Biometric, Smart Card & POS
- Interoperability & Standards
Glossary

- **ICT (Information & Communication Technology):** ICT is the convergence of IT and CT.
- **IT (Information Technology):** Technology that helps in capturing, storing, processing, retrieving and communicating information.
- **CT (Communication Technology):** The technology that helps in transmitting/communicating information/data on a network.
- **PSTN (Public Switched Telephone Network):** Landline telephone connection provided by a service provider like BSNL, Reliance, Tata Indicom etc.
Glossary

• **CDMA (Code Division Multiple Access):** This is a type of mobile technology in which SIM card is not used (TATA/RELIANCE) not like GSM (AIRTEL/IDEA). They require special type of handsets as CDMA has different frequency 600 mega hertz to 900 mega hertz and the GSM uses 900 MHz to 1800 MHz. The CDMA is safe speedy and clear and has long range.

• **GSM (Global System for Mobile communications):** World’s most widely used cell phone technology. Cell phones use a cell phone service carrier’s GSM network by searching for cell phone towers in the nearby area.

• **Smart card:** A smart card is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data, used for telephone calling, electronic cash payments, and other applications, and then periodically refreshed for additional use. (Contact and Contact less cards)
Glossary

- **POS (Point-of-sale) terminal**: A point-of-sale (POS) terminal is a computerized replacement for a cash register. Much more complex than the cash registers of even just a few years ago, the POS system can include the ability to record and track customer orders, process credit and debit cards, connect to other systems in a network, and manage inventory.

- **Interoperability**: Interoperability is the ability of a system or a product to work with other systems or products without special effort on the part of the customer.
Challenges / Issues

- Business Correspondent Related
  - Agency Risk
  - Reputation Risk
- Process Related
  - Enrollment and Card Production
  - Updation of new products
  - Cash Management
- Technology Related
  - Lack of standards & Interoperability
  - Competing Technologies
  - Training and Maintenance Issues
- Staff Related
  - Lack of Awareness
  - Need to open Large number of Accounts
- Cost
Challenges / Issues

• Minimum Standards for identifying and engaging a BC
• Methodology and Standards for Data Storage on Cards
• Finger print Storage and Retrieval Standards
• Risk Mitigation Criteria
• Authority to define Standards
Selection of Technology

• **Secure**
  ✓ Supports two factor authentication (Card & Biometric)

• **Scalable**
  ✓ Capability to handle multiple products & Services

• **Reliable**
  ✓ Transactions are secure and ensures non-repudiation

• **Flexible**
  ✓ Supports multiple connectivity and power options

• **Interoperable**
  ✓ Customers can transact from the branch or other BCs

• **Robust & Upgradable**
  ✓ Supports contact, Contact less and mag-stripe interfaces

• **Cost Effective**
Device Characteristics

- Card Based Device
- Support for Fingerprint Authentication
- Redundant Power Sources for continuous operation
- Mobile and easy to carry
- Voice Guidance in Local Language
- Support for multiple communication Channels
- Capability to support multiple power sources
- Device stores only minimal data
- Ability to handle multiple products and services
- Receipt printing
- Scalable
Biometric

- **Biometrics** comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.
The basic block diagram of a biometric system
Different Biometrics

- Finger print
- Face
- Iris
- Facial Thermogram
- Palmprint
- Voice
- Signature
Only once during the existence of our solar system will two human beings be born with two similar finger makings

Two like fingerprints would be found only once every $10^{48}$ years
– Scientific American 1911.
Fingerprint

- It is a pattern of ridges and furrows on the tip of each finger.
- Patterns are created by the inked impression on the paper or through digital images captured from the compact sensor.
- Matching is a process of comparing the minutiae patterns.
Fingerprint

crossover
core
bifurcation
ridge ending
island
delta
pore
Advantages:
1. High accuracy
2. Equipment is cheap
3. Easy to use device

Disadvantages:
1. Fake fingerprints can easily be created.
2. Liveness detection is a great problem.
3. Most devices are not able to enroll small percentage of users due to cuts and bruises on finger.
Biometric standards

• minimum requirements for image acquisition should be the Setting Level 31 as defined in the ISO/IEC 19794-4

<table>
<thead>
<tr>
<th>Setting level</th>
<th>Scan resolution pixels/centimeter (ppcm)</th>
<th>Scan resolution pixels/inch (ppi)</th>
<th>Pixel depth (bits)</th>
<th>Dynamic range (gray levels)</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>197</td>
<td>500</td>
<td>8</td>
<td>200</td>
<td>EFTS/F</td>
</tr>
</tbody>
</table>
Biometric standards

