
राष्ट्रीय स्वास्थ्य बीमा योजना
Rashtriya Swasthya Bima Yojana

Ministry of Labour and Employment
Govt. of India

RSBY Transaction System
Specifications

Version 2.02

Requirements Specifications Approval Form

Date : April 03, 2008

Project Code : RSBY

This Transaction Requirements Specifications document is approved by:

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

April 03, 2008

Document Prepared By:
Mr. Sathya Shankar &
Mr. Mujahid Ahsan
on behalf of Ministry of Labour & Employment, Government of India

Document Reference

Version	Date	Author	Authorized By	Released Date
1.0	11-FEB-2008	Mr. Sathya Shankar		11-FEB-2008
2.0	27 -FEB-08	Mr. Mujahid Ahsan Mr. Sathya Shankar		27-FEB-08
2.01	12-MARCH-08	Mr. Mujahid Ahsan		19-MARCH-08
2.02	28-MARCH-08	Mr. Mujahid Ahsan		03-APRIL-08

Change History

- a. Section 3.1- Package code for UNSPECIFIED package – code for packages not covered is removed
- b. Section 3.5 - Hospital Code and Hospital Authority ID format added.
- c. Section 4.1 - Serial No. 7 codes for Transaction modified.

TABLE OF CONTENTS

1. INTRODUCTION	5
1.1 OBJECTIVE	5
1.2 DOCUMENT SCOPE.....	5
1.3 NOT IN SCOPE	5
1.4 REFERENCE DOCUMENT.....	6
1.5 TERMINOLOGY: ACRONYMS AND ABBREVIATIONS.....	6
2. TRANSACTION SYSTEM.....	7
2.1 SYSTEM OVERVIEW:	7
2.2 SYSTEM ARCHITECTURE	8
2.3 USER INTERACTION AND SYSTEM RESPONSE.....	8
2.4 AUTHENTICATION DIAGRAM FOR MUTUAL AUTHENTICATION.....	10
2.5 SYSTEM FUNCTIONAL REQUIREMENTS.....	11
2.5.1 HAC Card Verification per session.....	11
2.5.2 Printing the Registration Slip	12
2.5.3 Block Treatment charge for the patient.....	13
2.5.4 Unblocking the Blocked Treatment charges	14
2.5.5 Pay Bill on Patient getting Discharged (Transaction completion).....	15
2.5.6 Non Surgical (Medical) Treatment in General Ward or ICU.....	16
2.5.7 In Case Treatment required is not covered under the prescribed list of packages	16
2.6 HARDWARE AND SYSTEM SOFTWARE REQUIREMENT:	18
2.6.1 Hardware Components:	18
2.6.2 Software components.....	18
2.6.3 Smart card	18
3. DATA ELEMENTS OF TRANSACTION SYSTEM:	19
3.1 PACKAGE DETAILS:	19
3.2 INSURANCE COMPANY DETAILS:.....	19
3.3 TRANSACTION DETAILS:	20
3.4 HOTLIST CARD DETAILS:	22
3.5 HOSPITAL CODE AND HOSPITAL AUTHORITY ID FORMAT:.....	22
4. STANDARD CODES FOR DATA ELEMENTS:	23
4.1 CODES:	23
4.2 FIELD FORMAT:	24
4.3 INSURANCE COMPANY CODES MASTER:	24
5. CONCLUSION:.....	25
APPENDIX 1: RSBY TRANSACTION DATA SECURITY GUIDELINES:	26
APPENDIX 2: SPECIFICATION FOR AUTHENTICATION BETWEEN HOSPITAL AUTHORITY CARD (HAC) AND RSBY (BENEFICAIRY) CARD.....	27

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. This document provides the requirement specifications of the **Transaction System Software** it has envisaged for this project to be used at the hospitals. The specifications is intended to serve as a reference for Insurance companies / Smart card service providers for designing and developing an interoperable Transaction system for the RSBY project.

