



Indian Banks' Association
&
Institute for Development and Research in Banking
Technology



Technical Document II

FI Bank Terminal Operator Card Data Architecture (Ver. 1.3)

Contributors

1. SHRI S.K. SINHA,
SENIOR TECHNICAL DIRECTOR,
NATIONAL INFORMATICS CENTRE
2. DR. PHALGUNI GUPTA,
PROFESSOR,
INDIAN INSTITUTE OF TECHNOLOGY
KANPUR
3. SHRI S. MUKHOPADHYAY,
GENERAL MANAGER,
STATE BANK OF INDIA
4. SHRI S. C. DHOLE,
GENERAL MANAGER,
UCO BANK
5. DR. K. RAVINDRANATH,
CHIEF MANAGER,
UNION BANK OF INDIA
6. SHRI R. SUBRAMANIKUMAR,
ASSISTANT GENERAL MANAGER,
PUNJAB NATIONAL BANK
7. SHRI K. RAMACHANDRAN,
ASSISTANT GENERAL MANAGER,
CORPORATION BANK
8. SHRI N. P. MOHAPATRA,
ASSISTANT GENERAL MANAGER,
NABARD
9. SHRI RAMESH KUMAR,
GENERAL MANAGER,
SOUTH MALABAR GRAMEEN BANK
10. DR. V.N. SASTRY,
ASSOCIATE PROFESSOR,
IDRBT
11. DR. M.V.N.K. PRASAD,
ASSISTANT PROFESSOR,
IDRBT
12. DR. MAHIL CARR,
ASSISTANT PROFESSOR,
IDRBT
13. MS. PRABHUTA VYAS,
SENIOR VICE PRESIDENT,
INDIAN BANKS' ASSOCIATION
14. SHRI K.I. VAREED,
VICE PRESIDENT,
INDIAN BANKS' ASSOCIATION

No Part of this document shall be reproduced without prior permission of IBA - IDRBT

Amendment Log

Version No.	Date	Change Number	Brief Description	Sections Changed
1.0	27/08/09	-	Initial Version	-
1.1	28/08/2009	1	Review by Technical Committee	
1.2	31/08/2009	2	Incorporated changes by Committee Members	Fingerprint
1.3	15/01/2010	3	Review by Technical Committee	Fingerprint Minutiae

Table of Contents

1	Introduction	6
1.1	Purpose	6
1.2	Scope and Presumptions	6
1.3	Glossary of Terms	7
1.4	References	8
1.5	Overview	8
2	Architecture Map of FITOC	9
3	Design Preamble	10
3.1	Data elements in Data Objects	10
3.2	Data elements in EF	10
3.3	Application Dedicated Files (DFs)	10
4	MF Architecture	12
4.1	MF FCP	12
4.2	Terminal Operator Identity Data Objects	12
4.3	Elementary Files	12
4.4	Finger Print Minutiae EF	14
4.4.1	FCP Table	14
4.4.2	Data Table	15
4.4.2.1	Finger Image Record Format [ISO/IEC 19794-4]	15
4.4.2.2	Image Acquisition Setting Level	16

4.4.2.3 Minutia Record Format	17
4.4.2.4 Handling of Finger Minutiae Card Formats	20
5 DF FCP	23
5.1 Elementary Files	23
5.2 Terminal Operator Dynamic Data EF	24
5.2.1 FCP Table	24
5.2.2 Data Table	25
5.3 Transaction Info File	26
5.3.1 FCP Table	26
5.3.2 Data Table	27
Annexure A	29
Appendix-1	32
Appendix-2	33

1 Introduction

1.1 Purpose

This document is prepared to bring uniformity in data layout architecture of the Financial Inclusion Bank Terminal Operator Card.

1.2 Scope and Presumptions

This document puts forward the standards only for data architecture of the Financial Inclusion Terminal Operator Card. Other components such as the Bank Customer Card, the Bank Terminal Specifications and the Key Management System are addressed in other documents. It is presumed that the card operating system is fully compliant to SCOSTA-CL Standard of the Government of India.

