnerabilities. Thus Digital Signatures verifiable under the provisions of the IT Act 2000 provide the following three features:

(a) Authentication- Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.

(b) Integrity - In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest function.

(c) Non Repudiation – Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

4.3.2 PKI enabling Plan

- There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. For carrying out critical transactions like fund transfers need to implement robust and dynamic two-factor authentication through user id/password combination and second factor like (a) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) or (b) One Time Password (OTP) / dynamic access code through various modes (like SMS over mobile phones or hardware token).
- Subsequently, the PKI enabled environment can be extended to other categories including retail sector.

4.4 Signing

4.4.1 Client side components to enable customers to digitally sign their transactions

- Should support as many popular browsers and their recent versions
- Should support as many mobile devices as possible
- Components should be transparently downloadable to any computer/mobile device

4.4.2 Server side components to verify

- That the customer has signed with the valid certificate
- That the signature is mathematically valid and is of an acceptable format (PKCS#7/CMS)
- That the certificate is valid at the time of signing

4.4.3 Server side components to archive

- Signatures in a verifiable format for a specified period of time to suit legal requirements
- Associate signatures with the original transactions and preserve the signature context
- Copies of relevant CRLs and CA certificate chains
- Reports to provide facilities for auditing
- Signing keys that should have the key size at least 2048 bits
- SHA-2 is the minimum acceptable Digest
- Signature format should be PKCS#7 or CMS
- CRL should be checked before EVERY transaction
- The application should accept certificates from any of the Licensed Certifying Authorities

4.5 Requirements for PKI enablement

4.5.1 Available Approaches (1) – API

PKI features available as APIs for multiple languages including java, .NET and others. These may be directly integrated into the banking applications

(a) Benefits:

- Banking application remains one single entity

(b) Challenges:

- Banking application provider and PKI experts should be brought together for collaboration
- As the application evolves, PKI integration should be continuously revisited

- The existing application should be modified to provide for archival of digital signatures and continuous downloading of CRLs. Most APIs will not have this functionality natively

4.5.2 Available Approaches (2) –API and Server

- All PKI functionality is built into a server and a shell API is integrated into the application

(a) Benefits:

- CRL, Archiving and core signature functionality available in a packaged form
- Application remains monolithic

(b) Challenges:

- The bank will still need the support of API provider and the Internet Banking software provider to come together
- Application evolution is still a problem

4.5.3 Available Approaches (3) – Zero Touch

An inline server positioned between Internet Banking server and the customers to provide all PKI functionalities transparently

(a) Benefits:

- No need to tamper with the existing Internet Banking Application
- Applications can evolve without any need for additional integration
- The application need not be aware of PKI at all

(b) Challenges:

- Higher initial cost as additional hardware is introduced

4.6 Electronic Signature

Government of India has notified Information Technology (amendment) Act 2008 on 5th February, 2009. The Act substitutes words “Digital Signature” by words “Electronic Signature”. In particular, the act specifies the security requirements for the methodology to be adopted which will qualify the methodology to be accepted as “Electronic Signature”. Accepted methodology / process will be included in the second schedule of the act and will qualify as valid and legal means of producing

(and using) electronic signature. It may be mentioned here that the second schedule (page 19 of the Gazette) is empty and no implementation methodology is specified till date even after more than three years have passed since passing of the act.

The actual act is reproduced below for easy reference.
The amendment specifies that (page 3 of the Gazette)

"a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which---

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfils such other conditions which may be prescribed.

As per the Act (page 5 of the Gazette)

An electronic signature shall be deemed to be a secure electronic signature if—

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) *The signature creation data was stored and affixed in such exclusive manner as may be prescribed.*

As published in the Business Standard dated April 20, 2012 which said that the Income Tax department is looking at replacing Digital Signatures with Electronic Signature, the article also said that,

"the e-filler will be required to provide certain information on the income tax web site related to the previous year's return. If the information matches the details already available with the department, a unique Personal Identification Number (PIN) would be sent to the taxpayer through mobile phone and email. The taxpayer will have to enter this PIN at the time of e-filling the return".

It says that, the procedure which Income Tax department is planning to adopt is more or less compliant, in context of reliability of Electronic Signature as also Security of Electronic Signature (page 3 and 5 of the Act) and that the IT department has taken / is taking necessary clearances from Ministry of Information Technology as well as Finance Ministry. It may be noted that this methodology is cost effective and convenient.

As mentioned above, since the act has not included any methodology in the second schedule till date, a sub-group may be formed under the aegis of IDRBT. The sub-group may devise and recommend a methodology to the government for its inclusion in the second schedule. This methodology can be for specific use of bank customers and officers for use in payment system and bank applications.

The Group is of the view that at this stage, spread of awareness about DSCs is bit premature. As and when a methodology is specified in schedule 2, the same need to be included in the training sessions for payment systems and security related programs.

4.7 Various technologies used by banking sector for authenticating Online banking Transactions

Banks use various technologies for authenticating the user in online banking sites to protect the customers from identity theft. There is no specific pattern in respect of uniformity in use of authentication factor for online banking transactions.

4.7.1 Authentication factors used by banks

(a) Authentication factors used by Indian banks

Indian banks generally resort to the use of two factor authentication by seeking the username, password and OTP's to authenticate the users in online banking. Most of the banks in India resort to OTP's by means of SMS or hard tokens as a second factor of authentication. After logging into the net banking using id, password, for making any transaction, banks provide OTP's and ask password (same as login password or different) to provide security and reduce fraud. Some of the banks use OTP's as a second layer of authentication immediately after logging in by id, password and also use these OTP for doing transactions. It may be mentioned that this has been implemented based on the regulatory requirements.

(b) Authentication factors used by foreign banks

Foreign banks also use two factor authentications for online banking. Most of banks use the basic user name password and OTP's through a mobile device or OTP's provided by a security device or by a hard token. There are also instances of certain banks providing an extra layer of authentication by introducing a site key, by means of which the user-customer can identify the fake websites. Some banks provide hard tokens or security device for getting dynamic OTP's. Some banks use security tokens or mobile phones to generate these OTP's.

Exhaustive list of security features deployed by Banks in their Internet Banking Applications by SBI, ICICI and other Banks is given in Annex I and II. If the same channel is used for password and OTP authentication and service access it makes service susceptible to e.g. MITM attacks. Hardware OTP tokens do not improve the situation as the OTP code is sent back through the same channel as is used for service access. Using a second channel for the authentication will improve the security considerably. Mobile PKI can be used as a convenient and secure second factor authentication method utilizing the second channel for communication.

4.7.2 From the above, it can be seen that although there is no specific pattern in respect of uniformity in the use of authentication factors for online banking, the

approaches seem to follow a general trend which pertains to the use of two factor authentication.

4.8 Each of these technologies may not fully address all security concerns and come with its own limitations and vulnerabilities. Certain other features which could also be used for authentication are as follows:

(a) Identifiable pictures used as authentication factor

Identifiable pictures can also be used as password for authentication. These pictures can be used to generate a graphical password every time the user logins from a set of images stored in the client's computer. These images can act as one of the authentication factors (password).

Suggestions	Risk Mitigation	Ease of use	Cost	Strengths/Weakness
Mutual Authentication between the user and the Organization using identifiable features – such as specific pictures selected by the user customer.	Reduces the risks associated with phishing attacks.	User friendly and easy to use, remember and implement; there are no major overheads for the bank either.	Minor Costs for the banks; no cost implication for the customer	**Strength:** It provides an extra layer of user authentication and helps the user to identify the real website. **Weakness:** If the entire repository of information storing the user features is compromised or breached, then the factor loses its significance.
Challenge-Response Mechanism for high value transactions	Reduces phishing type attacks; incidents arising out	Easy to use by simply answering questions	Cost is involved at the bank end for	**Strength:** This can be used as an extra layer of authentication to reduce online fraud

which exceed a particular threshold level.	MIM attacks, and easy pattern recognition. Reduces the risk of Unauthorized access of accounts; and enhances safety of large value transactions.	and can be implemented for transactions which cross the threshold.	posing the challenge questions. No cost is involved as far as the customer is concerned .	and to improve security. **Weakness:** It becomes difficult for a customer to remember many challenge questions for different types of authentications. This may entice him to use the same question across multiple locations and not changing them at all for long periods of time. The weaknesses associated with passwords may apply to this factor as well
Multi factor authentication can be provided for the transactions which exceed a specific threshold level.	Reduces the risks related to identity theft and man in the middle attacks etc.	Easy to use.	As biometrics is used cost will be involved for the bank as well as the customer.	**Strength:** This provides a secure environment since multiple factors are used. **Weakness:** The customer has to navigate through multiple levels of complexity making it cumbersome. Challenges

				associated with rejection of certain factors such as biometrics for some target population groups do exist thus resulting in customer difficulties.