1.2 Document Scope

The scope of the document is limited to the following:

- a. To provides guidelines and business requirement specifications for the transaction system.
- b. To provides details on the information that need to be stored, captured and maintained by the transaction system
- c. To provide the hardware, software and peripherals required for running the Transaction system.
- d. To provide the details of the card authentication process.
- e. To provide guidelines on the data protection and data transfer from transaction system to District server.

This document represents the transaction requirements analysis effort to define technical and business process requirements for. This document is produced prior to detailed design and development of the application. It will be used by the design team as the baseline for establishing systems design and ultimately the development of 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 Transaction system developed. The same would be released as a separate document.

1.4 Reference document

The following documents will be provided for development purpose.

- a. Rashtriya Swasthya Bima Yojana Draft Tender
- b. RSBY Process Flow
- c. RSBY Card Layout as specified in the Enrolment and Card Issuance specifications.

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. Transaction System

2.1 System Overview:

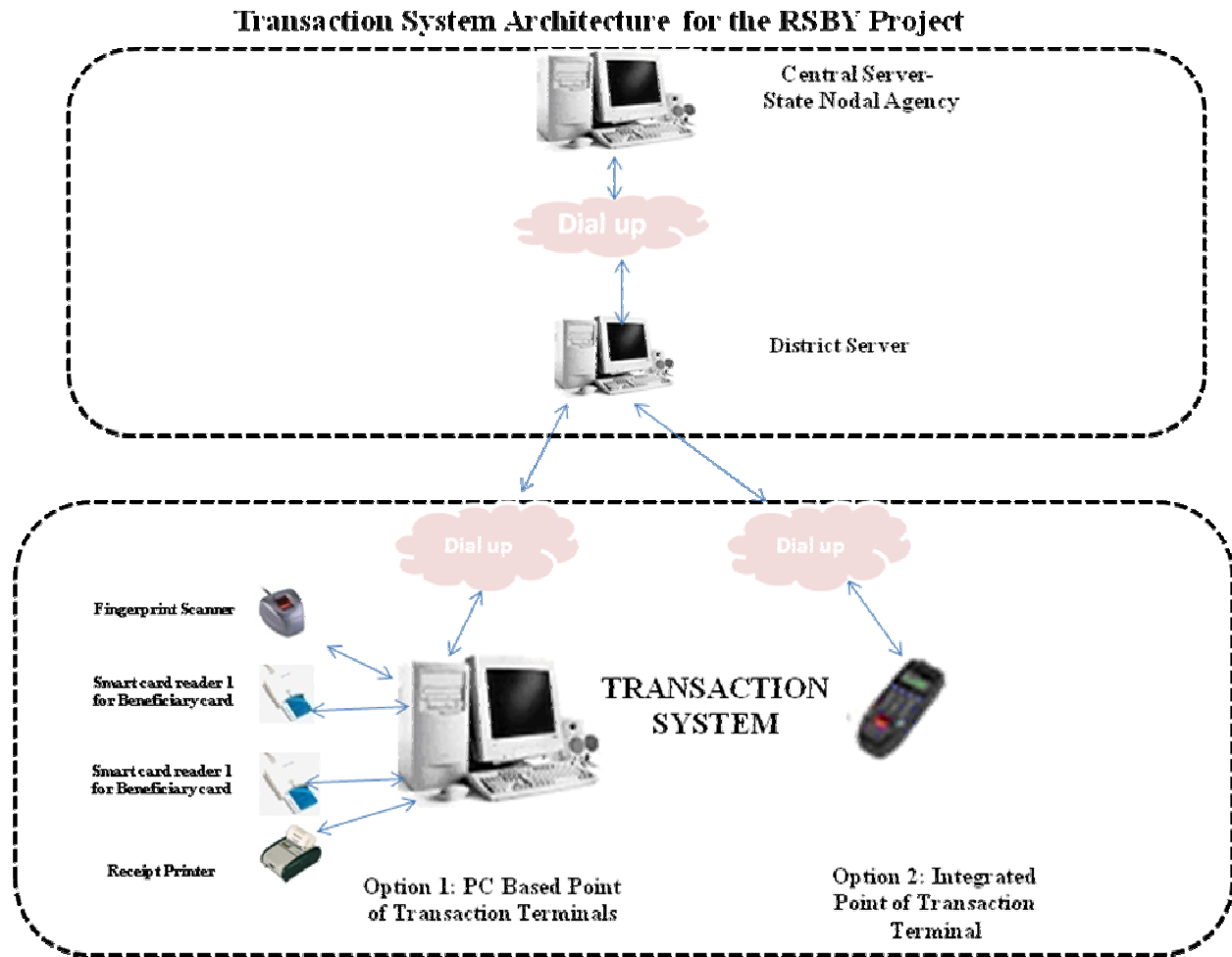
The Transaction system module will be primarily used for performing transactions using either the Smart card Point of Transaction terminal or PC at the hospitals / health centers.