• image grayscale shall be captured using atleast 200 grey levels
• finger image data field should contain the uncompressed – bit packed grayscale image data formatted and recorded in accordance with the uncompressed – bit packed image compression algorithm
• Image size 250x300 pixels
• All ten fingers image data storage in the server
• Minimum number minutiae for enrollment are 30 - 35 and for verification are 25 – 30 (max 60).(Recommended 16/12)
• The maximum number of minutiae to be sent to a card is implementation dependent and related to:
  – transmission time
  – memory resources
  – execution time
  – security aspects
• Threshold Value
  – Required False Acceptance Rate
  – Required False Rejection Rate
  – Matching conditions,
  – The amount of minutiae enrolled
  – The amount of minutiae presented
  – Strength of function.
• Retry Counter (5-15)
A **smart card**, **chip card**, or **integrated circuit card** (ICC), is any pocket-sized card with embedded integrated circuits. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps dedicated security logic. Microprocessor cards contain volatile memory and microprocessor components. The card is made of plastic, generally polyvinyl chloride, but sometimes acrylonitrile butadiene styrene or polycarbonate.
Contact smart card

- Contact smart cards have a contact area of approximately 1 square centimetre (0.16 sq in), comprising several gold-plated contact pads. These pad provide electrical connectivity when inserted into a reader.[6]
- The ISO/IEC 7816 series of standards define:
  - physical shape and characteristics
  - electrical connector positions and shapes
  - electrical characteristics
  - communications protocols, including commands sent to and responses from the card
  - basic functionality
- Cards do not contain batteries; energy is supplied by the card reader.
Standardization

- The Smart Card Numbering Scheme
- The Smart Card Operating System
- The FI Customer Card Data Architecture
- The FI Terminal Operator Card Data Architecture
- The Terminal Functionality Specification
- Key Management System
Card Numbering Scheme

• Length of the card number: 19 Digits
• 9 – National Scheme
• 356 – Country Code
• XXXX – Bank Identification Number*
• XXXXX – Branch Code*
• XXXXX – Card Serial Number*
• X – Checksum (Luhn’s algorithm)
Smart Card Hardware Specification

- Microcontroller based
- Interface: Contact or Contact less. In case of contact interface it must comply to ISO 7816 (T=0 or T=1). In case of contact less it must comply to ISO 14443 (Type A or Type B).
- EEPROM size: 32 or 64 K byte
- Size and material of card body: Size must comply to ISO 7816 Part 1 standard. Material of card body can be PVC, PET/PETG, Polycarbonate or composite plastic made up of combination of any of these plastic materials based on the required card life span.
- In case of contact interface card, it must comply to ISO/IEC 7816 - 1,2 &3.
Smart Card Hardware Specification

• In case of contact less interface card, must comply to ISO/IEC 14443-1,2&3
• Supply voltage 3V nominal (in case of contact)
• Transport protocol: T=0 or T=1 (in case of contact interface); T=CL (in case of contact less interface)
• Minimum 10 years data retention
• Min 300,000 E2PROM write cycles
• Operating ambient temperature range –25oC to +70oC
• In case of contact interface card, the card OS must comply to SCOSTA 1.2b or SCOSTA-CL 1.2 with all their addendum and errata
Terminal Functionality Specifications

- Minimal Functionality that should be supported
  - DEPOSIT
  - WITHDRAWAL
  - BALANCE ENQUIRY
  - MINI STATEMENT
- Full Functionality (optional)
  - FUNDS TRANSFER/ REMITTANCES
  - BILL PAYMENTS
  - LOANS
  - INVESTMENTS (TERM DEPOSITS, FDS, RDS ETC.)
- Extended Functionality
  - MUTUAL FUNDS
  - INSURANCE (LIFE, HEALTH, CROP, ETC.)
  - PENSIONS
Smart Card Security

• Mutual authentication between card and terminal using Triple-DES.
• Cardholder verification using biometric authentication – the fingerprint stored on the card is to be encrypted to prevent misuse. The fingerprint images are to be stored in WSQ format.
Data Storage Architecture Map of Customer Card

Data Objects Defined in table DO1.

Data Objects Defined in table DO2.