4.9 Current State of Online Banking Authentication Models

Two factor authentication methods verify users' identity based on something that they know (user name and password) and something else that they have. At present, authentication of online banking users is done using any or a combination of the above methods.

While multi-factor authentication looks like a foolproof solution under current circumstances, it is also true that even this will not stop an attacker forever, but merely slow him/her down.

The extent of authentication varies across banks, and depends on its security infrastructure as well as its risk tolerance guided by its risk policies. No doubt, two-factor authentication is more effective at preventing impersonation, but, as the recent breach of RSA's tokens showed, it is not 100 per cent foolproof.

This is the reason why banks take the additional precaution of restricting transactions in spite of implementing such security arrangements.

Certain minimum standards which need to be implemented by all banks in their online banking applications with suggestions as any of these techniques or method could be included in Schedule 2 of the IT Act

- A real time adaptive authentication and monitoring solution may be used to protect users from any unauthorized access by fraudsters. In case of any change in users normal transaction behavior an OTP may be sent on user's registered mobile number and after successful authentication of the same the

user may be allowed to transact further.

- URN authentication on payee addition.
- Change in mobile number through a written request at a branch or through any other secured mode.
- Grid based dual factor authentication.
- Enforcing Strong Password Policy
- Auto lock of user id on a specified number of wrong attempts of invalid user ids and passwords.
- Password expiry after a specified number of days
- Transaction monitoring mechanism to detect any suspicious transactions
- No use of emails in sending sensitive information like OTP or URN, Registered mobile number is the only available channel for the same.
- Virus scanners to prevent virus or Trojan on the systems used by the user.
- A second channel should be introduced for communicating the authentication request and response.

4.9.1 Password Security and Authentication Process: For the user password protection, the password should be shown as * to hide the exactly password in the password field. In application server, the data may be decrypted to get the original input password. After that the hash may be generated by strong hash algorithm. The application may compare and check the encrypted value present in the DB and may allow the user to proceed further as the hash of user password is stored as encrypted version. The authentication process should be transaction based rather than login-based.

4.10 To protect against more-sophisticated attacks, additional safeguards are required. Gartner research has discussed fraud detection (or transaction anomaly detection) services that enable risk-based authentication (RBA) and authentication complemented by fraud detection. The research points out that by implementing back-end fraud detection services, enterprises can minimize the inconvenience to customers caused by some authentication methods and at the same time increase their chances of catching fraudulent transactions.

According to Gartner research, the tools recognizing cross-industry fraud patterns could be the most effective solution as it can predict attempt to identity theft in advance. The research suggested that taking a cross-industry perspective would

enable better study of behavioral patterns to the credit markets to identify fraudulent usage of services. Banks could apply a combination of tools on their internal databases, external databases and introduce manual checks which would be a better option for banks because they can detect potential frauds.

MITM attacks can modify customer-generated transactions or generate new transactions; phishing/ pharming direct a customer to a bogus server that completes the connection to the bank's server. The man "in the middle" might actually be in the customer's PC: Trojan software can create a hidden browser session and generate transactions on the back of a legitimate strongly authenticated session — a "man in the browser" attack. Note that these are *not* attacks against the authentication method. They usurp or "piggyback" on legitimate user access to the bank's Web site and will succeed no matter how strong the authentication method. While the incidence of such attacks remains low, members expect that this will increase significantly within the next two to three years.

4.11 Using fraud detection services, enterprises can spot risky transactions and suspend them until they can verify the transaction with the user. This latter function is known as transaction verification.

Transaction verification provides two services:

(a) Data integrity: Protecting against unauthorized changes to the transaction by ensuring that changes to data are detectable.

(b) Data origin authentication: Verifying that the identity of the user submitting the transaction is as claimed. Hence, data origin authentication implicitly re authenticates the user.

By allowing the bank to verify individual transactions, transaction verification defends against bogus transactions created by MITM or Trojan attacks, or by simple account takeovers that got through the initial user authentication at login.

Transaction verification also provides an appropriate response when a fraud detection service identifies a transaction as risky — perhaps because it is of high value, is a transfer to a new account, or the customer's connection originates abroad. A common response would be to ask the users to reauthenticate, perhaps using a stronger authentication method than for their initial login. But transaction verification

adds more value — it confirms as correct the transaction details and simultaneously re authenticates the user.

Transaction verification can be provided in one of two ways:

- Interactive transaction confirmation
- Transaction authentication

4.11.1 Interactive Transaction Confirmation: Interactive transaction confirmation can be provided manually by live customer contact by phone or automatically via another channel, such as e-mail, voice telephony or text messaging.

4.11.2 Manual Interactive Transaction Confirmation:

(a) Strengths: This method requires no new technology.

(b) Limitations: It relies on current "knowledge-based authentication" to verify the identity of the customer, which is weaker than the authentication implicit in the automated transaction verification methods. A user may not be easily contacted by phone.

(c) Costs: As this method involves manual operator interaction with the customer, the per transaction costs can be very high. Any of the automated methods should be preferred; but banks must be able to support this method as a fallback.

4.11.3 Transaction Authentication: Transaction authentication uses an electronic signature to provide transaction verification. The signature may be either a Message Authentication Code (MAC) — based on secret-key cryptography — or a digital signature — based on public-key cryptography.

4.11.4 Transaction Authentication Using a Digital Signature: Digital signatures can be derived from PKI credentials held on a PC-connected smart token — or "soft" credentials held on the customer's PC — using suitable client software or on Mobile. The transaction details are hashed; that is, a hash value is calculated using a cryptographic hash function, and the hash value is encrypted with the customer's private key to create the signature. The signature is validated by the bank's systems — the bank generates its own hash of the transaction details, and it compares this against the customer's hash that it obtains by decrypting the signature with the user's public key.

As with a MAC, transactions with an invalid signature are rejected.

However, while digital signatures can protect against a true MITM attack (one "in the cloud"), because they are generated via the customer's machine, they can be compromised by a Trojan "man in the browser" attack. Flaws in Internet Explorer and in Windows (which mean other browsers, such as Firefox, aren't safe either) can allow a Trojan to send its own data to be signed, rather than customer's input values, so a bogus transaction can be seen by the bank as legitimate — it will have the right digital signature for that customer. This is true whether the signature is generated on the user's PC or on the card itself — it is the input data, not the signature generation, that is compromised. There's an irony here: PKI-based digital signatures are regarded as "strong." As the signing credentials are in the signer's sole control (if on a PIN-protected smart card/ e-token), digital signatures provide (in principal) a greater level of non-repudiation than MACs can and conform to the European Union (EU) specification for an "advanced electronic signature." Yet the signing process can be compromised if executed within browsers or operating systems (OSs) that are not immune to Trojans that intercept communications. OTP-token electronic signatures are based on a shared secret — that is, a credential not in the signer's sole control — and are weaker in principal than digital signatures. But in practice, they are more reliable because the MAC is generated completely onboard a trusted hardware token.

If digital signatures were generated wholly on an independent secure-hardware device for example, using a smart card / USB based token and handheld reader — they would be as resistant to Trojan attacks as token-generated MACs. However, no one currently uses this approach. As per the latest directives from the Controller of Certifying Authorities, the keys of subscribers are to be generated in a FIPS Federal Information Processing Standards) 140-1/2 Level 2 validated crypto device.

• *Strengths:* This method can be combined with authentication methods using PKI credentials with or without PC-connected smart tokens. It requires little additional activity by the user (more when the credentials are held on smart tokens). When using PKI credentials on PC-connected smart tokens, this method conforms to the EU specification for an "advanced electronic signature."

• *Limitations:* This method typically requires additional client software and may require a smart card reader, both of which may be OS dependent, may limit mobility,

and can attract significant support costs. Digital signatures generated on the user's machine may be compromised by Trojans or other malware.

• *Costs:* The costs for using PKI credentials in combination with a smart token are comparable with those for OTP tokens — and as with OTP tokens, these costs may be prohibitively expensive for transaction verification alone. Using "soft" PKI credentials held on the customers' PCs can be significantly less expensive, and may be viable for transaction verification alone, but it is not as secure. Banks risk difficult and costly technical support issues with customers whose software malfunction or fail.