The transaction system will run as a component of the smart card, smart card reader, fingerprint scanner and Transaction software. Each beneficiary of the RSBY scheme would be enrolled and issued a SCOSTA smart card with their details and also the details of their dependent. The card holder will have to insert his/her smart card in the smart card terminal / reader and once the terminal identifies and authenticates the beneficiary by matching the authentication key and the fingerprints, the application would allow the transaction to proceed further. The application will perform the below business functions:

1. Enable the beneficiary to register for treatment.
2. Enable the beneficiary to get cashless admission for treatment.
3. Enable the beneficiary to make payment using their smart card at the time of discharge

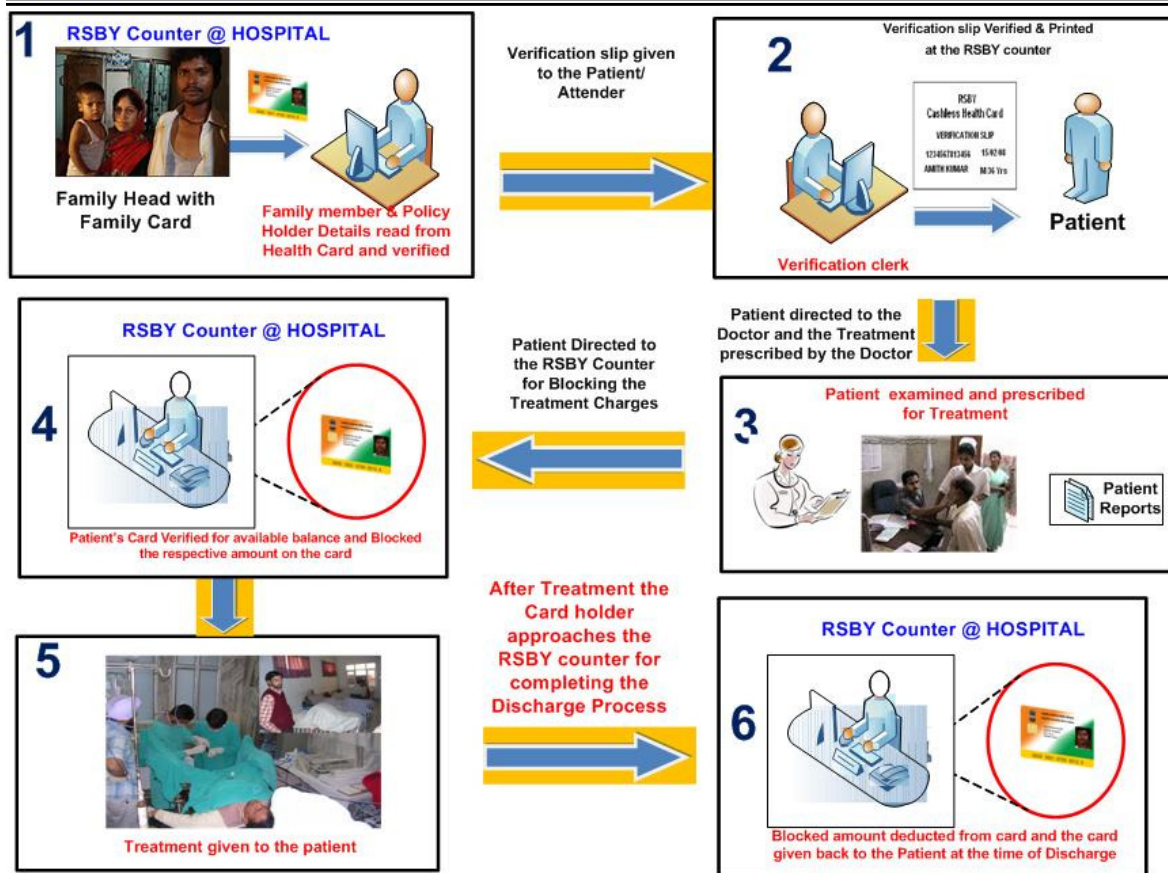
The above transactions are to be stored in the terminal and in turn are to be transferred to the Sever using dial-up connectivity at the end of every day.

