Securing Banking Eco-System Through PKI
About IDRBT

• Institute for Development and Research in Banking Technology (IDRBT) is an Autonomous Institution established by Reserve Bank of India in March 1996 for Research and Development in Banking Technology
Technology Initiatives by IDRBT

- INdian FIancial NETwork (INFINET)
- Structured Financial Messaging System (SFMS)
- Certifying Authority (CA)
- National Financial Switch (NFS)
- Other Activities
  - Research & Development in Banking Technology
  - Training programs for banks
  - Academic programs – PhD, PGDBT etc.
  - Technology consultancy to banks
About IDRBT Certifying Authority

• Functioning as a Certifying Authority since August 2002

• Caters exclusively to the Banking and Financial sector, primarily to Members of Indian Financial Network (INFINET)

• Service to about 700 organisations

• Issued over 300000 Digital Certificates
PKI and Payment Systems

• IT Act 2008 recognizes electronic signature as legally valid
• RBI proactively promotes use of PKI in electronic payment systems for security
• Uses in its payments systems
• and internal applications
Payment Systems/Infrastructure

• Next Generation Real Time Gross Settlement System (NG-RTGS)
  • Large value payment system, since 2004
• National Electronic Fund Transfer (NEFT)
  • Retail funds transfer system introduced in the late 1990s
  • Enables an account holder of a bank to electronically transfer funds to another account holder with any other participating bank
• Structured Financial Messaging System (SFMS)
• NPCI Applications
  • UPI, NACH, IMPS, Cheque Truncation System (CTS), AEPS
• Card Networks
• POS
• ATM
• Mobile Wallets/PPIs
Growth of Digital Transactions

• The payment and settlement systems recorded a robust growth

• During 2018-19, volume and value grew at 54.3 per cent and 14.2 per cent respectively

• The share of electronic transactions in the total volume of retail payments increased to 95.4 per cent in 2018-19, up from 92.6 per cent in the previous year
## Payment System Indicators – Annual Turnover

<table>
<thead>
<tr>
<th>Payment System</th>
<th>Volume (million)</th>
<th>Value (₹ billion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. RTGS</td>
<td>107.8</td>
<td>124.4</td>
</tr>
<tr>
<td>2. NEFT</td>
<td>1,622.1</td>
<td>1,946.4</td>
</tr>
<tr>
<td>3. IMPS</td>
<td>506.7</td>
<td>1,009.8</td>
</tr>
<tr>
<td>4. UPI</td>
<td>17.9</td>
<td>915.2</td>
</tr>
<tr>
<td>5. NACH</td>
<td>2,057.3</td>
<td>2,503.3</td>
</tr>
</tbody>
</table>

Source: RBI
PKI Usage

• NEFT/RTGS
  • Message signing and encryption

• Forex Clearing, Govt. Securities Clearing Systems

• Unified Payments Interface (UPI)
  • Secure communication between UPI and PSPs/Banks
  • APIs signed and verified by PSP/Bank
  • Secure credentials are encrypted using public key by PSP
PKI Usage

- Bharat Interface for Money (BHIM)
  - Mobile app to BHIM Web server secure communication (SSL)
  - PSP to UPI secure Communication

- Cheque Truncation System (CTS)
  - Signing of files

- National Automated Clearing House (NACH)
  - Digital Signing of File
New Applications of PKI

• Submission of reports by banks

  • Two factor authentication for Internet banking applications
  • Banks to provide option for the customers to use PKI for authentication
  • PKI for transaction verification

• Use of ECC by NPCI

• Use in email – Issues with mobile apps
Thank You