
राष्ट्रीय स्वास्थ्य बीमा योजना
Rashtriya Swasthya Bima Yojana

Ministry of Labour and Employment
Govt. of India

RSBY Enrolment & Card Issuance
System Specifications

Version 1.03

Requirements Specifications Approval Form

Date : June 20, 2008

Project Code : RSBY

This Enrollment and Card Issuance Requirements Specifications document is approved by:

**Approval committee,
Ministry of Labour & Employment, Govt. of India.**

June 20, 2008

Document Prepared By:
Mr. Mujahid Ahsan
(World Bank Consultant)

on behalf of Ministry of Labour & Employment, Government of India

Change History:

1. Section 2.3.1 removed as the Enrolment software need not support 16KB cards.
2. Section 2.3.2 Serial No. 2 **the data object under the DF E000 has been changed from 0200 to 0202.**

TABLE OF CONTENTS

1. INTRODUCTION	5
1.1 OBJECTIVE	5
1.2 SCOPE.....	5
1.3 NOT IN SCOPE	5
1.4 REFERENCE DOCUMENT.....	5
1.5 TERMINOLOGY: ACRONYMS AND ABBREVIATIONS.....	6
2. ENROLMENT & CARD ISSUANCE SYSTEM.....	7
2.1 SYSTEM OVERVIEW:	7
2.2 SYSTEM FUNCTIONAL REQUIREMENTS.....	7
2.3 CARD LAYOUT:	11
2.3.1 16KB Card:	11
<i>Deleted as Enrolment software no longer required to support 16KB card.</i>	<i>11</i>
2.3.2 32KB Card	12
2.4 HARDWARE AND SYSTEM SOFTWARE REQUIREMENT:.....	22
2.4.1 Hardware Components:.....	22
2.4.2 Software components.....	23
2.4.3 Smart card	23
3. STANDARD CODES FOR DATA ELEMENTS:	24
3.1 CODES:	24
3.2 FIELD FORMAT:	25
3.3 INSURANCE COMPANY CODES MASTER:	25
4. CARD ISSUANCE SYSTEM PROCESS	26
4.1 BENEFICIARY ENROLLMENT	26
4.2 PERSONALISATION & ISSUANCE OF SMART CARDS.....	27
4.3 WORKFLOW PROCESS MODEL FOR CARD ISSUANCE.....	29
5. POST ISSUANCE SERVICES.....	30
5.1 RE-ISSUANCE OF LOST CARD.....	30
5.2 CARD SPLITTING.....	30
5.3 CARD MODIFICATION.....	31
6. KEY MANAGEMENT SYSTEM.....	32
6.1 KEY MANAGEMENT SYSTEM COMPONENT.....	33
6.2 KMS INTERFACE FOR RSBY HEALTH CARD.....	33
6.3 INTERFACE TO DKMA SOFTWARE OF NIC.....	34
7. CONCLUSION:.....	36

1. Introduction

1.1 Objective

The **RASHTRIYA SWASTHYA BIMA YOJANA** a Government of India scheme for providing Health Insurance to BPL Citizens of India is in the process of being implemented by different States across India. The Ministry of Labour department, GoI the governing agency for the scheme intends to provide specifications for the software so as to have interoperable software PAN India. The objective of this document is to highlight the requirement specification for automating the Card Issuance workflow of the requirements of Ministry of Labour & Employment (MoLE) for the RSBY project.

1.2 Scope

The scope of the document is limited to the following:

- a. To provides guidelines and business requirement specifications for the Enrolment and Card Issuance system.
- b. To provides details on the information that need to be stored, captured and maintained by the system
- c. To provide the hardware, software and peripherals required for running the system.

1.3 Not in Scope

The following is not covered as part of this document.

- a. Details of the certification process for the Enrolment and Card Issuance system developed.
- b. Data elements required to develop the software. To be defined by the Application development Vendor based on these specifications.

1.4 Reference document

The following documents have been refered / incorporated for framing the specifications:

- a. Rashtriya Swasthya Bima Yojana Draft Tender
- b. RSBY Process Flow
- c. RSBY Card Layout of Beneficiary card
- d. RSBY KMS Specifications of NIC
- e. Database format of BPL database

1.5 Terminology: Acronyms and Abbreviations

AID	Application Identifier
BC	Beneficiary Card
DES	Data Encryption Standard
DF	Dedicated File
DKMA	District Key Management Authority
DO	Data Object
EF	Elementary File
FCP	File control Parameter
HAC	Hospital Authority Card
ICAO	International Civil Aviation Organization
ISO	International Standard Organization
LSB	Least Significant Bit
MF	Master File
MSB	Most Significant Bit
NA	Not Applicable
PIN	Personal Identification Number
RS	Requirements Specifications
RSBY	Rashtriya Swasthya Bima Yojana
SCOSTA	Smart Card Operating System for Transport Applications
TLV	Tag-Length-Value
URN	Unique Relationship Number

2. Enrolment & Card Issuance System

2.1 System Overview:

This module would be primarily used for capturing of the beneficiary data in the field. The software will have the feature to import the data in English and the respective regional language of the particular state BPL database. The enrollment and the card personalization and distribution would be performed over-the-counter i.e. the cards are to be personalized and issued on the spot.