2.2 System Architecture



2.3 User Interaction and System Response

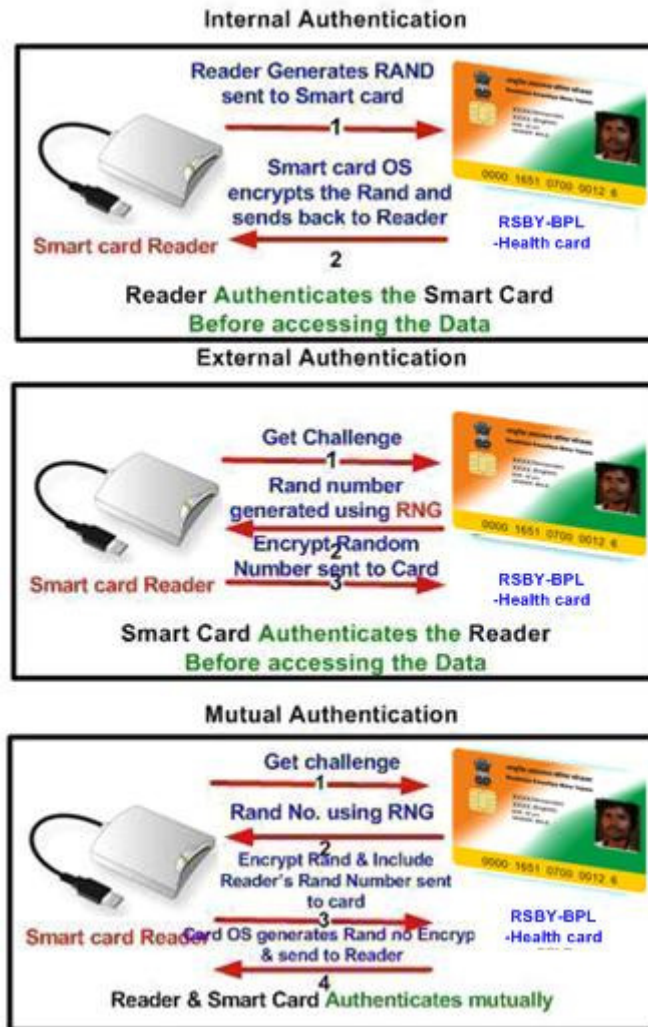
- Overall Context diagram of system usage



- Note: The treatment details, i.e. the Package Code, the Package Name and Amount is frozen by the State and **CANNOT** be changed at either the District or by the Hospital.

2.4 Authentication Diagram for Mutual authentication

A typical authentication diagram is as per the mutual authentication process defined for SCOSTA card is shown below. The Beneficiary card would be authenticated using the Hospital Authority card and vice versa.



2.5 System functional requirements

2.5.1 HAC Card Verification per session

SRS ID	Spec	RSBY_001
SRS Description		Verifying the HAC

Every time the HAC card is inserted into the designate card reader, it would have to be authenticated for the PIN of the card holder. Once this verification is complete, the card holder only needs to be verified through the fingerprint for every transaction till the time the card is taken out and reinserted at which time the session would have ended a new session created.

RSBY-01 On application startup the system shall look for the Hospital Authority card (HAC) and prompt for the PIN

RSBY-02 The Application shall accept a PIN for the HAC and verify with the HAC.