4.11.5 Combining Transaction Verification with Other Safeguards: A bank might ask for transaction verification for every transaction, but it is more effective to ask for it only for "risky" transactions. This is particularly pertinent if transaction authentication via MAC is used because, more than the other transaction verification methods, it increases the burden on the users. A simple rule might be to ask for transaction verification for transactions above a certain monetary value. More complex requirements can be met by additional methods that incorporate transaction anomaly detection. However, banks and other service providers that decide to go this route will have to ensure that the user has a pre-enrolled method for participating in transaction verification.

Real time adaptive authentication: Banks may employ the real time adaptive authentication and monitoring system to dynamically use its logic to learn user behaviour and detect fraudulent activity. It may look at various client side parameters like behavioral profile, device-related profile, what sort of web browser is being used, the plug-ins used in the browser, etc and second set of values, which are based on the effect of a potential compromise of the function in question, such as letting a hacker log in as another user. Based on the risk profile additional means of authentication may be deployed in the real time.

Successful deployment requires the bank to find the right risk threshold at which to invoke transaction verification: Too high, and the incidence of fraudulent transactions will be unacceptably high (and the investment in transaction verification will have been wasted). Too low, and it will place an unacceptable burden on customers, deterring them from using the bank's Internet channel or — worst case — that bank.

From the customers' perspective, the ideal is for each customer to choose a preferred method for automated transaction verification through alternative means. However, few banks likely will be able to justify deploying more than one automated method. Most will in any case mandate one automated method and use manual interaction only for exceptional circumstances. There is value in habituating customers to a consistent way of interacting with the bank, so where a bank does offer more than one method, it may be able to differentiate them in some way; for example, cost or volume and value of the transactions.

In all cases, the key issue is that the bank ensures that risky transactions are verified. Although transaction verification is not yet demanded by regulators, it is used successfully by many banks. An emerging best practice. Complementary Security Methods Reduce Fraud and Strengthen Authentication"

On the face of it, banks apply such restrictions to protect their customers. There is also an element of self-interest in it as the banks would like to limit their own risk as well in the event of a transaction being initiated by someone who is not authorized to do so.

Tools of two-factor authentication have other limitations– token are expensive to produce, distribute and administer, and OTPs sent via SMS could take time to reach.

However, this is not the end of the road. While two-factor authentication looks like a foolproof solution under current circumstances, it is also true that even this will not stop an attacker forever, but merely slow him/her down. The implementation of security technology is neither a one-time effort, nor a guarantee of lifetime protection. What looks like a cutting-edge solution today will be standard fare tomorrow and out of date a few years thereafter.

This is an ongoing journey.

Chapter V

Implementation strategy by Banks: Short-term, Medium-term and Long-Term and Recommendations of the Group

5.1 PKI versus Non-PKI based payment systems

Reserve Bank has been promoting use of Public Key Infrastructure (PKI) technology in the electronic payments systems to secure a transaction from non-repudiation angle. Various electronic payments systems introduced by RBI and other agencies viz. Real-Time Gross Settlement (RTGS) System, National Electronic Fund Transfer (NEFT), CBLO, Forex Clearing, Government Securities Clearing, and Cheque Truncation System (CTS). In volume terms, these systems contributed 25.1 per cent whereas in value terms these systems contributed 93.7 per cent share to the total number of payment transactions carried out in the year 2012-13 (Table 2.2). Whereas non-PKI enabled payment systems contributed 75 per cent in volume terms bout only 6.3 per cent in value terms in the year 2012-13.

Of the non-PKI enabled payment systems, MICR Clearing and non-MICR clearing contributed 37 per cent and 10 per cent in volume terms (Chart 2.5) and 69 per cent and 25 per cent respectively in value terms (Chart 2.6). However, with the implementation of CTS system across the country, the cheque clearing will also be PKI enabled. Of the remaining, debit cards and credit cards transactions contribute 21 per cent and 18 per cent in volume terms (Chart 2.5) and 1 per cent and 2 per cent in value terms respectively (Chart 2.6) and ECS debit contributed 8 per cent and ECS credit contributed 6 per cent in volume terms (Chart 2.5) and 1 per cent and 2 per cent respectively in value terms (Chart 2.6).

5.2 Contribution of different Payment systems within PKI enabled payment systems

Chart 2.3 gives the contribution of various PKI enabled payment systems in terms of volume of transactions processed during 2012-13. It is observed that NEFT handles highest number of transactions processed among PKI enabled payment system and contributes 54 per cent followed with CTS payment system which contributes 37 per cent and RTGS system contributes 9 per cent of the total number of payment transactions happening through PKI enabled payment systems. Thus, all the three

payment systems together constitute nearly 100 per cent of volume of transactions processed in PKI enabled payment systems. Contribution of volume of transactions in other payment systems such as 'CBLO', 'Govt. Securities Clearing' and 'Forex' is negligible as their contribution is less than 1 per cent of the entire PKI enabled payment systems.

Chart 2.4 gives the contribution of various PKI enabled payment systems in terms of value of transactions processed during 2012-13. It is observed that value-wise RTGS system contributes 55 per cent (i.e. Rs. 676841 billion in the year 2012-13) among PKI enabled payment systems. PKI enabled Forex payment system constituting 21 per cent i.e. around Rs. 261170 billion comes in second position. The 3rd and 4th ranks are occupied by Govt. Securities clearing system and CBLO each constituting 10 per cent in terms of value of transaction processed in PKI based payment systems i.e. Around Rs. 120000 billion.

The contribution of PKI based NEFT system is only 2 per cent in terms of value of transaction i.e. Around Rs. 29022 billion.

Comparing Charts 2.3 and 2.4, it may be concluded that volume wise number of transactions processed in NEFT is the highest. However, in terms of value wise transactions processing in PKI enabled systems; RTGS is the highest.
Chart 2.5 gives the contribution of various Non-PKI based payment systems in terms of volume of transactions processed during 2012-13. It is observed that volume wise the highest number of transactions processed in Non-PKI based payment system is MICR Clearing i.e., 37 per cent. It is followed by Debit Card payment systems with 21 per cent, credit Cards with 18 per cent, Non-MICR Clearing with 10 per cent; ECS-Debit with 8 per cent and ECS-Credit 6 per cent respectively.

Further, both debit and credit cards together constitute 39 per cent of the entire Non-PKI based payment systems which exceeds the percentage of MICR Clearing.

Hence, the entire Card (debit and Credit) based payments systems together may be considered as a major non-PKI based payment system. The banks have been mandated to issue EMV cards (with chip and PIN) to certain category of customers

and for other customers, banks have been given option to either issue EMV cards or adopt Aadhaar biometric authentication as additional factor of authentication. Banks have been advised to enable infrastructure for both EMV and Aadhaar authtication.

5.3 Contribution of various Payment Systems within Non-PKI Enabled Payment Systems

Chart 2.6 gives the contribution of various Non-PKI based payment systems in terms of value of transactions processed during 2012-13. It is observed that value wise the highest number of transactions processed in non-PKI based payment systems is MICR Clearing i.e., 69 per cent. It is followed by non-MICR payment systems with 25 per cent.

Further, it may be noted that both MICR Clearing and non-MICR clearing together contribute 94 per cent of the entire non-PKI based payment systems in terms of value of transaction processed. However, with the implementation of CTS system across the country, the cheque clearing system will also be PKI enabled.

It may be noted that within non-PKI based payment systems, there are two categories of payment systems i.e. electronic and non-electronic payment systems. While MICR and non-MICR clearing payment systems are considered as non-electronic payment systems, the electronic payment systems are ECS-Debit, ECS-Credit, Card Payment systems such as Debit Card Payment Systems and Credit Card Payment system contributed only 6 per cent in value terms during 2012-13.

As seen from the above analysis, there is a feasibility of PKI implementation in electronic payment systems which may be proposed in the following order:

- Card Based Payment systems like Debit Card and Credit Card systems
- ECS payments systems such as ECS-Debit and ECS-Credit

However, banks at present use alternative technologies (i.e. other than PKI) in their online Banking Transactions which is discussed in detail in in Chapter IV.