2.2 System functional requirements

The Card Issuance Module consists of the following two subsystems:

- a. Enrollment
- b. Personalisation

The Enrollment sub-system shall perform the following functionality:

- Will have the provision to import data from the data ported from the existing BPL database available at the District level server.
- Will have the provision to authenticate the IA Card using the PIN before the commencement of capturing of Enrolment data.
- Software will have the feature to capture fingerprint of up to 5 individuals of the beneficiary family. (maximum 2 fingerprint per individual)
- Ability to capture photograph of the individual and the family
- Will have the provision to split the cards (Main Card and Add-On card)
- Will have the provision to back up the enrolled data for transferring it to the District server.

Pre requisite:

- BPL data from state as per attached format is ported in the District server.
- URN to be generated at the District server as per the format provided in the Tender document.
- Ported BPL data is transferred into Enrolment station for Enrolment and Card Issuance.
- Availability of Insurance related data – Insurance co code, name, Policy number, Policy start & end date

Table 1 : Functional Requirements for Data Enrollment

Purpose	This screen provides information specific to the Beneficiary and the dependents that needs to be captured and stored in the database of the enrollment and personalization software.
Inputs	Data entry Demographics - only age & gender, capturing of fingerprints and photographs of the head of family and dependant. All other information taken from the BPL database cannot be modified.
Processing	<ul style="list-style-type: none"> a. system checks for mandatory data b. Store the family photograph in the smart card (minimum resolution of 96 dpi) c. Generate a ISO 19794-2 template using the fingerprint image d. Stores the data in the database.
Outputs	Output consists of a screen for verification displaying the data that would be printed and stored in the card.

The Personalisation sub-system shall perform the following functionality:

- The system shall have the capability to authenticate the Issuer Authority card holder through fingerprints before the card is personalised.
- Will have the ability to create file structure on the card.
- Will have the ability to write the relevant beneficiary data on the Smart card.(Machine readable zone)
- Will have the ability to write the Insurance product details on the Smart card. (Machine readable Zone)
- Will have the ability to print the cardholder data on the Smart card using dye sublimation printer. (Visual Inspection Zone)
- Will have the provision in case of split cards to capture the corresponding cards details i.e. the master card would maintain the details of the add on card and vice versa
- Will have the ability to inject keys and activate the beneficiary cards by using the Issuer authority card issued to the Government official
- Will have the ability to capture the Issuer authority card details used for personalizing the beneficiary card.

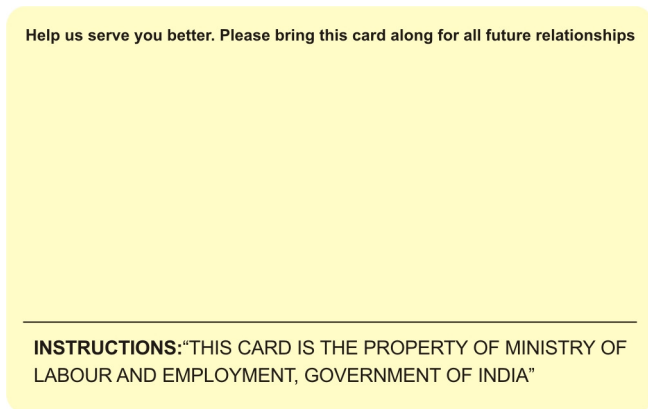
Table 2 : Functional Requirements for Card personalization

Purpose	Electrical and Graphical personalization of the Beneficiary smart card.
Inputs	The user selects the beneficiary card to be printed. Factory blank 16 KB / 32 KB SCOSTA Smart card (ISO 7816) is placed in the Smart card printer.
Processing	<ul style="list-style-type: none"> a. Fingerprint verification of IA card b. System creates necessary file structure on the card as per the Card layout specified. c. System writes all information pertaining to the card holder in the card chip including the ISO fingerprint template and photograph of family. d. Insurance company details and scheme details are written on to the chip of the smart card. e. Storing of corresponding card details in case of card being spitted into Main card and Add On card f. Injection of security keys on the card g. Storing of details in database <ul style="list-style-type: none"> a. Issuer authority ID b. Chip serial number h. Printing of the beneficiary details on the Smart card surface as per layout attached <ul style="list-style-type: none"> a. Head of the family's photograph b. Issuance date c. Name of the head of the family in local language (vernacular) d. Name of the head of the family (English) e. Age of the head of the family f. Gender of the head of the family g. Unique relationship number
Outputs	Activated personalized smart card as per the below artwork.

FRONT



BACK



2.3 Card Layout:

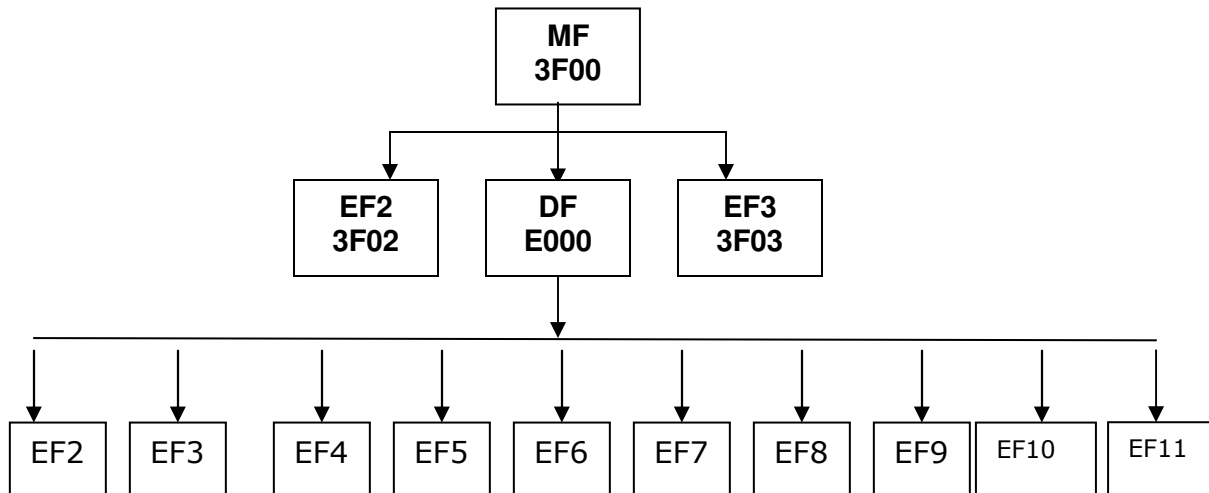
2.3.1 16KB Card:

Deleted as Enrolment software no longer required to support 16KB card.