1.3 Glossary of Terms

S.No.	Term	Definition
1	FICC	Financial Inclusion Customer Card
2	IBA	Indian Banks Association
3	IDRBT	Institute for Development and Research in Banking Technology
4	NIC	National Informatics Center, Government of India
5	SCOSTA	Indian Standards for Smart Card Operating System - Smart Card Operating System for Transport Application.
6	MF	Master File
7	DF	Dedicated File
8	EF	Elementary File
9	TLV	Tag Length Value
10	FCP	File Control Parameters
11	FDB	File Descriptor Byte
12	SFI	Short File Indicator
13	RFU	Reserved for Future Use
14	LCSI	Life Cycle Status Integer
15	DCB	Data Coding Byte
16	FITOC	Financial Inclusion Terminal Operator Card

Table 1: Glossary of the terms

1.4 References

- 1.4.1 All SCOSTA related specifications
<http://www.scosta.gov.in>
- 1.4.2 <http://www.iba.org.in> IBA web site
- 1.4.3 <http://www.idrbt.ac.in> IDRBT web site
- 1.4.4 ISO/IEC 7816-4,-8 and -9

1.5 Overview

The remainder of this document gives following sections:

Architecture Map of FITOC, this section gives a map of internal architecture of FI Terminal Operator Card.

Design Preambles, this section sets the rules and conventions followed in the Architecture Design.

MF Architecture describes the data architecture of the MF at the top level.

Application DF Architecture describes the data architecture of the DF's at the application level.

2 Architecture Map of FITOC

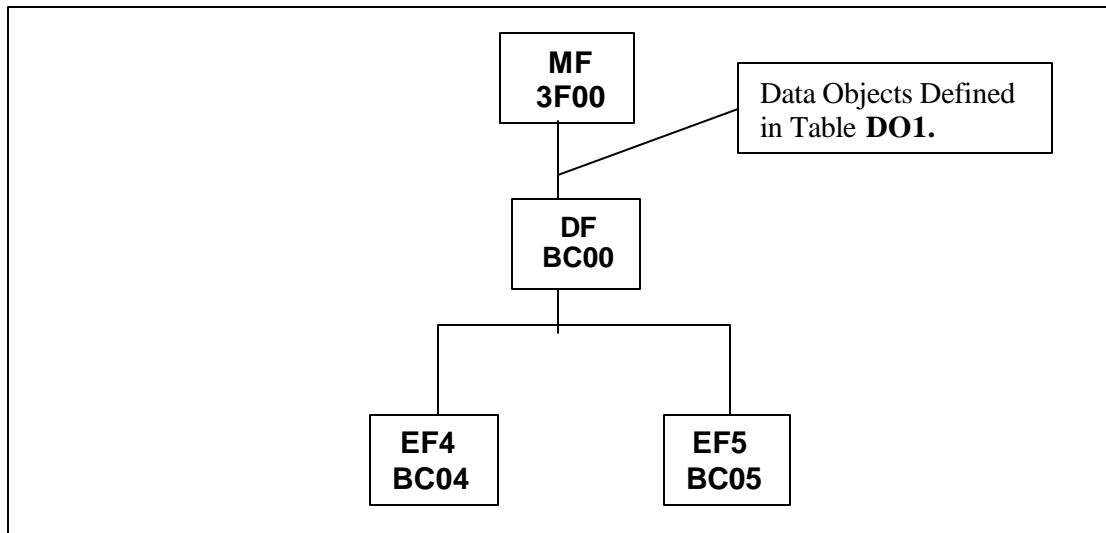


Table 2: Architecture Map of FITOC

3 Design Preamble

3.1 Data elements in Data Objects

For the purpose of simplicity and ease of use, all the static nature of data elements have been stored in the form of data objects in TLV structure. These data objects have been placed directly under MF. As these data objects are static in nature, must be protected from modification/deletion, once created initially.

3.2 Data elements in EF

The data elements, which are dynamic and need modification at field, are stored in a protected EF. Access privileges for these EFs are defined and distributed only to authorized entities, in form of Master Keys.

3.3 Application Dedicated Files (DFs)

Different FI Applications shall be residing as separate DFs on the FITOC, directly under the MF.

Following is the DF for the FITOC.