RBI had issued guidelines via Circular DPSS (CO) PD No.1462/02.14.003 / 2012-13 dated 28.02.2013 on “Security and Risk Mitigation Measures for Electronic Payment Transactions” given in detail in Annex III. Accordingly, the issuing bank were advised to convert the older cards (the ones with the traditional magstrip) into EMV chip and pin enabled ones (this will be done for users who have used their cards

internationally at least once before). In respect of cards, not specifically mandated by the Reserve Bank to adopt EMV norms, banks may take a decision whether they should adopt Aadhaar as additional factor of authentication or move to EMV Chip and Pin technology for securing the card present payment infrastructure (Circular DPSS (CO) PD No.1164/02.14.003/2013-14 dated November 26, 2013).

5.3.1 PKI Implementation Strategy: PKI implementation strategy for system environment for authentication and transaction verification by banks may be carried out in three phases:

- Short-Term Implementation Strategy (phase-I)
- Medium-Term Implementation Strategy (Phase-II)
- Long-Term Implementation Strategy (Phase-III)

Phase	Description	Remarks
I	Implementation of DSC as an optional feature for certain role holders in Corporate Internet Banking for login as additional authentication.	To be implemented by Banks within 6 months.
II	Implementation of DSC as an optional feature for Authorizers in Corporate Internet Banking for authorizing the transactions.	To be implemented by banks within 12 months.
III	Implementation of DSC as an optional feature for Personal Internet Banking Users for authorizing the transactions.	To be implemented by Banks within 18 months.

Group suggests that i) the issues involved in the PKI based mobile transaction may be studied ii) promote the use of PKI enabled banking transaction keeping in view of higher penetration of mobile communication in India

5.4 Recommendations of the Group

The recommendations of the Group are as under:

(i) Customers should be informed of risks, existing security measures and also given a choice of different methods of authentication to be able to select a system that matches their security requirements.

(ii) Internet banking applications of all Banks should mandatorily create authentication environment for password-based two-factor authentication as well as PKI-based system for authentication and transaction verification in online Banking Transaction.

(iii) DBOD may review the KYC process in banks in view of issuance of Digital Signature Certificates (DSCs) for internet banking applications by Banks.

(iv) The major cost of the DSC is found to be the verification cost. Banks follow verification process of their customers, which is similar to the requirements of DSC application. CCA may examine to permit banks as RA for their customers for issue of DSCs.

(v) CCA to also examine exemption to all CAs from the circular/ guidelines issued by Government of India on physical verification of forms of subscriber as it is involved with banks regulated under Reserve Bank of India. Physical form verification should rest at Registration Authority (RA) level.

(vi) The following points need to be considered for Digital Signature Certificate (DSC) issued by CA

(a) Validity of DSCs may be increased from 3 years to 5 years

(b) the cost of DSC certificate to be brought down,

(c) Renewal of DSC to be made simple and same may be renewed with digitally signed prior to expiry. If DSC is expired, physical verification may be followed,

(d) CCA may examine issues of DSCs on various form factors

(vii) A group under the aegis of IDRBT may be set-up to study and Include alternative techniques/technologies used in Internet Banking Applications in Schedule 2 of the IT Act.

(viii) In Online banking transactions, banks should provide the option to its customers for enabling PKI for its online banking transactions as optional feature for all customers. Issues Involved in the PKI implementation in mobile environment need to be studied in detail keeping in view of indian context

(ix) Time-line for Implementation Strategy:

The implementation strategy for PKI-based system environment for authentication and transaction verification by banks may be carried out in three phases:

- Short-Term Implementation Strategy (phase-I)
- Medium-Term Implementation Strategy (Phase-II)
- Long-Term Implementation Strategy (Phase-III)

Phase	Description	Remarks
I	Implementation of DSC as an optional feature for certain role holders in Corporate Internet Banking for login as additional authentication.	To be implemented by Banks within 6 months.
II	Implementation of DSC as an optional feature for Authorizers in Corporate Internet Banking for authorizing the transactions.	To be implemented by banks within 12 months.
III	Implementation of DSC as an optional feature for Personal Internet Banking Users for authorizing the transactions.	To be implemented by Banks within 18 months.

(x) After infrastructure is enabled in all the banks a review may be taken for mandating digital signature for large value payments.

Annex I

Internet Banking Security features deployed by SBI and ICICI

(a) SBI

The following security mechanism is available currently on our Net Banking platform every time after login:

- ✓ Secure financial site, certified by VeriSign
- ✓ All communication between customer and the site is encrypted – with SSL encryption is in use.
- ✓ The address bar turns green after accessing the website indicating that the site is secured with an SSL Certificate that meets the **Extended Validation Standard**.(Supports all leading browsers e.g. Internet Explorer, Mozilla Firefox, Opera, Safari, Google chrome etc.)

For Retail Customer

1. User Id and Password for Login
2. SMS alert after accessing profile Section.
3. Mandatory SMS based OTP for addition of beneficiary
4. SMS alert on random times during beneficiary approval process.
5. Mandatory SMS based OTP transactions above Rs 10,000 for third party and above Rs 5,000 for merchant transactions.
6. SMS alert for every INB originated debit transaction on the registered mobile number.

For Corporate Customer

1. User Id and Password for Login
2. SMS based OTP or OTP through Hardware Token for Login
3. SMS alert after accessing profile Section
4. Maker Checker Concept for addition of beneficiary and performing transaction
5. Transaction Password to Authorize the transaction
6. Optional SMS based OTP to Authorize the transaction
7. SMS alert for every INB originated debit transaction on the registered mobile number.
8. Digital Signature Certificate (DSC) in lieu of SMS based OTP or OTP through Hardware Token for Login in

ATM Security features:

- **Proactive Risk Manager a fraud mitigation tool has been implemented in the Base24 ATM switch in Near Real time mode.**

  Proactive Risk Manager is a solution procured from ACI along with Base-24 Switch upgrade and can work in RT (Real Time) Mode or NRT (Near Real time) mode.

  This tool is for fraud monitoring for ATM, INB, Mobile Banking, CBS- Cheque Clearing.

- **Termination of transactions with wrong/invalid Amount, wrong PIN**

  Earlier if the customer was entering wrong Amount, Wrong Pin or Invalid amount then the ATM was prompting to re-enter the values, giving the customer a fresh cycle of 20 sec for re-entering the value.

  This was reading to frauds related to social engineering, therefore SBI is now terminating these transactions in case of invalid inputs.

- **For transactions through positive Balance File**
  1. **Declining of Balance Enquiry Transaction**
  2. **Stopping the printing of available balance**

PBF (positive Balance file) is maintained by ATM switch centre and is used for approving the transactions in case CBS is down.

In some cases for the transaction authorised through PBF, the customers were being shown older balance (sometimes inflated balance).

Therefore for the transactions authorised through PBF, SBI has stopped printing of Available Balance in the customer receipt.

- **Reduced screen time from 30sec to 20sec.**

  Time allotted to the customers for entering the value in any ATM screen was 30 sec and after this transaction will be timed out.
  As a security measure it was reduced this time to 20 sec.

- **Introduction of disabling cash retraction as advised by RBI.**
  This is as per the RBI guidelines, in this the cash will not be retracted back into the Rejected BIN.

- **Introduction of two digits Screen before entering the PIN.**
  This measure was taken to avoid the frauds related to keypad tampering.

After the insertion of ATM card and selection of language the customers will be prompted to enter 2 digits, by performing this activity the status of the Key pad will be checked

Mobile Banking Security features:

- 128 bit AES Encryption end-to-end.
- Three wrong MPIN entries block MBS for the day and two consecutive such blockage de-registers the customer.
- Maintaining of black-lists for user ID, mobile number and account numbers for fraud/doubtful transactions.
- Wrong User ID:
  - In application based – if wrong user ID entered 3 times, application is reset and payee information lost.
  - In MBS over USSD - session ends if wrong user ID is entered twice.
  - In MBS over SMSB – user is locked for a day if wrong MPIN is entered thrice.
- Mobile Number is validated with CBS before linking the primary account with a user id.
- WAP customers are authenticated using OTP as an additional layer of authentication.

(b) ICICI Bank Limited

Network Firewall Security

- Data kept in set of servers in a firewall zone which has no direct access to the outside world. These servers can only be accessed from outside through the Web server.
- The Web server is also in a separate firewall zone which has very restricted access to outer world.
- Clients having proper Login/Passwords can only access their respective data once the authenticity is verified by the Web server.

Entrust Security

- An SSL EV certificate is used.