2.3.2 32KB Card

Version : V 2.0
Size : 32K

The **RSBY** card will have a file structure shown below.



Details of files are listed below: -

1. **E004: Family File**
2. **E005: Template File**
3. **E006: Member File**
4. **E007: Family Photograph File**
5. **E008: Insurance details File**
6. **E009: Blocked Transactions File**
7. **E010: History Transactions File**
8. **E011: Amount Utilisation File**

1. FCP of MF

The MF will have the following 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 Later it will be turned to 05 after Key Insertion).
8C	07	6F FF FF FF 21 FF FF	Security Attributes. Delete File(Self): Never Terminate Card Usage MF: Never Deactivate: Never Create File -DF : SE#1 Create File-EF : Never Delete File (Child) : Never
AB	05	84 01 DA 97 00	PUT DATA (INS DA) Never allowed.
8D	02	3F03	SE File

2. RBC-DF

The RBC-DF will have the following FCP.

Tag	Len	Value	Remarks
82	01	38	FDB Only
83	02	E000	File identifier
8A	01	01 or 05	LCSI (When file is created First in Creation State Later it will be turned to 05 after Insertion of Key).
8C	07	6F FF FF FF FF 23 FF	Security Attributes. AM Byte: 6B Delete File(Self): Never Terminate DF: Never Deactivate: Never Create File -DF : Never Create File-EF: Conditional upon SE#3. Delete File (Child) : Never
AB	06	84 01 DA 9E 01 23	PUT DATA (INS DA) CONDITIONAL UPON SE#3.
8D	02	E003	SE File

Note: - There is only one data object under this DF, which has Tag 02 02 to store the chip number of the split card. This has the TLV structure.

3. Family File: DF-EF4 (Non Modifiable)

The FCP of the Family file will be as follows:

Tag	Len	Value	Remarks
80	02		File size Dynamic.
82	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
83	02	E0 04	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 after Key Insertion).
8C	05	6A FF FF FF FF	Security Attributes. Delete File: Never Terminate EF: Never Deactivate EF: Never Update Binary: Never

This file has Composite TLV structure with TAG **C0**, the two byte length of this tag will be calculated dynamically, based on the overall size of data stored within. Value field shall be a sequence of TLV structures for respective data elements with the tags as defined in the table given below.

The file size will be calculated dynamically and shall be of the length of **C0** Tag plus three bytes (One byte for Tag code C0 and two bytes for length field).

Field	Description	TAG	Max Size
URN	UNIQUE RELATIONSHIP NUMBER	C1	17
FAMID	Family ID for the respective family	C2	10
MEMID	Member ID of the respective family	C3	1
Enrl Date	Enrollment Date	C4	4(BCD)
NAME	NAME OF THE HEAD OF FAMILY	C5	75
NAMEREG	Name In regional language (Unicode)	C6	75
FName	Father/Husband Name	C7	75
Age	Age of head of family	C8	2(BCD)
Gender	Gender of head of family	C9	1
Add1	Door/House #	CA	50
Add2	Village Code	CB	13
Add3	Village Name	CC	50
Add4	Panchayat /Town Code	CD	10
Add5	Panchayat Name	CE	50
Add6	Block code	D0	7

Add7	Block Name	D1	50
Add8	District Code	D2	4
Add9	District Name	D3	50
Add10	State Code	D4	2
Add11	State Name	D5	50
CardIssueDate	Date of Card Issuance	D6	4(BCD)
CVT *	Card Valid Till	D7	4(BCD)

* Card Valid till shall be 10 years from the date of issuance.

4. Family File: DF-EF5 (Modifiable)

The FCP of the Member file will be as follows:

Tag	Len	Value	Remarks
80	02	02 08	File size (520 bytes fixed)
82	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
83	02	E0 05	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).
8C	05	6A FF FF FF 23	Security Attributes Delete File: Never Terminate EF: Never Deactivate EF: Never Update Binary: SE#3

Field	Description	Start Byte	End Byte	Length
FinID	Finger ID	1	1	1
MTemp	Minutia Template	2	513	512
BPLC	BPL Citizen	514	514	1
CType	Card Type(Split/New/Duplicate)	515	515	1
App Flag	Application Flag	516	516	1

3. Member File: DF-EF6 (Modifiable)

The FCP of the Member file will be as follows:

Tag	Len	Value	Remarks
80	02	0D F9	File size (3600 bytes fixed)-32 K
82	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)

83	02	E0 06	File identifier
88	01	30	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).
8C	05	6A FF FF FF 23	Security Attributes Delete File: Never Terminate EF: Never Deactivate EF: Never Update Binary: SE#3

The data in the file shall be structured as described below,

A	B	C	D	E	F	G
---	---	---	---	---	---	---

As described above figure, data shall be structured in the blocks from A to G, such that,