Application Name	DF Name
Account Transaction	BC 00

Table 3: Application with DF name

The MF architecture of the card should comply with the structure as defined in this document.

The transaction history and operational limits are mandatory for FI Terminal Operator Card and the architecture should comply with the structure as defined in this document.

4 MF Architecture

4.1 MF FCP

Tag	Len	Value	Remarks
'82'	01	38	FDB Only
'83'	02	3F 00	File identifier
'8A'	01	01 or 05	LCSI (When file is created first in creation state, it will be in 01 state. Later it will be turned to 05 after key insertion).

Table 4: FCP of the MF

4.2 Terminal Operator Identity Data Objects (D01)

MF shall be hosting few Data Objects directly under itself. These data objects are prominent to terminal operator identity and have controlled access. Following table describes these data objects (all mandatory).

4.3 Elementary Files

Following three EF Files shall be residing directly under MF. The table below describes these EFs.

Sr.N.	Name/ID	Description
1	3F 04	This EF shall contain the data elements which are static and are related to terminal operator
2	3F 05	This EF shall contain the fingerprint minutiae data

Table 5: Elementary File details

S. No	Data Element	Description	Tag	Size (bytes)	Data Type
1.	CN	Operator Card No	'CE'	19	N
2.	NAME	Operator Name	'C1'	30	AN
3.	MOTHER_NAME	Name of Operator's mother	'C5'	30	AN
4.	ADDRESS	Terminal Operator Address	'D8'	90	AN
5.	SEX	Gender	'C9'	1	A
6.	DOB	Date of Birth	'CA'	4	B
7.	PI	Primary Identification(Type)*	'E2'	2	N
8.	PID	Primary ID (Number)	'C0'	20	N
9.	CID	Card Issue Date	'CD'	4	B
10.	UID	Unique ID	'CB'	20	N
11.	OPCODE	Operator Code**	'CC'	22	N
12.	OPSTATUS	Operator Status**	'CF'	1	N
13.	CARDEXP	Card Expiry Date**	'E3'	4	B

Table 6: Terminal Operator identity data objects in the Master File

*Refer to Appendix 1

**Refer to Annexure A

4.4 Finger Print Minutiae EF (3F 05)

4.4.1 FCP Table

Tag	Len	Value	Remarks
'80'	02		File size 5 K (5120 bytes)
'82'	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
'83'	02	3F05	File identifier
'88'	01	28	SFI
'8A'	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state).

Table 7: FCP of the Finger Print Minutiae EF

4.4.2 Data Table

4.4.2.1 Finger Image Record Format [ISO/IEC 19794-4]

Field	Size	Valid Values	Remarks
Format Identifier	4 bytes	46 49 52 00	"FIR"- Finger Image Record
Version of this standard	4 bytes	30 31 30 00	"010"
Length of record	6 bytes	32 + Number of Finger Views * (14 bytes + Data Length)	Includes all Finger Views
Capture Device ID	2 bytes		Vendor specified
Image Acquisition Level	2 bytes	00 1F	Level 31
Number of fingers/palms	1 byte	≥ 1	In pixels
Scale Units	1 byte	01	Pixels per Inch or Pixels per cm
Scan Resolution (Horizontal)	2 bytes	01 F4	500 ppi
Scan Resolution (Vertical)	2 bytes	01 F4	500 ppi
Image Resolution (Horizontal)	2 bytes	01 F4	500 ppi
Image Resolution (Vertical)	2 bytes	01 F4	500 ppi
Pixel Depth	1 byte	1-16 bits	2-65536 gray levels
Image Compression Algorithm	1 byte	00, or 01, or 02, or 04	Uncompressed is recommended; Otherwise WSQ or JPEG 2000
Reserved	2 bytes	For Future Revision of Standards	Bytes set to '0x0'

Table 8: Finger Image Record Format

4.4.2.2 Image Acquisition Setting Level

Setting Level	Scan Resolution (pixels/cm)	Scan Resolution (pixels/inch)	Pixel Depth (bits)	Dynamic Range (Gray Levels)	Certification
31	197	500	8	200	EFTS/F or IDRBT or UID*

