Use of PKI in Payment Systems in India and way forward

Dr. Anil Kumar Sharma
(anilksharma@rbi.org.in)
Adviser
Department of Statistics & Information Management
Reserve Bank of India

PKI enabled Payment Systems in India

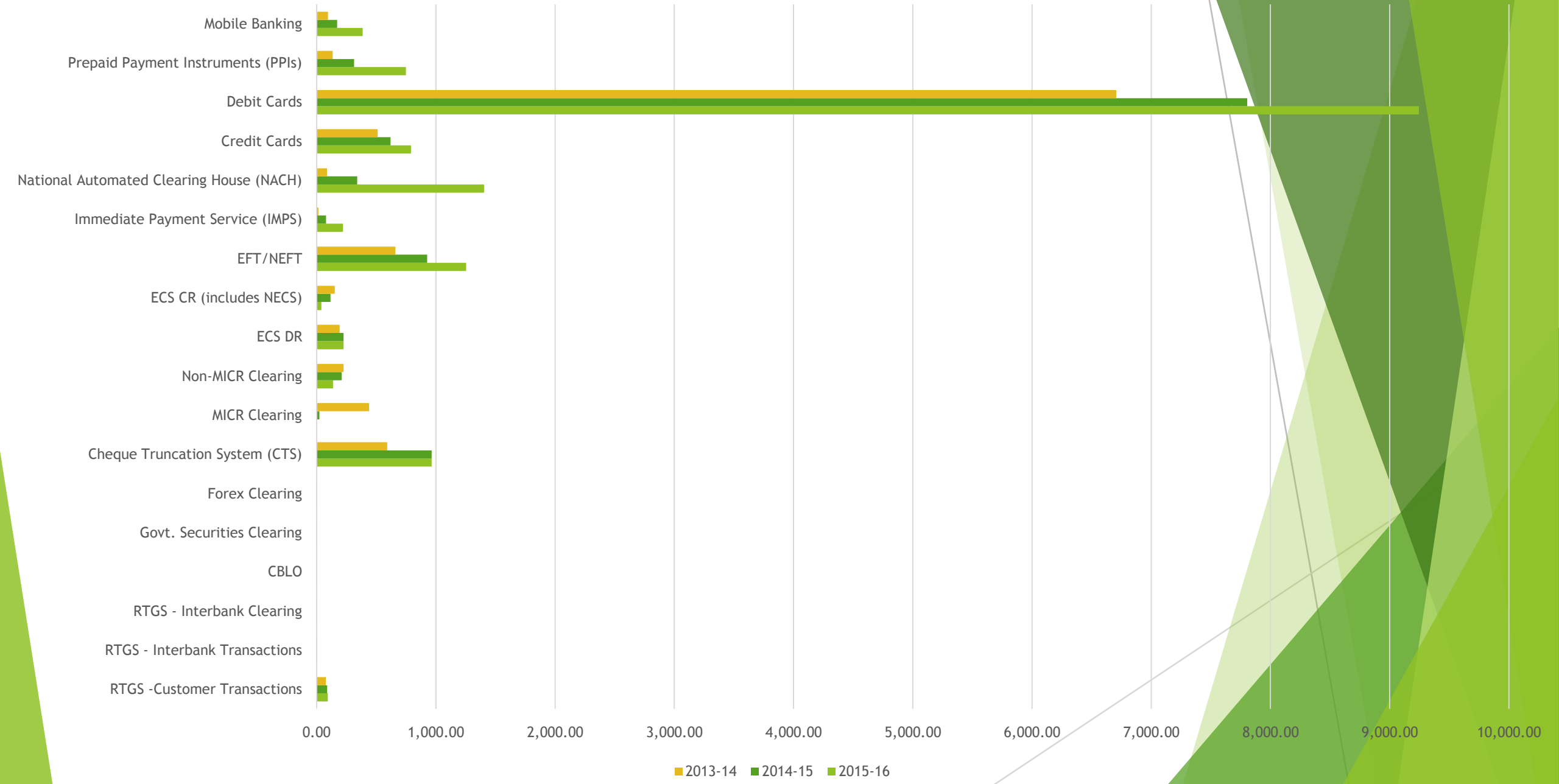
- Real Time Gross Settlement (RTGS)
- National Electronic Fund Transfer System (NEFT)
- Cheque Truncation System (CTS)
- Collateral Borrowing and Lending Obligation (CBLO)
- e-Kuber System (Security auction and settlement DvP)
- Forex settlement system
- NACH (it will replace NECS, RECS, ECS Debit,Credit)