- A Block is of one byte which contains the number of blocks, subsequently written in the file. For example if only B,C and D blocks are written then A shall have number 3 written in one byte.
- Blocks B to G shall have data stored for respective family members, thereby enabling to store the data of maximum six(in **32K Card**) family members as described in Table A given below. Each block shall be of size 596 bytes.
- If the number of members is less than six/four then the data will be written only for the existing members and spaces ear marked for non existing members shall be filled with all zeros. **The empty space in the file will be padded with all zeros.**
- **In case of deletion of any member details, all the record will be moved upward, so that all trailing zeros will be in the end of file.**
- **Internal structure of each block from B to G i.e. data elements for each family members are described in Table B, with the byte positioning within block for each family member specific data element.**

Block	Start Byte	End Byte	Length
B	2	597	596
C	598	1193	596
D	1194	1789	596
E	1790	2385	596
F (RFU)	2386	2981	596
G (RFU)	2982	3577	596

Table A(for 32 K Card)

Field	Description	Start Byte	End Byte	Length
MEMID	Member ID of the respective family	1	1	1
NAME	Name of the Member of the family	2	76	75
Age	Age of Member of the family	77	79	3
Gender	Gender of Member of the family	80	80	1
RelCode	Relation Code	81	82	2
Application Flag	Flag	83	83	1
FinID	Finger ID	84	84	1
MTemp	Minutia Template	85	596	512

Table B

4. Family Photograph File: DF-EF7 (Modifiable)

The FCP of the Photograph file will be as follows:

Tag	Len	Value	Remarks
80	02	2008	File size (8200bytes)-32K Card
82	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
83	02	E007	File identifier
88	01	38	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).
8C	05	6A FF FF FF 23	Security Attributes. AM Byte: 6A Delete File: Never Terminate EF: Never Deactivate EF: Never Update Binary: SE#3

Field	Description	Start Byte	End Byte
Image	Photograph of the family	1	8194

5. Insurance Details File: DF-EF8 (Modifiable)

The FCP of the Insurance file will be as follows.

Tag	Len	Value	Remarks
80	02	005E	File size (94bytes)
82	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
83	02	E008	File identifier
88	01	40	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).
8C	05	6A FF FF FF 23	Security Attributes. AM Byte: 6A Delete self: Never Terminate EF: Never Deactivate EF: Never Update Binary: SE#3

Field	Description	Start Byte	End byte	Length
INSCCode	Insurance Company Code	1	12	12
INCCName	Insurance company name	13	42	30
PolicyNo	Policy No	43	62	20
MAmtIns	Maximum amount Inserted	63	70	8
TravelAmtS	Amount sanctioned for travel claim	71	78	8
SDateIns	Start Date of Insurance	79	86	8
ExDateIns	Expiry Date of Insurance	87	94	8

6. Blocked Transactions File: DF-EF9 (Modifiable)

The FCP of the file will be as follows.

Tag	Len	Value	Remarks
82	05	03 01 00 37 0A	FDB (Liner Fixed Record simple TLV working EF) DCB (Write Once, 1 byte Data unit) MRL (55 bytes Size Of each record including Tag and length) Number of records
83	02	E009	File identifier
88	01	48	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).

8C	05	6A FF FF FF 21	Security Attributes. AM Byte: 6A Delete self: Never Terminate EF: Never Deactivate EF: Never Update Record: SE#1
----	----	----------------------------	--

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.

Field	Description	Max Size
MemberID	Member ID	1
AuthorityID	Authority ID	8
HsCode	Hospital Code	8
AdminDate	Date of Admission	4(BCD)
PkgCode	Package Code	10
AmtBlock	Amount Blocked	8
Appl Data	Application Data	14

Application Data of 14 bytes will have No. of days (for variable Package Type) in the following TLV structure

TLV for storing No. of days:

Tag : C0
Length : 1
Value : XX (No. of days) in BCD

TLV for storing Travel Claim flag:

Tag : C1
Length : 1
Value : 0 or 1. (0 for Travel claim not claimed and 1 for Travel claim claimed)

Remaining 8 bytes left will be used for any application specific future requirements. Any information written in this field shall have the approved TLV structure.

7. History Transactions File: DF-EF10 (Modifiable)

The FCP of the file will be as follows.

Tag	Len	Value	Remarks
82	05	03 01 00 60 0F	FDB (Liner Fixed Record simple TLV working EF) DCB (Write Once, 1 byte Data unit) MRL (96 bytes size Of each record including Tag and length) Number of records (15)
83	02	E010	File identifier
88	01	50	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).
8C	05	6A FF FF FF 21	Security Attributes. AM Byte: 6A Delete File: Never Terminate EF: Never Deactivate EF: Never Update Record: SE#1

The contents of the file will include the records with simple TLV structure. The tags will be a number from 01 to 0F, unique for each record.

Field	Description	Max Size
MemberID	Member ID	1
TransCD	Transaction Code	2
TerminalID	Terminal ID	4
BatchID	Batch ID	3
SERReceipt	Serial No of Receipt	3
TransDate	Transaction Date	4
TransTime	Transaction Time	3
HSCode	Hospital Code	8
PREBal	Previous Balance	8
TransTyp	Transaction Type	1
AMTBlock	Amount Blocked/ Debited	8
PAKcd	Package Code/Authorization No	10
DateofAdmin	Date Of Admission	8
DateDis	Date Of Discharge	8
InFun	In-Sufficient Funds	1
Amt	Amount	8
Appl Data	Application Data	14

Note: -

- **In case of empty space in the end all will be filled with zeros. Record with oldest Transaction Date and Transaction Time will be overwritten if all the fifteen records are written.**
- **Application Data of 14 bytes is reserved for any application specific future requirements. Any information written in this field shall have the approved TLV structure.**

8. Amount Utilisation File: DF-EF11 (Modifiable)

The FCP of the Insurance file will be as follows.