EF7 F104  EF8 F105
## Master File

<table>
<thead>
<tr>
<th>S.No</th>
<th>Data element</th>
<th>Description</th>
<th>Tag</th>
<th>Size (Byte)</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CN</td>
<td>Card No</td>
<td>‘CE’</td>
<td>19</td>
<td>N</td>
</tr>
<tr>
<td>2</td>
<td>NAME</td>
<td>Customer Name</td>
<td>‘CI’</td>
<td>30</td>
<td>AN</td>
</tr>
<tr>
<td>3</td>
<td>MOTHER NAME</td>
<td>Mother’s Name of Cardholder</td>
<td>‘C5’</td>
<td>30</td>
<td>AN</td>
</tr>
<tr>
<td>4</td>
<td>SEX</td>
<td>Gender</td>
<td>‘C9’</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>5</td>
<td>DOB</td>
<td>Date of Birth</td>
<td>‘CA’</td>
<td>4</td>
<td>B</td>
</tr>
<tr>
<td>6</td>
<td>LP</td>
<td>Language Preferences</td>
<td>‘E1’</td>
<td>2</td>
<td>AN</td>
</tr>
<tr>
<td>7</td>
<td>PI</td>
<td>Primary Identification</td>
<td>‘E2’</td>
<td>2</td>
<td>N</td>
</tr>
<tr>
<td>8</td>
<td>PID</td>
<td>Primary ID</td>
<td>‘C0’</td>
<td>20</td>
<td>N</td>
</tr>
<tr>
<td>9</td>
<td>CID</td>
<td>Card Issue Date</td>
<td>‘CD’</td>
<td>4</td>
<td>B</td>
</tr>
<tr>
<td>10</td>
<td>UID</td>
<td>Unique ID</td>
<td>‘CB’</td>
<td>20</td>
<td>N</td>
</tr>
</tbody>
</table>
# Dedicated File

<table>
<thead>
<tr>
<th>Application name</th>
<th>DF name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saving Account</td>
<td>F1 00</td>
</tr>
<tr>
<td>Cash Credit</td>
<td>F2 00</td>
</tr>
<tr>
<td>Demand loan</td>
<td>F3 00</td>
</tr>
<tr>
<td>Remittance</td>
<td>F4 00</td>
</tr>
<tr>
<td>Insurance</td>
<td>F5 00</td>
</tr>
<tr>
<td>Term Deposit</td>
<td>F6 00</td>
</tr>
<tr>
<td>Recurring Deposit</td>
<td>F7 00</td>
</tr>
<tr>
<td>SHG Savings Bank</td>
<td>F8 00</td>
</tr>
<tr>
<td>Overdraft</td>
<td>F9 00</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Address</td>
<td>Cardholder Address</td>
</tr>
<tr>
<td>LCN</td>
<td>Linked Card Number</td>
</tr>
</tbody>
</table>
## Data table of the Finger Print Image EF

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Tag</th>
<th>Max size</th>
<th>Data type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finger Image 1</td>
<td>Finger Image 1</td>
<td>‘D4’</td>
<td>12288 (12 Kb)</td>
<td>AN</td>
</tr>
<tr>
<td>Finger Image 2</td>
<td>Finger Image 2</td>
<td>‘D5’</td>
<td>12288 (12 Kb)</td>
<td>AN</td>
</tr>
<tr>
<td>Total Size</td>
<td></td>
<td></td>
<td>24576 Bytes</td>
<td></td>
</tr>
</tbody>
</table>
### Application Specific Data Objects

<table>
<thead>
<tr>
<th>S.No</th>
<th>Data Element</th>
<th>Description</th>
<th>Tag</th>
<th>Size (Bytes)</th>
<th>Date Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACCNO</td>
<td>Account Number</td>
<td>‘E4’</td>
<td>20</td>
<td>N</td>
</tr>
<tr>
<td>2</td>
<td>OPENDATE</td>
<td>Open Date</td>
<td>‘E5’</td>
<td>4</td>
<td>B</td>
</tr>
<tr>
<td></td>
<td>TOTAL SIZE</td>
<td></td>
<td></td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>
## Data Table of Account Info File

<table>
<thead>
<tr>
<th>S.No</th>
<th>Field</th>
<th>Description</th>
<th>TAG</th>
<th>Size (Bytes)</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ACSTATUS</td>
<td>Account Status</td>
<td>‘E8’</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>2</td>
<td>MODEOP</td>
<td>Mode of Operation</td>
<td>‘E9’</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>3</td>
<td>CBALANCE</td>
<td>Current Balance</td>
<td>‘EA’</td>
<td>10</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>ABALANCE</td>
<td>Available Balance</td>
<td>‘EB’</td>
<td>10</td>
<td>N</td>
</tr>
<tr>
<td>5</td>
<td>DPOWER</td>
<td>Drawing Power</td>
<td>‘EC’</td>
<td>10</td>
<td>N</td>
</tr>
<tr>
<td>6</td>
<td>IRAC</td>
<td>Assert Code</td>
<td>‘ED’</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>7</td>
<td>IS</td>
<td>Irregular Since</td>
<td>‘EE’</td>
<td>4</td>
<td>B</td>
</tr>
<tr>
<td>8</td>
<td>MOCOUNTER</td>
<td>Manual Override Counter</td>
<td>‘EF’</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>9</td>
<td>TRANSVOL</td>
<td>Transaction Volume in the day</td>
<td>‘E7’</td>
<td>10</td>
<td>N</td>
</tr>
</tbody>
</table>