Table 9: Image Acquisition Setting Level

Image Compression Algorithm Codes

Compression Algorithm	Code
Uncompressed- no bit packing	0
Uncompressed- bit packed	1
Compressed- WSQ	2
Compressed- JPEG2000	4

Table 10: Image Compression Algorithm Codes

* In future IDRBT, UIDAI or any other Indian agency may issues certification

**4.4.2.3 Minutia Record Format [Essential]
[ISO/IEC 19794-2]
One per Record**

Field	Size	Valid Values	Remarks
Format Identifier	4 bytes	0x464D5200 (‘F’‘M’‘R’ 0x0)	"FMR"- finger minutiae record
Version of this standard	4 bytes	n n n 0x0	"XX", with XX =20 or greater
Length of total record	4 bytes	24-4294967295	Either 0x0018 to 0x0000FFFFFFFF
Capture Equipment Certification	4 bits		Compliance with ISO standards
Capture Device Type ID	12 bits		Vendor specified
Image Size in X	2 bytes		In pixels
Image size in Y	2 bytes		In pixels
X (horizontal) Resolution	2 bytes		In pixels per cm
Y (vertical) Resolution	2 bytes		In pixels per cm
Number of finger views	1 byte	0 to 255	
Reserved byte	1 byte	0	0 for this version of the standard

Table 11: Minutia Record Format

One per Finger View

Field	Size	Valid Values	Remarks
Finger Position	1 byte	0 to 10	Mentioned below
Version of this standard	4 bits	0 to 15	
Impression Type	4 bits	0	
Finger Quality	1 byte	0 to 100	
Number of Minutiae	1 byte		At least 16 for enrollment & 12 for verification

Table 12: Minutia Record Format
Finger Position Code

Finger Position	Code
Unknown Finger	0
Right Thumb	1
Right Index Finger	2
Right Middle Finger	3
Right Ring Finger	4
Right Little Finger	5
Left Thumb	6
Left Index Finger	7
Left Middle Finger	8

Left Ring Finger	9
Left Little Finger	10

Table 13: Finger Position Code

One per Minutiae

Field	Size	Valid Values	Remarks
X Coordinate (Minutiae type in upper 2 bits)	2 bytes		Expressed in Image pixels
Y Coordinate (upper 2 bits reserved)	2 bytes		Expressed in Image pixels
Angle	1 byte	0 to 255	Resolution is 1.40625 degrees
Quality	1 byte	0 to 100	

Table 14: Minutia Record Format

Extended data formats which is mentioned in ISO 19794-2 for including additional data such as ridge counts and core and delta location is optional.

Best Practices:

1. Image size 250x300 pixels
2. All ten fingers image data storage in the sever
3. Minimum number minutiae for enrollment are 30 - 35 and for verification are 25 - 30.

4.4.2.4 Handling of Finger Minutiae Card Formats [ISO/IEC 19794-2]

Number of minutiae

The number of minutiae is a security sensitive parameter and depending on the security policy of the application. Persons who do not meet the minimum required number for enrolment cannot be enrolled. The maximum number of minutiae for the reference data is implementation dependent.

The recommended minimum number of minutiae required for enrollment is 16 and for verification is 12. The strength of function may have impact on these values.

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

The recommended maximum value for enrollment and verification is 60. However, it is up to the extraction device to limit the number of minutiae sent to the card to 60 or the indicated value.

Number of required finger presentations

The number of required finger presentations during an enrollment process is enrollment system dependent.

Matching

The verification data is subject to translation (in x- and y-direction), rotation (deviation of the orientation) and distortion.

Matching also has to take into account components or factors like FAR/FRR.

The result of the matching process is a score, which may denote the number of matching minutiae or any other appropriate value. In interoperability tests, it may be verified whether different implementations of the matching algorithm meet a required FAR/FRR e.g. in relation to the strength of function for the respective application.

Threshold Value

A verification decision result is positive (i.e. the user verification is successful), if the score as matching result is greater or equal than the required threshold value which depends on several factors or components such as

- 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

For on-card matching, a retry counter (which is decremented by subsequent negative verifications and set to its initial value by positive verification) has to be implemented in order to limit the number of trials. The following aspects have impact on the initial value:

- Experience of the user
- Environmental conditions (e.g. construction of sensor embedding and finger placement)
- Quality of verification data
- Strength of function.