Tag	Len	Value	Remarks
80	02	003C	File size (60 bytes)
82	02	01 01	FDB (Transparent Working EF) DCB (Write Once, 1 byte Data unit)
83	02	E011	File identifier
88	01	58	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).
8C	05	6A FF FF FF 21	Security Attributes. AM Byte: 6A Delete self: Never Terminate EF: Never Deactivate EF: Never Update Binary: SE#1

Field	Description	Start Byte	End byte	Length
AmtCT	Amount claimed for treatment	1	8	8
AmtCTravel	Amount claimed for travel	9	16	8
AmtBlk	Amount Blocked	17	24	8
AuthorityID	Authority ID	25	32	8
HSCode	Hospital Code	33	40	8
UptDate	Last updated date	41	48	8

NOTE: All Data in the card is to be written in ASCII format wherever it is not specified.

2.4 Hardware and System Software requirement:

2.4.1 Hardware Components:

- Computer
 - Capable of supporting all devices as mentioned below
 - Loaded with standard software as per specifications provided by the Ministry of Labour, Government of India.
- Fingerprint Scanner/ Reader Module
 - Thin optical sensor
 - 500 dpi @ 8bit per pixel
 - Active area: 13mm x 20mm
 - Interface: USB 1.1 and 2.0
 - Operating temperature: -10°C to +50°C
 - 1:1 verification
 - Verification time < 0.8s
 - Identification time < 1s
 - Tunable false acceptance rate
 - Verify Fingerprint Template as per ISO 19794
 - Compatible Drivers
- Camera
 - Sensor: High quality VGA
 - Still Image Capture: up to 1.3 megapixels (software enhanced). Native resolution is 640 x 480
 - Automatic adjustment for low light conditions
- Smartcard Reader – 2 Nos.
 - PC/SC and ISO 7816 compliant
 - Read and write all microprocessor cards with T=0 and T=1 protocols
 - USB 2.0 full speed interface to PC with simple command structure
 - PC/SC compatible Drivers
- Smart card printer
 - Supports Colour dye sublimation and monochrome thermal transfer
 - Edge to edge printing standard
 - Integrated ribbon saver for monochrome printing
 - Prints at least 150 cards/ hour in full colour and upto 1000 cards an hour in monochrome
 - Minimum Printing resolution of 300 dpi

- Compatible with Windows / linux
- Automatic or manual feeder for Card Loading
- Compatible to Microprocessor chip personalisation

2.4.2 Software components

- Operating System : Vendor can adapt any OS for their software
- Database : Vendor shall adapt a secure mechanism for storing transaction data.

2.4.3 Smart card

The Card Issuance System shall be able to personalize a 16 KB / 32KB NIC certified SCOSTA Smart chosen by the Ministry for the RSBY scheme as per the Card Layout.

3. Standard Codes for Data elements:

3.1 Codes:

SI No.	Data element	Description	Code assigned
1	Relation Code		
		Self	1
		Spouse	2
		Father	3
		Mother	4
		Son	5
		Daughter	6
		Brother	7
		Sister	8
		Father In Law	9
		Mother In Law	10
		Grand Son	11
		Grand Daughter	12
		Grand Father	13
		Grand Mother	14
		Brother In Law	15
		Sister In Law	16
		Other	17
2	Member ID		
		Head of family default	1
		Spouse	2
		Dependent 1	3
		Dependent 2	4
		Dependent 3	5
		<i>Dependent 4 for 32KB card only - RFU</i>	6
		<i>Dependent 5 for 32 KB card only - RFU</i>	7
3	Gender		
		Male	M
		Female	F
3	Card Type		
		Main Card	0
		Split Card	1
		Duplicate Main card	2
		Duplicate Split card	3
4	BPL Citizen	Whether the citizen is a BPL citizen is not. Default is Yes.	Yes- Y No- N

5	Finger ID	ID of the finger for which the ISO fingerprint template has been captured.	0- Left Thumb finger 1 - left Index finger 2- Left Middle finger 3 - Left Ring finger 4- Left Small finger 5- Right Thumb finger 6- Right Index finger 7- Right Middle finger 8 - Right Ring finger 9 - Right Small finger
6	Application Flag	Member status on the card	0 - Inactive 1 - Active

3.2 Field Format:

SI No.	Field	Format	Eg.
1	Amount	All Amount is stored in card as paise padded with leading zeroes	Rs. 98.00 will be stored as 00009800 Rs. 98.56 will be stored as 00009856
2	Date	DDMMYYYY	27 th February 2008 would be stored in BCD format as 27022008
3	Time	HHMMSS	8.30 PM would be stored as 203000 in BCD format

3.3 Insurance Company Codes Master:

The following Codes have been assigned by the Ministry for the Insurance companies. It is mandatory that **ONLY** the allotted codes are to be used by the Insurance company during the card Issuance.