- Authentication- by checking the Entrust server ID, customers can verify that the web site belongs to the Bank, and not an impostor.
- Message privacy- The secure socket layer encrypts all information exchanged between the web server and customers, using 2048 bit encryption to ensure that information cannot be viewed if it is intercepted by unauthorized parties

Other security measures

- Use of a real time adaptive authentication and monitoring solution which protects users from any unauthorized access by fraudsters. In case of any change in users normal transaction behavior an OTP is sent on user's registered mobile number and after successful authentication of the same the user is allowed to transact further.
- URN authentication on payee addition.
- Change in mobile number through a written request at a branch or through any other secured mode.
- Grid based dual factor authentication.
- Auto lock of user id on a specified number of wrong attempts.
- Password expiry after a specified number of days
- Transaction monitoring mechanism to detect any suspicious transactions
- No use of emails in sending sensitive information like OTP or URN, Registered mobile number is the only available channel for the same.

  Password Security and Authentication process: For the user password protection, the password will be shown as * to hide the exactly password in the password field.

  In application server, the data is decrypted to get the original input password. After that the hash is generated by MD5 hash algorithm. The application compares and checks the encrypted value present in the DB and allows the user to proceed further. It is because the hash of user password is stored as encrypted version.

Annex II

Exhaustive List of Security features deployed by other Banks

The following various security features are available in Internet Banking Applications for Other Banks:

1. User-ID and Password
2. OTP : One Time Password
3. Combination of User ID, Password and OTP
4. Profile change Alert
5. Adding new beneficiary alert
6. Cooling Period for adding beneficiary
7. Number of Transaction Limit (in a day)
8. Transaction Amount Limit (in a day)
9. Number of Transaction Limit (per beneficiary) i.e. Velocity Checks
10. Transaction Amount Limit (per beneficiary)
11. Maker Checker Concept for both Corporate and Retail Customer
12. To increase the transaction (both in number as well as in amount) limit, visit to branch is a must
13. Auto installation of Anti-Trojan software on the PC from where Internet banking is initiated
14. Anti-phishing Software
15. Site User Authentication
16. Personalized images
17. Phrases to customer
18. Risk based authentication
19. DSCs for corporate customers
20. Software token for retail customer
21. Hardware token for corporate customer
22. Grid Card Authentication
23. Change in Mobile Number by visit to a branch or any other secured mode
24. Call on increase in number of beneficiary beyond limit
25. Extract IP address
26. OTP on Change of IP address

27. Blocking and issuing a new Card i.e. in case of doubt about fraudulent transaction
28. Aggregate limit
29. NETSECURE with SMS (using the mobile phone), NETSECURE with WebPin (registration of a computer) or NETSECURE with 1-Touch (a small hardware device).

Annex III

Security Measures Proposed by RBI for Electronic Payment Transactions

With cyber-attacks becoming more unpredictable and electronic payment systems becoming vulnerable to new types of misuse, it is imperative that banks introduce certain minimum checks and balances to minimize the impact of such attacks and to arrest/minimize the damage. Accordingly, banks were advised to put in place security and risk control measures as detailed here under:

A. Securing Card Payment Transactions

(i) All new debit and credit cards to be issued only for domestic usage unless international use is specifically sought by the customer. Such cards enabling international usage will have to be essentially EMV Chip and Pin enabled. **(ii)** Issuing banks should convert all existing Magstripe cards to EMV Chip card for all customers who have used their cards internationally at least once (for/through e- commerce/ATM/POS) (

(iii) All the active Magstripe international cards issued by banks should have threshold limit for international usage. The threshold should be determined by the banks based on the risk profile of the customer and accepted by the customer). Till such time this process is completed an omnibus threshold limit (say, not exceeding USD 500) as determined by each bank may be put in place for all debit cards and all credit cards that have not been used for international transactions in the past.

(iv) Banks should ensure that the terminals installed at the merchants for capturing card payments (including the double swipe terminals used) should be certified for PCI-DSS (Payment Card Industry- Data Security Standards) and PA-DSS (Payment Applications - Data Security Standards).

(v) Bank should frame rules based on the transaction pattern of the usage of cards by the customers in coordination with the authorized card payment networks for arresting fraud. This would act as a fraud prevention measure.

(vi) Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS certification. This should include acquirers, processors / aggregators and large merchants.

(vii) Banks should move towards real time fraud monitoring system at the earliest.

(viii) Banks should provide easier methods (like SMS) for the customer to block his card and get a confirmation to that effect after blocking the card.

(ix) Banks should move towards a system that facilitates implementation of additional factor of authentication for cards issued in India and used internationally (transactions acquired by banks located abroad).

(x) Banks should build in a system of call referral1 in co-ordination with the card payment networks based on the rules framed at (v) above.

B. Securing Electronic Payment Transactions

The electronic modes of payment like RTGS, NEFT and IMPS have emerged as channel agnostic modes of funds transfer. These have picked up to a large extent through the internet banking channel and hence it is imperative that such delivery channels are also safe and secure. Some of the additional measures that need to be introduced by the banks could be as follows:

(i) Customer induced options may be provided for fixing a cap on the value / mode of transactions/beneficiaries. In the event of customer wanting to exceed the cap, an additional authorization may be insisted upon.

(ii) Limit on the number of beneficiaries that may be added in a day per account could be considered.

(iii) A system of alert may be introduced when a beneficiary is added.

(iv) Banks may put in place mechanism for velocity check on the number of transactions effected per day/ per beneficiary and any suspicious operations should be subjected to alert within the bank and to the customer.

(v) Introduction of additional factor of authentication (preferably dynamic in nature) for such payment transactions should be considered.

(vi) The banks may consider implementation of digital signature for large value payments for all customers, to start with for RTGS transactions.

(vii) Capturing of Internet Protocol (IP) address as an additional validation check should be considered.

(viii) Sub-membership of banks to the centralized payment systems has made it possible for the customers of such sub-members to reap the benefits of the same. Banks accepting sub-members should ensure that the security measures put in place by the sub members are on par with the standards followed by them so as to ensure the safety and mitigate the reputation risk.

(ix) Banks may explore the feasibility of implementing new technologies like adaptive authentication, etc. for fraud detection.

Annex IV

Security in EMV Cards

EMV stands for Europay, MasterCard and Visa, a global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card and transactions.

The India PKI Root hosts self-signed certificate (for signing CA Public Key Certificates and CRLs). A CA licensed by CCA, issue certificates to subscribers. Digital Signature Certificate profiles of PKI framework in India is a subset of X.509 (RFC 5280) standard. Digital signatures are legally valid provided with the corresponding signing certificate should be issued from licensed CA of India PKI hierarchy and signatures are applied as per the standards mentioned in the IT Act(RSA 2048, SHA2, PKCS7 etc).

It is understood that banking transaction also use EMV based Digital Signature functionality for authentication and securing transactions As of today the Digital signature certificates are issued to cards from CAs operated by Visa, MasterCard or their country partners which may not meet the legal requirements. The EMV use certificates based on the ISO international standard ISO/IEC 9796-2. CRLs are not signed. The issuer certificates sign the IIN of the issuing bank, its key and the expiry date of the certificate. The ICC keys (for DDA and CDA) sign the PAN, expiry date, key and a set of issuer and scheme mandated data that is variable in contents. The EMV specifications are set out as a toolbox to enable global interoperability in a secure environment. Most PC/SC compliant readers can read EMV cards. Readers for EMV chip card must be EMV L1 compliant, i.e., implement a particular subset of ISO 7816. The Card Network use a specific international programme managed by EMVCo for the security of the chip. For the security of the payment application they use the CAST programme. These are specific and tailored to the security needs of EMV. The EMVCo and CAST security evaluations programs are designed based on 20 years of chip security experience to give high assurance in the protection offered to the security of the assets contained in the chip including keys and PIN against an attacker with high attack potential. Typically card products are certified for CC (Common Criteria) or ITSEC at various evaluation levels to conform to the required

security levels. In EMV payments scenario, FIPS certifications are attained by the hardware HSMs used for key generation and storages. The current EMV standards are:

Asymmetric key size (max)	:1984 bit
Hashing Algorithms support	: SHA1
Storage of keys	: Use Hardware HSMs to store the keys.
Interface requirement for reading card:	PC/SC complaint Readers as per ISO 7816 standards

The PKI used on EMV Cards, containing the Public keys of the Issuing bank, is used to check the authentication of the card, i.e., to establish whether a genuine card is used in each transaction.