**TOTAL SIZE** 48 bytes
### Data Table of Transaction Info File

<table>
<thead>
<tr>
<th>S.No</th>
<th>Field</th>
<th>Description</th>
<th>Size (Bytes)</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TID</td>
<td>Transaction Id</td>
<td>16</td>
<td>N</td>
</tr>
<tr>
<td>2</td>
<td>TYP</td>
<td>Type (DR/Cr)</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>3</td>
<td>TXAMT</td>
<td>Transaction Amount</td>
<td>10</td>
<td>N</td>
</tr>
<tr>
<td>4</td>
<td>CASHIND</td>
<td>Cash/Transfer</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>5</td>
<td>TRCONTRA</td>
<td>Contra A/C Number</td>
<td>20</td>
<td>N</td>
</tr>
<tr>
<td>6</td>
<td>TXNAR</td>
<td>Transaction Narration</td>
<td>25</td>
<td>AN</td>
</tr>
<tr>
<td>7</td>
<td>TXDATE</td>
<td>Transaction Date</td>
<td>25</td>
<td>B</td>
</tr>
<tr>
<td>8</td>
<td>TXTIME</td>
<td>Transaction Time</td>
<td>3</td>
<td>B</td>
</tr>
<tr>
<td>9</td>
<td>TID</td>
<td>Terminal Id</td>
<td>12</td>
<td>N</td>
</tr>
<tr>
<td>10</td>
<td>MO</td>
<td>Manual Over Ride</td>
<td>1</td>
<td>N</td>
</tr>
<tr>
<td>11</td>
<td>STX</td>
<td>Source of Transaction</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>12</td>
<td>TS</td>
<td>Transaction Status</td>
<td>1</td>
<td>AN</td>
</tr>
<tr>
<td>13</td>
<td>CBALANCE</td>
<td>Current Balance after Transaction</td>
<td>10</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>--------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Side Panel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Power Cable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Antenna for GPRS Connection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Display Screen</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Key Pad</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Paper Holder</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Printer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Paper Feed Button</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Status Indicators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Fingerprint Sensor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Contactless Card Slot</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Contact Card Slot</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Standards for POS Terminal

• Smart Card Readers
  – The terminal may have one or more card readers. Each card reader should conform to the appropriate ISO standard:
    • Contact - ISO 7816
    • Contactless - ISO 14443 (Type A and Type B)

• Mutual authentication between terminal and card should be ensured.

• Speaker
Standards for POS Terminal

• Fingerprint Sensor
  – ISO 19794 compliant

• Printer
  – Should be able to print receipts in local languages

• Storage –
  – RAM (Minimum 4 MB)
  – Flash Memory

• Power Backup
  – Minimum 4 hours battery back up for 4 hours operation
  – 24 hours standby
  – Provisioning for charging from motorcycle/car batteries or any other alternates
Standards for POS Terminal

• Connectivity (At least one these as per local requirement)
  – GSM/CDMA
  – Ethernet
  – PSTN

• Display
  – 128 x 64 pixels
  – Number of lines - 8 lines
  – Gray Scale
  – Color (optional)
Standards for POS Terminal

• Sensor
  – Optical/Capacitive/Spectral
  – Image size should be at least 250 X 300 pixels

• Storage Recommended
  – 256 MB RAM expandable to 1 GB
  – 256 MB storage expandable to 8 GB (Flash Memory)
Standards for POS Terminal

• Security Aspects
  – Once the application is loaded on the device there should be no possibilities to modify the application at the field. Reloading or modifying of application should be possible only by an authorized agency or the bank.
  – Fingerprint matching (1:1) – Fingerprint image shall be captured live which shall be matched with fingerprint stored in the card. Matching algorithm can be implemented by the manufacturers with high level of accuracy.
  – Connectivity of terminal to backend protected through SSL/PKI
  – The terminal will have provision for a SAM card. The flash memory can be used for storing BOD file, data downloaded from back end, transaction data etc. in an encrypted form. SAM is for authentication and not storage.
Key Management System

A Symmetric Key Based, Key Management System shall be required in order to fulfill the above mentioned Security Requirements. 3-DES can be used as symmetric Key Algorithm for performing various security operations (Mutual Authentication, Data Encryption, Key Derivation etc.).
Key Management System

• Generation of Parent/Seed Keys (Three of Five Scheme) and their safe storage and Usage.

• Generation of Master Keys and production of Master Key based Authority Cards.

• Key Diversification from Master keys and safely injecting them to the FI Customer Cards to activate them.

• Providing an External Authentication Protocol to perform authentication of FI Customer Card.

• Providing an External Authentication Protocol to perform Role Authentication before Field Transaction by a BC.

• Providing an External Authentication Protocol to perform Role Authentication before allowing to load a new application.

• Providing a Mutual Authentication Protocol between FI Customer Card & BC Card.
Thank You

simanchalasahu@rbi.org.in