S.NO	NAME OF THE COMPANY	Insurance Company Code
1	ICICI Lombard General Insurance Co. Ltd.	01
2	The Oriental Insurance Co. Ltd.	02
3	Bajaj Allianz General Insurance Co. Ltd.	03
4	National Insurance Co.Ltd.	04
5	The New India Assurance Co. Ltd. New India Assurance	05
6	United India Insurance Co. Ltd.	06
7	Cholamandalam MS General Insurance Co. Ltd.	07

8	HDFC General Insurance Co. Ltd.	08
9	Star Health and Allied Insurance Company Limited	09
10	Apollo DKV Insurance Company Limited	10
11	Future Generali India Insurance Company Limited	11
12	Universal Sompo General Insurance Co. Ltd.	12
13	Reliance General Insurance Co. Ltd.	13
14	Royal Sundaram Alliance Insurance Co. Ltd	14
15	Tata AIG General Insurance Co. Ltd.	15
16	IFFCO Tokio General Insurance Co. Ltd.	16
17	Export Credit Guarantee Corporation of India Ltd.	17
18	Agriculture Insurance Co. of India Ltd.	18

4. Card Issuance System Process

The card Issuance process involves Enrollment of beneficiary, Personalisation and Issuance of Smart card to the Beneficiary. This process would be done over the counter and the card is to be issued on the spot at the Enrolment location. The process of each sub stages is defined below:

4.1 Beneficiary Enrollment

1. Soft copy of the text Data (From the BPL List) as available related to Beneficiaries shall be provided to Insurance companies by the State Nodal Agency.
2. The Insurance Company shall together with the Smart card service provider provide a roster for enrollment camps at the defined locations, to the State Nodal agency.
3. The Insurance Company & State Nodal agency shall carry out a campaign for spreading awareness about the scheme & the enrollment activity in the defined locations to ensure availability of maximum number of beneficiaries at the agreed date.
4. Simultaneously the BPL list (list of beneficiaries eligible for cover under RSBY scheme) should be posted prominently in each of the villages.
5. Smart card service provider shall ensure availability of sufficient Enrollment stations and trained personnel to man them as per the defined roster and specifications below.
6. The enrollment kits carried to a village would have the following data pre-populated
 - a. BPL data pertaining to the village.
 - b. Master tables for the Village, state, District codes, etc as per the BPL data

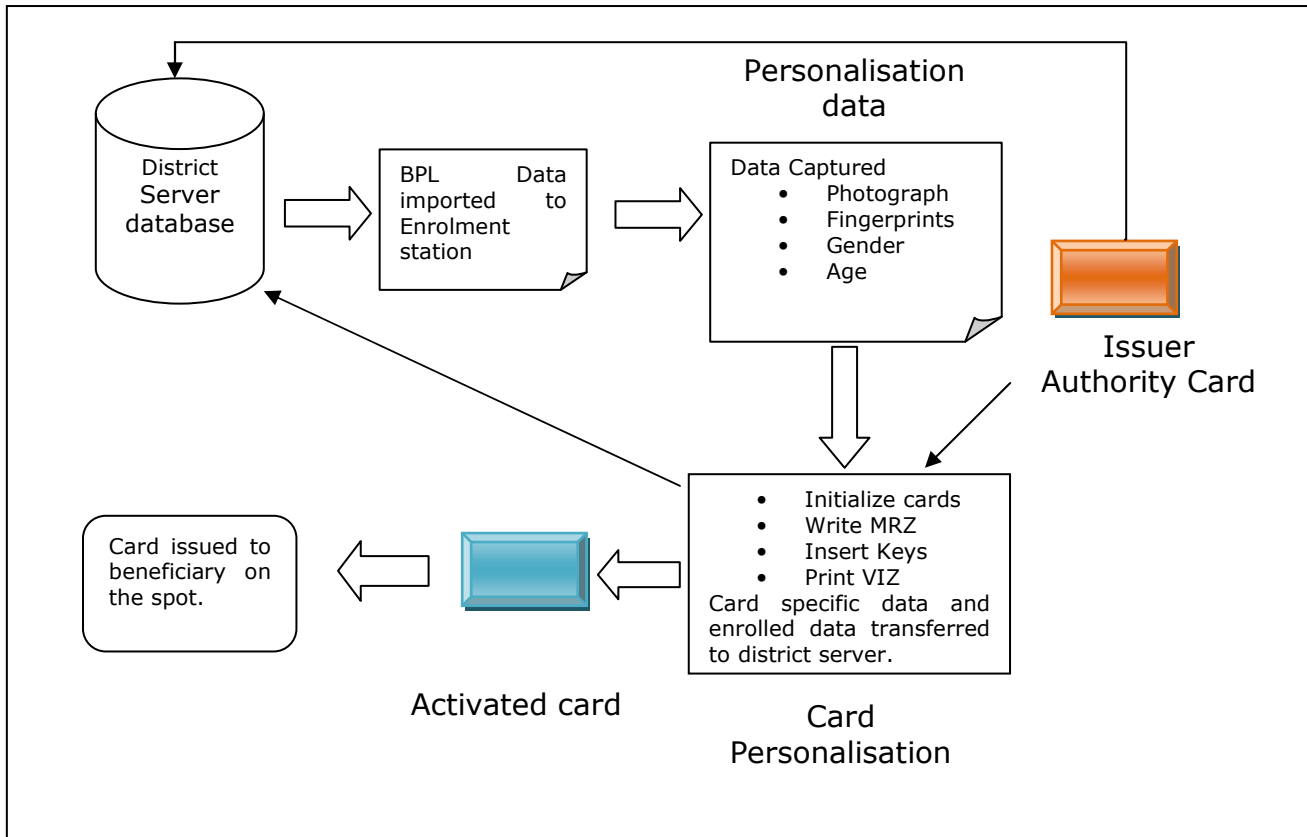
-
-
- c. Insurance Company ID, Policy number, Policy end date and other data pertaining to Insurance company
 7. At the camp, the government official shall identify every beneficiary in the presence of the Insurance company representative based on the hard copy of the BPL list. (Beneficiary would be carrying his BPL card/ or proof of ID as designated by State Nodal agency.)
 8. Beneficiaries who are registered in the state BPL List can only be considered for enrollment. Fresh addition into the BPL list cannot be carried out in this process.
 9. Once the beneficiary is identified & verified by the Government official, Rs. 30/- would be collected from him by the Insurance co. representative and the family would be sent to the enrollment station.
 10. Based on the beneficiary details (Name, URN, Village), the record would be pulled out from the database and displayed to the beneficiary.
 11. For the enrollment process
 - a. The text details already available would be verified by the beneficiary. No change in spellings/ name/ address can be made.
 - b. Additional information required would be age & gender
 - c. Photographs of the head of family and of the complete family would be taken
 12. Two Fingerprints of each of the family member captured. The primary fingerprints to be captured would be right & left thumb, however in case the print is not of good quality or either/ both thumbs missing, sequence of other fingers would be defined in the software.
 13. It is mandatory for the head of the family to be present at the enrollment, in case other family members are not present, they may be added later to the card data at the district kiosk. However, if the entire family is present but not the head of the family, enrollment cannot be done
 14. The enrollment camps in the 1st phase shall not cater to issuance of duplicate cards or card modification. However, if requested, splitting of card may be carried out.