.

Annex V

PKI enabled Payment Systems in Various Countries

	Name of the Country	Name of the PKI enabled projects
1.	**Canada ***	- Customs Internet Gateway Project (CCRA) - Business Registration Internet Pilot (CCRA) - New Payroll Savings - Secure Website (Bank of Canada) - Internet Auction of Radio Licenses (Industry Canada) - Canada Education Savings Grants (Human Resources Dep. Canada) - Labour Market Development Agreements (HRDC) – access to central government databases - Secure Electronic Service Delivery (HC) - Network Security Strategy (INAC) -Large Value Transfer System (CPA) - Investment Review (IC) -Spectrum Radio Licensing (IC) -Secure Applications and Key Management Services (GTIS) -Secure Remote Access (GTIS) -Electronic Regulatory Filing (NEB) -Travel Management System (Statistics Canada)
2.	**Ireland ***	-Electronic information services; -Interactive electronic services (stand-alone); and, -Integrated electronic services. -Revenue Online Service (ROS)
3	**Netherlands ***	PKI-projects carried out within the areas of taxes, unemployment benefits, social care and "citizens' service card".

4	**United Kingdom ***	-personal tax filings -value-added-tax filings, -pay-as-you-earn tax filing by businesses, and -Some life event services such as birth of children and moving to a new location (address update which propagates across multiple agencies/uses).
5.	**United States ***	-Department of Defense (over 250.000 certificates issued, target is well over 4 million by 2002; high assurance with smartcards) -Federal Aviation Authority (ca 1.000 certificates issued, this will increase to ca 20.000 in 2000; software-based now, migrating to smartcards) -Federal Deposit Insurance Corporation (ca 4.000 certificates issued, over 7.000 in 2000) - NASA (ca 1.000 certificates issued, over 25.000 expected issued in 2000) United States Patent and Trademark Office (ca 1.000 certificates issued, expect ca 15.000 in 2000).
6.	**Finland ***	- the FINEID-card: electronic registration of change of address by Population Register Centre and Finnish Post -Application and financial services by the Finnish patent organization -Electronic tax filing service for companies and organizations -Employment services by the Ministry of Labour -Electronic application form by the Office of Education and social and welfare services / makropilot

7.	**Sweden ***	-business monthly tax declaration (tax administration) -starting a business (tax administration and company file) -sickness and parent benefits (social security administration) -employer and job seeker communication web sites (employment administration) -student loan system (central education grant agency) -real estate board's applications.
8.	**China**	

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	CHINA MERCHANTS BANK
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 10 Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : □ Certifying Authority or □ Registration Authority or □ No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2000
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://english.cmbchina.com/

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	Agricultural bank of China
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 12.3 Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token

5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2009
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.abchina.com/en/default.htm

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	China Construction Bank
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 6.0 Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2007
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.ccb.com/en/home/index.html

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	Bank of China
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 1.7Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token

5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2010
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.boc.cn/ebanking/

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	China Shanghai Pudong Development Bank
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 4Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2010
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.spdb.com.cn/chpage/c510/

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	China Huaxia Bank
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 1.5Million

4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2006
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.hxb.com.cn/english/index.jsp

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	China Minsheng Bank
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 5.8Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2006
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.cmbc.com.cn/index_en.shtml

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	Rural Credit Cooperatives Union of ShanDong

3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 2 Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2011
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.sdnxs.com/Site/Home/CN

Sl. No.	**Description**	**Details**
1	Name of the country	China
2	Bank Name	Shanxi Rural Credit Cooperatives Union
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 0.57 Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2012
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.10106262.com/

Sl. No.	Description	Details
1	Name of the country	China
2	Bank Name	Rural Credit Cooperatives Union of HeiBei
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 0.42Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2011
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.hebnx.com/

Sl. No.	Description	Details
1	Name of the country	China
2	Bank Name	Rural Credit Cooperatives Union of ZheJiang
3	Number of customers using PKI enabled online banking facility (number of crypto Tokens Issued)	Around 0.3 Million
4	Private key storage medium and standard prescribed for Key storage medium	USB Crypto Token
5	Role of Bank for issuing DSC to Bank account holders : • Certifying Authority or • Registration Authority or • No role	Registration Authority
6	Usage of PKI token : • Authentication or • Transaction signing or • Both	Both
7	Banks have PKI setup operational from when:	Year 2012
8	Whether PKI based Banking is Optional or Mandatory for the users	Optional
9	Whether signatures have legal validity:	Yes
10	Any Reference or website link or Document:	http://www.zj96596.com/

Annex VI

Recommendation of the Working Group headed by Shri G. Gopalakrishna on "Information security, electronic banking, technology risk management and cyber frauds"

The recommendations of the Working Group headed by Shri G. Gopalakrishna on Electronic Banking are as under:

ATM related measures:

- Every ATM may have an unique ID for easy reference, when required.
- Robust tuning and configuration of ATMs
- Cameras - ATM cameras should be so placed as to take a clear picture of the person doing the ATM operations and the lighting inside the ATM centre should facilitate the same. An additional small camera can also be explored by banks to take a snapshot of the customer picking up the money from the bin so as to assist customers when cash disbursement does not take place
- Time out for cash dispensed and swallowing of card (If cardholder has not collected the card in stipulated time)
- Firewall and Antivirus systems
- Security person at ATM location
- One person at a time to operate ATM.
- Controls relating to generation, transmission, loading and destruction of the ATM keys at the time of installation
- The message transmission between the ATM and Switch uses IPSec

Switch

- Card/Account authentication and validation using Switch.
- PIN based authentication using Hardware Security Module.
- Concept of daily limit for transactions to contain the risk in the event of card misuse.
- Activation of new card (PIN verification is must for first transaction at ATM: Card cannot be used for shopping at first time because PIN is not needed presently while shopping).
- Card is blocked if cardholder enters incorrect PIN a certain number of attempts, say three times; this blocked card is not usable for ATM and shopping transactions.
- Firewall

Card Management System:

• Controls relating to verification of card number.

Card based online transactions/E-Commerce:

• Secured e-commerce transactions through second factor authentication.

• Email alerts: After successful registration of the card, email alert can be sent on email-id entered during registration process.

Phone Banking:

- Suitable security measures for authenticating customers through phone banking.
- As a part of the security measures, no customer data like account number, status, etc. is stored in cache memory. Information provided by the customer on the IVR is sent to back-end host directly after encryption. Information received from the host is sent back to application and when the caller disconnects the call all the information inputted by the caller is deleted automatically.
- Critical details like change in phone details and address details should not be allowed through phone banking but only through a branch after due verification.
- From January 01, 2011, (circular RBI/2009-2010/420, DPSS No. 2303 / 02.14.003/2009-2010 dated April 23, 2010) RBI has made it applicable for providing for additional authentication/validation based on information not visible on the cards for all on-line card not present transactions including through IVR mode. Subsequently, deadline has been extended in view of the requests received by RBI.

Mobile Banking:

Technically speaking most of these services can be deployed using more than one channel. At present, Mobile Banking is being deployed using mobile applications developed on one of the following channels.

- SMS (Short Messaging Service)
- WAP (Wireless Access Protocol)
- Web Browser Based
- Mobile Application Client
- USSD
- IVR (Interactive Voice Response)

SMS (Short Messaging Service)

SMS uses the popular text-messaging standard to enable mobile application based banking. The main advantage of deploying mobile applications over SMS is that almost all mobile phones, including the low end, cheaper ones, which are most popular in countries like India and China are SMS enabled. An SMS based service is hosted on a SMS gateway that further connects to the Mobile service providers SMS Centre.

WAP (Wireless Access Protocol)

WAP uses a concept similar to that used in Internet banking. Banks maintain WAP sites which customer's access using a WAP compatible browser on their mobile phones.

WAP sites offer the familiar form based interface and can also implement security quite effectively. A bank's customers can now have an anytime, anywhere access to a secure reliable service that allows them to access all enquiry and transaction based services and also more complex transaction like trade in securities through their phone. A WAP based service requires hosting a WAP gateway. Mobile Application users access the bank's site through the WAP gateway to carry out transactions, much like internet users access a web portal for accessing the banks services.