If the retry counter has reached the value 0, then the respective biometric verification method is blocked. The recommended initial value of the retry counter lies in the range of 5 and 15. The security policy of the application provider and the required strength of function have impact on the possible range and the value applied.

Security Aspects of Finger Minutiae Presentation to the Card

Fingerprints are left everywhere and therefore this kind of biometric data are considered to be public. An attacker may succeed in getting a good fingerprint of a person, derive from them the biometric verification data and present it to the stolen card of the respective person. To avoid this kind of attack and also replay attacks of data used in a previous verification process, a trusted path between card and service system is required. Such a trusted path is achieved by cryptographic means, e.g. using secure messaging according to ISO/IEC 7816-4.

Empanelment of Vendors

When a bank deploys one type of biometric fingerprint scanner from a particular vendor X, and consequently wants to add another biometric fingerprint scanner from another vendor Y the bank has to be assured of interoperability between X and Y. For all consequent additions this interoperability has to be similarly tested and assured.

5 DF FCP

Tag	Len	Value	Remarks
'82'	01	38	FDB Only
'83'	02	BC 00	File identifier
'8A'	01	01 or 05	LCSI (When file is created first in creation state, it will be in 01 state. Later it will be turned to 05 after key insertion).

Table 15: FCP of the DF

5.1 Elementary Files

Following two EFs shall be residing directly under DF. The table below describes these EFs.

Sr.N.	Name/ID	Description
1	BC 04	This EF shall contain the data elements which are dynamic and are related to operator limits.
2	BC 05	This file will contain the history of transactions performed by operator.

Table 16: Elementary File details

5.2 Terminal Operator Dynamic Data EF (BC 04)

5.2.1 FCP Table

Tag	Len	Value	Remarks
'80'	02	96	150 bytes with RFU space
'82'	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
'83'	02	BC04	File identifier
'88'	01	20	SFI
'8A'	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state).

Table 17: FCP of the Card Holder Dynamic Data EF

Note: - Access rules for this EF shall be governed by the KMS software and respective card architecture.

5.2.2 Data Table

S. No.	Field	Description	TAG	Size (byte)	Data Type
1	CASHINH	Cash in hand	'D6'	10	SN
2	CASHINHP	Cash in hand permitted	'D7'	10	SN
3	MAXMOC	Maximum manual override permitted per Customer	'D9'	1	N
4	MAXMOP	Maximum manual override permitted for Operator	'DA'	2	N
5	MAXMO	Manual Override Counter	'DB'	2	N
6	MAXSYNC	Maximum number of hours before sync	'DC'	1	N
7	LASTSYNC	Last date/time of sync	'DD'	7	B
8	MAXT	Maximum number of transactions between sync	'DE'	2	N
9	TRANSYNC	Number of transactions since last sync	'E1'	2	N
10	TURNSYNC	Turnover since last sync	'E3'	10	N
11	MAXTO	Maximum turnover between sync	'E4'	10	N

Table 18: Data table of Card Terminal Operator Dynamic Data EF

5.3 Transaction Information File (BC 05)

5.3.1 FCP Table

Tag	Len	Value	Remarks
'82'	05	03 01 00 B3 FA	FDB (Linear Fixed Record simple TLV working EF) DCB (Write Once, 1 byte Data unit) MRL (200 bytes Size 0f each record including tag and length & RFU) Number of records (250)
'83'	02	FC05	File identifier
'88'	01	28	SFI
'8A'	01	01 or 05	LCSI. When file is created first, it will be in 01 state (creation). Later it will be turned into 05 (activated state after key insertion).

Table 19: FCP of Transaction Information File

Note: - This EF shall have controlled access through biometric authentication of operator.

5.3.2 Data Table

The contents of the file will include the records with simple TLV structure. The tags will be a number from 01 to 0A, unique for each record. The records will be stored in FIFO format and when the threshold is reached the card has to sync (go online) the information before new transactions can be added.