4.2 Personalisation & Issuance of Smart cards

1. The Government official would be carrying the Issuer Authority card (KMS) for insertion of keys into the card at time of personalisation.
2. The data to be written to the card would be displayed on screen.
3. After approval from Issuing authority, the Card will be printed physically with the Head of the family's photograph & other details. The Chip will be personalized with the beneficiary family's data, photograph, fingerprints and insurance details.
4. The government official would insert his Issuer Authority card into the card reader and be authenticated through his finger print. Unique keys for the beneficiary card will be generated by the Issuer Authority card.

-
-
5. The details of personalisation including ID of the Issuing Authority would be stored in the database.
 6. A record would also be written to the Issuing Authority's card for conformance of cards personalized.
 7. The card would be handed over to the beneficiary by the Government official after verification of fingerprints along with a booklet providing
 - i. key features of the scheme
 - ii. helpline numbers
 - iii. process for reissuance of cards
 - iv. cost in case of reissuance of card
 - v. details of Network Health service providers
 - vi. all other details required for smooth usage of card
 8. At the end of each day or completion of Enrollment & Personalisation at a single location, whichever is earlier, the data so collected and generated would be transmitted to the District server via CD. This data must be backed up at the server within the time span defined.
 9. A copy of the database shall also be maintained at State Level Servers for verification purposes which will be synchronous with the Central Server on a day to day basis

4.3 Workflow process model for Card Issuance



5. Post Issuance Services

Insurance companies would be issued a Master Key card for every district for this purpose. This could be only used for issuance of limited number of cards at the District Kiosk. After this limit is exhausted, these cards cannot be used to issue further card till they are recharged by the State Key Management authority.

5.1 Re-issuance of Lost Card

1. In case a Card is reported as lost through any of the channels prescribed by the Insurance Company, it should be marked as Hot Listed in the backend (District and Central Server). The details (Card Serial Number) of all Hot Listed cards must be transmitted to the connecting Devices at the next communication.
2. The devices should not accept any Hot Listed cards and a Warning message flashed in case such a card comes in for transacting and also the card would be blocked by the devices.
3. In case of such card come in contact with the devices the operator would be alerted and the card would be blocked permanently.
4. The beneficiary will go to the kiosk co-located with the District server for Reissuance of Card.
5. The beneficiary existing data, Photograph, Fingerprint & transaction details shall be pulled up from the District server and a fresh card will be immediately issued to the Beneficiary family. Verification of Main member (i.e head of family) fingerprint is to be done before the card is handed over to the beneficiary.
6. The cost of the Smart card would be paid by the beneficiary at the kiosk, as prescribed by the nodal agency in the contract.

5.2 Card Splitting

In case the Beneficiary wishes to split the insurance amount available between two cards to help avail the facilities at two diverse locations.

1. The beneficiary will go to the kiosk which is co-located with the District server for splitting of Card.
2. The fingerprint of the beneficiary shall be verified against those available in card.
3. The splitting amount should be confirmed from the beneficiary.
4. The data in the Main card is modified.
5. The beneficiary existing data, Photograph, Fingerprint & transaction details shall be pulled up from the District server and a fresh card (add-on card) will be issued immediately to the Beneficiary family.
6. Both cards would have details of all family members and also would maintain details (card number) of the corresponding cards i.e. the master card would maintain the details of the add on card and vice versa

-
-
7. Based on these details a fresh card will be immediately issued to the Beneficiary family and the existing card modified.
 8. The cost of the fresh card is to be borne by the beneficiary as per cost decided by state Nodal agency.
 9. Fresh and modified data shall be uploaded to the District Server.

Note: This process can be also performed during the Card Issuance (Enrollment)

5.3 Card Modification

In case a dependent family member is to be added or removed from the card, the beneficiary along with the family members will go to kiosk which is co-located with the District server for modification of Card.

1. A new photograph of the family shall also be captured.
2. Fingerprint in case of addition of member shall also be captured.
3. The existing details shall be modified in the database (District and Central Server) and the Chip of the card.