Web Browser Based

For years, this solution has been shunned as slow, insecure and impossible to develop because of rendering. This is no longer the case, with the launch of high end phones with browsers supporting HTML and support of HTTPS this channel has now become secure and easy to use. The speed of download has also increased with GPRS and 3G coming into picture. In fact, after implementation of 3G it will be better than a standard internet connection on PC. The main advantage of this solution will be the bank can use the same infrastructure which is used for hosting its online banking solution. All the features of online banking can be extended to the customer with minimal efforts for customization of the site for mobile phones. As the solution is browser based, it will be accessible on both GSM and CDMA phones without any changes required.

Mobile Application Client

Mobile applications are the ones that hold out the most promise, as they are most suitable to implement complex transactions like trading in securities. They can be easily customized according to the user interface complexity supported by the mobile. In addition, mobile applications enable the implementation of a very secure and reliable channel of communication. One requirement of mobile applications clients is that they require to be downloaded on the client device before they can be used, which further requires the mobile device to support one of the many development environments like J2ME or BREW. J2ME is fast becoming an industry standard to deploy mobile applications and requires the mobile phone to support Java.

Unstructured Supplementary Services Data (USSD)

USSD stands for Unstructured Supplementary Services Data and is only available on GSM carrier networks. This communication protocol can be used for many mobile banking processes such as balance inquiry, money transfer, bill payment and airtime top up. USSD is similar to SMS technology only in that it too has data payload limits between 160 – 182 alphanumeric characters in a single transmission. However, USSD has a number of advantages over SMS technology such as unlike Short Message Service (SMS) messages, USSD messages create a real-time connection during a USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS

Interactive Voice Response IVR) service operates through pre-specified numbers that banks advertise to their customers. The most commonly used technologies across banking domain are Mobile Application Client, SMS, WAP and Web Browser Based Applications. Most financial institutions around the world have initiated basic mobile banking programs; others are contemplating more advanced and secure mobile banking options(Please refer RBI circular : RBI/2009-2010/420 RBI / DPSS No. 2303 / 02.14.003 / 2009-2010 dated April 23, 2010 on "Credit/Debit Card transactions- Security Issues and Risk mitigation measures for IVR transactions")

Security measures in Mobile Banking

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, is the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the bank.

The following aspects are among the security measures in respect of mobile banking :

- 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 a 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
- Two-factor authentication through mPIN or higher standard and end-to-end encryption of mPIN is desirable
- The mPIN shall be stored in a secure environment.
- Encryption of the data being transmitted over the air.

DEBIT CARD SECURITY MEASURES

- Personalization of card, generation of card through a specific algorithm and verification of the same at switch level.
- Delivering securely to customer after customer identification
- Controls around activation of card
- Blocking of cards after certain number of attempts with wrong PINs
- An instant SMS message is sent to the customer's registered mobile number with the bank on usage of card at any ATM, POS or E Commerce site.

Anti-skimming Measures:

'Card skimming' is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam.

The scammers try to steal a customer's details so that they can access the relative accounts. Once scammers have skimmed the card, they can create a fake or 'cloned' card with details from the skimmed card on it. The scammer is then able to run up charges on customer's account.

There are a variety of methods that may be employed to deter card skimming.

a. Awareness among consumers, branch personnel, and ATM service technicians can result in the detection of devices added to an ATM fascia. Visual clues such as tape residue near on a card reader may indicate the former presence of a skimming device.

b. Any servicing in onsite ATMs by external service personnel may be done in the presence of a bank official and in respect of off-site ATMs random checks by bank officials may be conducted.

c. All ATMs including offsite ATMs need to be manned by security guards

d. Physically inspecting the ATMs once a day. Best practices include doing a physical inspection during maintenance or cash replacement etc. by the bank or outsourced agency managing the ATM network for the bank.

e. Enforce standards for the appearance of ATMs. Adopt visual standards for ATMs so all ATMs should look alike.

f. Banks can ask the customers to provide / register their mobile numbers for sending an alert message for transactions done on alternate channels.

g. Looking for anomalous activity in customer accounts. Fraud detection software isn't foolproof, but it can detect some behaviours associated with a fraudulent transaction. Updated customer contact information is critical for quickly verifying the legitimacy of transactions or stopping fraud. Deploying fraud monitoring system especially in on-line environment may be difficult and expensive but will be useful in fraud detection and timely action.

h. The banks may consider dynamic scoring models and related processes to trigger or alert transactions which are not normal to improve preventive/detective capability. Study of customer transaction behavioural patterns and stopping irregular transactions or getting confirmation from customers for outlier transactions may be part of the process.

i. Network with other bank security / branch officers by participating in electronic security taskforces, or even casual cooperative agreements with other local banks, can help ensure that bank's branch managers / ATM officers are the first to know when a skimmer is targeting his area.

j. All ATM/Debit cards by default may be payable only in India, Nepal and Bhutan and if any card holder wants to use his ATM/Debit cards abroad he should either obtain separate PIN before he leaves India or international usage may be separately activated either online or through call centre.

k. Banks may also explore usage of biometric ATM cards to illiterate customers who may not be at ease while using ordinary ATM cards.

Further, the following anti-skimming solutions can be introduced:

Jittering: Jittering is a process that controls and varies the speed of movement of a card as it's swiped through a card reader, making it difficult – if not impossible – to read card data by the external device.

Chip-based cards: These cards house data on microchips instead of magnetic stripes, making data difficult to be cloned. It is recommended that RBI may consider moving over to chip based cards along with upgradation of necessary infrastructure like ATMs/POS terminals in this regard in a phased manner.

PIN based authorization: For debit / credit card transactions at the POS terminals, PIN based authorization system needs to be put in place (without any looping) in place of the existing signature based system and the non-PIN based POS terminals need to be withdrawn in a phased manner.

Internet banking:

i. Banks need to ensure suitable security measures for their web applications and take reasonable mitigating measures against various web security risks indicated earlier in the chapter.

ii. Web applications should not store sensitive information in HTML hidden fields, cookies, or any other client-side storage leading to compromise in the integrity of the data. Critical web applications should enforce at least SSL v3 or Extended Validation –SSL / TLS 1.0 128 bit encryption level for all online activity.

iii. Re-establishment of any session after interruption should require normal user identification, authentication, and authorization. Moreover, strong server side validation should be enabled.

iv. Banks need to follow a defence in depth strategy by applying robust security measures across various technology layers

Authentication practices for internet banking:

1) Authentication methodologies involve three basic "factors":

- Something the user knows (e.g., password, PIN);
- Something the user has (e.g., ATM card, smart card); and
- Something the user is (e.g., biometric characteristic, such as a fingerprint).

2) Properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents and are more difficult to compromise. The principal objectives of two-factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber attack mechanisms like phishing, key logging, spyware/malware and other internet-based frauds targeted at banks and their customers.

iii. The various major two- factor techniques/methodologies include the following:

Tokens: Tokens are physical devices (something the person has) and may be part of a multifactor authentication scheme. Three types of tokens are the USB token device, the smart card, and the password-generating token.

USB Token Device: The USB token device typically plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system. USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment. The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and there is no need for additional hardware is eliminated. However there are logistics issues in managing USB token devices for large retail customer base.

Smart Card: A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer. If

the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process. Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer. Thus may not be the preferred option for the bank as well as customers. In case an organisation security policy donot permit use of USB, the use of crypto smart card embedded in their organizational identity card to store their key-pairs may be helpful.

Password-Generating Token: A password-generating token produces a unique pass-code, also known as a one-time password (OTP) each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token, consisting of 6 or more alphanumeric characters (sometimes numbers, sometimes combinations of letters and numbers, depending upon vendor and model). The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor) into the banks website. The customer is authenticated if (a) the regular password matches and (b) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber fraudster from capturing and using OTPs gained from keyboard logging. However, it has the same logistics issues as highlighted in case of USB token devices.

SMS based One Time Password: In this method, the one-time password sent in an SMS to the user, is used in the bank's website. The user enters this code into the website to prove their identity and to authenticate transactions, and if the PIN code entered is correct, the user will be granted access to their account. This process provides an extra layer of online security beyond merely a username and password. These solutions can be used with any telephone, not just mobile devices. As with any out-of-band authentication method, SMS one time password methods are also vulnerable to man-in-the-middle attacks.

Biometrics: Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (something a person is). Physiological characteristics include fingerprints, iris configuration, and facial structure. Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification. Although end users should have little trouble using a fingerprint-scanning device, special hardware and software may need to be installed on the user's computer. At this junction it is not feasible to implement this technology for applications like Internet banking, Mobile etc at large scale as technology required to minimize error free authentication is very complex and expensive.