S. No.	Field	Description	Size(bytes)	Data Type
1	TID	TRANSACTION ID	16	N
2	CCARDNO	CUSTOMER CARD NUMBER	21	N
3	ACCNO	ACCOUNT NUMBER	19	N
4	TYPE	TYPE(DEBIT/CREDIT)	1	AN
5	CASHIND	CASH/TRANSFER	1	AN
6	TRCONTRA	CONTRA A/C NUMBER FOR TRANSFER TXN	20	N
7	TXAMT	TRANSACTION AMOUNT	10	N
8	TXNAR	NARRATION	25	AN
9	CLOBAL	RESULTING CURRENT BALANCE	10	SN
10	TXDATE	TRANSACTION DATE	4	B
11	TXTIME	TRANSACTION TIME	3	B
12	TID	TERMINAL ID	12	N
13	MO	MANUAL OVERRIDE	1	N
14	STX	SOURCE OF TRANSACTION	1	AN

Table 20: Data table of Transaction Info File

Note: - Modification Access to this file will be given to the authorized person only after biometric authentication of terminal operator.

Annexure A

This section explains the Financial Inclusion Terminal Operator Card architecture where it needs clarification

All dates are to be in DDMMYYYY format in packed BCD.

All timestamps should be in HHMMSS in packed BCD.

All other data is to be written in ASCII format.

For overlapping details refer to FICC Data Architecture (Technical Document I).

4.2 Terminal Operator Identity Data Objects

In Table 6:

- The data field 5 identifies the gender of the terminal operator it should be “M” or “F” accordingly.
- The data field 7 identifies type of primary identification e.g., passport based on Appendix 2.
- The data field 8 is the actual number of the primary identification document e.g., M79679540.
- The data field 11 Operator Code is to be designated as follows with a total of 22 digits with the following structure which identifies an operator uniquely:

Bank Code	4 digits
Branch Code	5 digits
BC Code (Within a bank)	6 digits
Specific Operator Code (Within a BC)	6 digits
Checksum (Luhn’s Algorithm)	1 digits

- The data field 12 Operator Status is to be defined as:
 - 0 – Active
 - 1–Suspended
 - 2 – Temporarily suspended

5.2 Terminal Operator Dynamic Data

In Table 18:

- The data element 3 gives the permitted total number of manual overrides permitted for a particular customer.
- The data element 5 gives the number of overrides done by the terminal operator for all customers .
- The data element 7 Last date/time of sync should be written based on the clock of the back-end host

5.3 Transaction Information File

In Table 20

- The data element 8 provides space for narration of a transaction e.g., By interest paid, By Cheque etc. The information need not be printed on the transaction slip provided to the customer.
- The data element 13 manual override should be
 - 0- No
 - 1 – Yes
- After reaching FITOC memory threshold the backend application should ensure
 - Upload to device storage/backend and
 - Upload methods from device/FITOC to backend should leave no gap/overlap in maintaining an unbroken sequence of card- backend data synchronization from the front-end to the back-end (CBS)
 - This mechanism may be controlled by maintaining a control record in the device where the transaction data is stored. The control record may constitute of a date timestamp, a sequence no and a hash value. (The specific structure of the control record may be decided by the bank).

Appendix 1

01	Passport with same address
02	Passport with different address
03	Election ID Card
04	PAN Card
05	Ration Card
06	Government/Defense
07	ID Card of reputed employer
08	Letter from Employer
09	Letter from recognized public authority/servant
10	Self Declaration
11	Driving License
08	Credit card statement
09	Salary Slip
10	Income/Wealth tax assessment
11	Electricity Bill
12	Telephone Bill
13	Nomination Form (For Nominee)
14	Unique ID (will be added when it comes)
15	National Rural Employment Guarantee Card Number
16	Social Security Pension ID
17	RFU
18	RFU
19	RFU
20	RFU

Appendix 2

- a Alphabetic data elements contain a single character per byte. The permitted characters are alphabetic only (a to z and A to Z, upper and lower case).
- an Alphanumeric data elements contain a single character per byte. The permitted characters are alphabetic (a to z and A to Z, upper and lower case) and numeric (0 to 9).
- n Numeric data elements consist of a digit (having values in the range Hex '0' – '9') per byte.
- sn Signed numeric digit
- b Packed binary coded decimal
- '\n' Padding character