6. Key Management System

The Smart Card system shall function under a central Key Management System (KMS) to be implemented by Ministry of Labor, for the data and card security. The KMS shall provide the following security features:

- To prevent generation & issuance of fake RSBY Cards, by providing mechanisms to verify authentic cards.
- To protect on-card data against illegal tampering.
- To enable performance of post issuance card transactions at various locations by authorized agencies only.

Below is the brief process flow for KMS operations for issuance of Issuer Authority Card, after the Mother Keys are generated and are in safe custody of Ministry of Labour.

State Nodal agency consolidates the requirements of various authority cards for the state which also includes the requirement of the insurance company.

1. State Nodal agency sends these requirements along with the details of trusted authorities, already earmarked for the purpose, to the Central Key Management Authority (CKMA).
2. CKMA processes the request produces the authority cards and dispatches the authority cards to the State Nodal agency.
3. State Nodal agency sends acknowledgement of receipt of cards along with card details and certifies the safe receipt of cards.
4. State Nodal agency personalizes each authority card based on the requirements and details it received, and generates unique PIN/Password for individual card.
5. Personalized Issuer Authority cards are delivered to State Government officials and Insurance companies along with PIN's for the purpose of issuing cards to the beneficiary.

Note: Detailed process would be defined and provided by NIC.

6.1 Key Management System component

The security requirements for the issuance of the RSBY Health Card are provided by the Key Management System. In order to fulfill the security requirements a Symmetric Key Infrastructure shall be required to be set-up with the help of appropriate Key Management System to undertake following functionalities.

- Root Keys Generation and Management.
- Master Keys Generation and Management.
- Master Keys Issuance.
- Key Derivation and activation of Health Cards.
- Mutual Authentication based card transaction at Hospital/Health Service Provider.
- Mutual Authentication based card transaction by Insurance Service Provider, if any.
- Mutual Authentication based post issuance card modification and re-validation etc.
- PIN Based Master Key Cards protection, Blocking/un-blocking of cards.
- Charging and re-charging of issuance key cards.

6.2 KMS Interface for RSBY Health Card

The DLL for KMS of **RSBY Health Card** would be provided by the Ministry. The DLL has following functions:-

1. This function as defined below is for MIC Card verification through PIN
VerifyIA(readerHandle as long, appData as String) as Boolean
 - a) ReaderHandle (Input Parameter): Reader Handle in which the IA card is connected.
 - b) applicationData(output parameter): returns 512 bytes of applicationData as byte array.
 - c) Return True in case of success else False.

ReaderHandle:

Handle that identifies the connection to the smart card in the designated reader. This handle of type long is return by *ScardConnet* (PCSC command from *Winscard API*)

Reader Handle of the IA card reader is given as input, only once. It prompts for the Pin of IA card and verifies the pin once at the beginning of invocation of application. After this personalization of RSBY cards can be carried out. In case IA card has been disconnected this function shall be required to be invoked again

2. This function is for derivation of unique key for Health card and injecting it to the card.

InsertKey (ReaderHandle as Long, IAID as String) as Boolean

- a) ReaderHandle (Input Parameter): - Reader Handle in which the RSBY Health Card is connected. This handle of type long is return by *ScardConnet (PCSC command from Winscard API)*
- b) IAID (Output Parameter): - Returns ID of RSBY Issuing Authority Card
- c) Return True in case of success else False.

The ReaderHandle is supplied whenever a fresh RSBY card needs to be personalized. The module will insert keys in the RSBY Health Card and activate the card.

Version of KMS DLL: 2.0

6.3 Interface to DKMA Software of NIC

An interface tool is to be developed for the DKMA software for the purpose of capturing the Issuer Authority fingerprint (ISO template) only. Following are the details of the DKMA DB using which the Interface to the DKMA software is to be designed.

Database Name: RSBY_DKMA

1. Table Name: MICMinutia (Write Access)

1. CREATE TABLE [dbo].[MICMinutia] (
 [auth_id] [varchar] (8) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL ,
 [minutia] [varbinary] (512) NULL ,
 [fpimage] [Image] (16) NULL
) ON [PRIMARY]
 GO
 ALTER TABLE [dbo].[MICMinutia] WITH NOCHECK ADD
 CONSTRAINT [PK_Minutia] PRIMARY KEY CLUSTERED
 (
 [auth_id]
) ON [PRIMARY]
 GO

2. Table Name: FKOCardInfo (Read Access)

2. CREATE TABLE [dbo].[FKOCardInfo] (
 [DKMAREfNo] [int] NOT NULL ,
 [DKMAChipNo] [varchar] (32) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
 [BatchNo] [int] NULL ,
 [cardno] [int] NULL ,
 [CardType] [varchar] (4) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
 [ChipNo] [varchar] (32) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
 [distCode] [varchar] (2) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
 [AuthName] [varchar] (25) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
 [AuthID] [varchar] (8) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,
)

```
[designation] [varchar] (25) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,  
[department] [varchar] (25) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,  
[officeAttached] [varchar] (25) COLLATE SQL_Latin1_General_CP1_CI_AS NULL ,  
[Personalizeddt] [datetime] NULL ,  
[ReqCounter] [int] NULL ,  
[CumCounter] [int] NULL ,  
[revalDate] [datetime] NULL  
) ON [PRIMARY]
```

Version of DKMA software: 2.1

7. Conclusion:

The Insurance Company / Smart card service provider shall develop their Enrolment System application based on the above specification guideline. The system would be certified by a 3rd Party Government agency appointed by the Ministry. The information regarding the certification shall be provided on a separate circular. Any additional documents / details required for development would be provided by the Ministry based on written request only.