Digital Signature Certificates: Digital Client certificates are a PKI solution for enabling the user identification and access controls needed to protect sensitive online information. Digital certificates can also be stored and transported on smart cards or USB tokens. Each certificate can only be used to authenticate one particular user because only that user's computer/token has the corresponding and unique private key needed to complete the authentication process. However, there are issues with deployment and support of digital certificates.

In the Indian context, the following are some of the operational issues in case banks are required to act as Registration Authority / Certifying Authority:

a. The digital certificates issued could be used for any purpose other than internet banking transactions also.
b. If a customer has accounts with more than one bank, the customer may need to carry as many number of certificates as the number of accounts he/she is having in case bank chooses to issue bank / application specific certificates.
c. If Certifying Authority performs Registration Authority's role, cost involved may be high and if a bank is to act as a Registration Authority, it will give rise to logistic issues for maintaining documentation and other processes required as part of RA.
d. The costs involved may be high in acquiring digital certificates for customers/banks. Another critical factor would be who will bear the cost of DC as this will not only increase the transaction cost but will also make the channel less attractive and more expensive.
e. The responsibility for the safe custody of the digital certificates, backups, key compromise, timely renewal, accidental erase, etc. are a challenge with the customers. Further, banks would not be in a position to assume any onerous responsibilities in this regard.

f. Renewal of digital certificates at periodical intervals may be a repetitive job for banks or users.

g. There may be higher effort involved in installation of hardware or card reader at client's or customer's end.

h. Tremendous efforts would be required towards customer education and certificate helpdesk.

i. The need for suitable integration of PKI algorithms/technology with Internet Banking and provision for automated online validation and verification through linkage with Certificate Revocation Lists may be a key requirement.

j. A secure way of handling the digital certificates by customers is an issue and lapses in this regard may actually reduce overall security.

k. One of the most effective methods in combating MITM, MITB and similar session hijack attacks is by signing transactions. Till recently, the only way to sign transactions digitally was by using PKI. Now there are technologies available to sign transactions using software tokens which involve generating a transaction signature corresponding to the values of the transaction and then entering the signatures on the online application (which can also support non-repudiation in respect of the transaction.)

Further, it would not be ideal to mandate a specific technology for all online internet banking transactions.

'Electronic Signature' has been defined in Section 2(ta) of the IT Act (vide 2008 Amendment). However, in terms of the definition, the electronic techniques through which an electronic record is to be authenticated is to be specified in the Second Schedule. The 'techniques' have so far not been specified in the Second Schedule of the Act. Though the current legal position favours a specific technology for authenticating records/transactions i.e. asymmetric crypto-system and hash function, the amendment to IT Act has also allowed for 'electronic signatures' (which are to be notified by the Government in Second Schedule to the Act) where more options may be provided in future. There are also operational issues relating to widespread use of digital signatures as detailed earlier which require further assessment and clarification before being widely used. Hence, it is felt that any stringent prescription regarding digital signature or big bang approach to use of digital signatures may be counter-productive. Detailed discussion on the legal aspects, in this regard, is available in the "Legal issues" chapter later in the report.

Implementation of two-factor authentication and other security measures for internet banking:

1. In view of the proliferation of cyber attacks and their potential consequences, banks should implement two-factor authentication for fund transfers through internet banking.
2. The implementation of appropriate authentication methodologies should be based on an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or corporate/commercial); the customer transactional capabilities (e.g., bill payment, fund transfer), the sensitivity of customer information being communicated to both the bank and the volume of transactions involved.
3. Beyond the technology factor, the success of a particular authentication method depends on appropriate policies, procedures, and controls. An effective authentication method should take into consideration customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with other systems.
4. While not using the asymmetric cryptosystem and hash function is a source of legal risk, keeping in view the various methods and issues discussed above, for carrying out critical transactions like fund transfers, the banks, at the least, need to implement dynamic two-factor authentication through user id/password combination and second factor like (a) OTP/dynamic access code through various modes (like SMS over mobile phones or hardware token) or (b) a digital signature (through a token containing digital certificate and associated private key) (preferably for the corporate customers) .
5. To enhance online processing security, confirmatory second channel procedures(like telephony, SMS, email etc) should be applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank should take into account their efficacy and differing customer preferences for additional online protection.
6. Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the secure sockets layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security Web browsers to

clearly identify a Web site's organizational identity. It should, however, be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.

7. An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.
8. Changes in mobile phone number may be done through request from a branch only
9. Implementation of virtual keyboard
10. A cooling period for beneficiary addition and SMS and E-mail alerts when new beneficiaries are added
11. Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.
12. Risk based transaction monitoring or surveillance process needs to be considered as an adjunct.
13. An online session would need to be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.
14. By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute a true multifactor authentication.
15. As an integral part of the two factor authentication architecture, banks should also implement appropriate measures to minimise exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack. The banks should also consider, and if deemed appropriate, implement the following control and security measures to minimise exposure to man-in-the middle attacks:
    a. Specific OTPs for adding new payees: Each new payee should be authorized by the customer based on an OTP from a second channel which also shows payee details or the customer’s handwritten signature from a manual procedure which is verified by the bank.

b. Individual OTPs for value transactions (payments and fund transfers) :Each value transaction or an approved list of value transactions above a certain rupee threshold determined by the customer should require a new OTP.

c. OTP time window: Challenge-based and time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend user behaviour. It is recommended that the banks should not allow the OTP time window to exceed 100 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

d. Payment and fund transfer security: Digital signatures and key-based message authentication codes (KMAC) for payment or fund transfer transactions could be considered for the detection of unauthorized modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him, which means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

e. Second channel notification / confirmation: The bank should notify the customer, through a second channel, of all payment or fund transfer transactions above a specified value determined by the customer.

f. Session time-out: An online session would be automatically terminated after a fixed period of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.

g. SSL server certificate warning: Internet banking customers should be made aware of and shown how to react to SSL or EV-SSL certificate warning.

References

Bank of Communications (Hong Kong Branch) www.bankcomm.com.hk

Dah Sing Bank, www.dahsing.com

BankId Financial ID Technology Stockholm http://www.bankid.com/en/

BankId White paper, Norway
http://www.eurim.org.uk/activities/pi/BankIDWhitePaper.pdf)

CHINA MERCHANTS BANK, China http://english.cmbchina.com/

Agricultural bank of China http://www.abchina.com/en/default.htm

China Construction Bank http://www.ccb.com/en/home/index.html

Bank of China http://www.boc.cn/en/ebanking

Shanghai Pudong Development Bank http://www.spdb.com.cn/chpage/c510/

Hua Xia Bank http://www.hxb.com.cn/english/index.jsp

China Minsheng Bank http://www.cmbc.com.cn/ index_en.shtml

Rural Credit Cooperatives Union of ShanDong, China
http://www.sdnxs.com/Site/Home/CN

Shanxi Rural Credit Cooperatives Union, China http://www.10106262.com/

Rural Credit Cooperatives Union of HeiBei http://www.hebnx.com/

Rural Credit Cooperatives Union of ZheJiang, China http://www.zj96596.com/

Information Technology Act 2000, Department of Telecommunications, Ministry of Communications & Information Technology, Government of India.

Implementing Public Key Infrastructure in Government Aug 25, 2000: Report from an international meeting In Oslo, Norway, May 2000.

Request for Proposal (RFP) for Next Generation Real Time Gross Settlement System, Reserve Bank of India.

Reserve Bank of India Annual Report 2012-2013.

RBI Circular: RBI/2009-2010/420 RBI / DPSS No. 2303 / 02.14.003 / 2009-2010 dated April 23, 2010 on “Credit/Debit Card transactions- Security Issues and Risk mitigation measures for IVR transactions”.

RBI Circular DPSS (CO) PD No.1462/02.14.003 / 2012-13 dated 28.02.2013 on "Security and Risk Mitigation Measures for Electronic Payment Transactions"

RBI Circular DPSS (CO) PD No.1164/02.14.003/2013-14 dated November 26, 2013 on "Security and Risk Mitigation Measures for Card Present Transactions".

Shanghai Commercial Bank,www.shacombank.com.hk

The Bank of East Asia, www.hkbea.com

M V N K Prasad and S Ganesh Kumar "Authentication factors for Internet banking" IDRBT Working Paper No. 11 http://www.idrbt.ac.in/publications/workingpapers/Working%20Paper%20No.%2011.pdf