Non-PKI Payment Systems

- MICR and Non- MICR clearing systems
- ECS – Debit and Credit Clearings
- Credit Cards and Debit Cards Payment systems
- Mobile Payment Systems (IMPS)

Payment System During 2015-16	Volume (Million)	% to Total	Value (Rs. Billion)	% to Total
RTGS	98.34	0.60	1,035,552	48.83
CBLO, Forex and G-Sec (CCIL)	3.12	0.02	807,370	38.07
CTS	963.92	5.85	70,235	3.31
Retail Electronic Clearing (ECS, NEFT, IMPS and NACH)	3,141.60	19.06	91,407	4.31
Paper Clearing (MICR and Non-MICR)	1,101.91	6.69	82,207	3.88
Cards	10,036.73	60.90	29,324	1.38
Prepaid Payment Instruments (PPIs)	747.96	4.54	490	0.02
Mobile Banking	386.55	2.35	4,018	0.19
Total	16,480.13	100.00	2,120,603	100.00

Payment System Transactions (Volume - in Millions):2013-14 to 2015-16



Payment System Value (Rs. Billion): 2013-14 to 2015-16

Payment Systems Statistics

- About 94.5 per cent of total value of payment systems are being settled using PKI enabled payment systems
- However, only about 25.5 per cent of transactions (volume) are settled using PKI enabled payment systems
- About 61 per cent of transactions are card related payments which are being settled without PKI enabled systems. These are low value transactions.

PKI Implementation in RTGS – a brief

PKI in RTGS

Three different classes of client systems –

Thick Clients Security

The messages received by the RTGS from the thick clients connected to the INFINET network are digitally signed

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

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 ensures that the owner of the certificate used to sign the incoming message is also the debited party indicated within the message‘s details.

RTGS: Web-service API Clients Security

- The client application must connect to the RTGS using HTTPS protocol only.

  For this, the client application must have access to a digital certificate and recognized by the RTGS.

- 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.

RTGS: Browser-based Clients Security

- Each user must have an individual certificate 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 has a profile defined in the RTGS that describes the system functions the user has access. These functions are 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.

User security Management:

- All users of RTGS and PO are authenticated based on a digital certificate issued by Certifying Authority, a username and a secret password and user certificate serial number.
- The certificate is stored securely on token device along with the private and public keys. The user account definitions along with their passwords and certificate serial numbers are 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.) has been enforced to all users according to RBI internal regulations. The system also forces the users to periodically update their passwords, without reusing the same values.
- User Management is the responsibility of the admin of respective participants.
- RTGS uses Class III Signing and Encryption certificates with SHA2/RSA 2048 bits key for both SFMS-MI (Thick Client) and Web-API

Way Foreword

- Low value transactions are about 74.5 per cent in volume which are being processed using Non-PKI based Payment system
- These systems are having security features like OTP, PIN, etc. Do we need to extend coverage of PKI to these transactions?
- PKI provides technical infrastructures which need to be supplemented by IT security policy and practices. Are banks aware of various threats and what precautions to be taken care beyond PKI?
- Need to increase IT security awareness and lot of threats can be avoided if proper practices are put in place.
- IT Security features needed to be enhanced for Mobile instrument as there is huge potential of increase of mobile payment transactions in future.