RSBY-03 On successful verification of the PIN, the Hospital Code shall be displayed for confirmation.

RSBY-04 In case of verification failure, the application requests for re-entering PIN for verification. Maximum retry entry is 3 after which the card is automatically blocked and can only be unblocked by the District Key Management Authority (DKMA) only.

RSBY-05 After successful verification of the PIN, the application can carry out the transactions on the Beneficiary card.

2.5.2 Printing the Registration Slip

SRS ID	RSBY_002
SRS Description	Verifying the beneficiary with fingerprint and Printing the Registration slip

Beneficiary approaches the RSBY help desk at the network hospital available at the district. The RSBY beneficiary needs to be verified for genuine usage of the card.

RSBY-06 On successful verification of the HAC, the application shall wait for insertion of the RSBY Beneficiary card. Symmetric key based external authentication of the RSBY card with the HAC card is done.

RSBY-07 On successful authentication the RSBY card is validated for

- a. Hot listing
- b. Policy start
- c. Policy end
- d. Hospital being a part of the Issuing Insurance company's network

RSBY-08 the application reads the RSBY card and displays

- a. The family photo (optional)
- b. URN
- c. The name, age & gender of all members in the card
- d. Insurance policy number
- e. Available Claim
- f. Policy start & End date
- g. Transaction History (Optional)

RSBY-09 Finger print verification of the patient is carried out. In case, patient's fingerprint cannot be verified, another enrolled family member's fingerprint may be verified. A flag indicating the person authenticated along with the reason is written in the database.

RSBY-010 On successful finger print verification of the beneficiary, a confirmation for printing the verification slip is asked for.

RSBY-011 On confirmation print the verification slip with the following details

- a. URN

- b. Transaction Date
- c. Name of patient
- d. Age of Patient
- e. Hospital Code

RSBY-012 In case printing is refused, the application should go back to the menu

RSBY-013 Transaction details are written to the local database

2.5.3 Block Treatment charge for the patient

SRS ID	RSBY_003
SRS Description	Capturing treatment procedure and blocking the claim amount

After getting diagnosis sheet from the doctor, beneficiary approaches RSBY help desk again for the purpose of admission. Verification process is carried out and package selected. Package cost & travel reimbursement amount will be blocked from the available claim amount in case there is sufficient balance in the card.

RSBY-014 In case of new session, repeat steps RSBY-01 – RSBY-05.
Repeat steps RSBY-06 – RSBY-09

RSBY-015 A list of Major Treatment Types shall be displayed from the local database.

RSBY-016 The related packages shall be displayed as the next item.

RSBY-017 Once selected, the corresponding Package Charge fixed for the state would be displayed.

RSBY-018 Once transaction is confirmed, the application will read the balance claim amount available on the card and verify whether the selected package can be provided.

RSBY-019 If sufficient balance is available for the selected package the respective amount shall be blocked from the available claim.

RSBY-020 In case balance claim on the card is insufficient to cover the total package cost confirmation for making balance payment shall be asked for from the beneficiary.

RSBY-021 In case it is not confirmed, the application will exit without updating the card.

RSBY-022 Once transaction is confirmed, the following is written on the RSBY card

- a. Date
- b. Beneficiary ID
- c. Hospital ID
- d. Hospital Authority ID
- e. Package Code
- f. Amount blocked.

RSBY-023 Store all these transaction details as a log into the local database.

RSBY-024 Generate two slips – one for the beneficiary and the other for the hospital

2.5.4 Unblocking the Blocked Treatment charges

SRS ID	RSBY_003
SRS Description	Unblocking the blocked transaction amount if treatment not taken by the beneficiary

In case for any reason the beneficiary does not avail treatment at the hospital after the amount is blocked or the hospital is unable to provide the required treatment, the RSBY help desk can unblock the amount of a blocked transaction. Unblocking cannot happen for a debited transaction. Unblocking can only be done at the same hospital where the amount was blocked.

RSBY-025 In case of new session, repeat steps RSBY-01 – RSBY-05.
Repeat steps RSBY-06 – RSBY-09

- RSBY-026** All blocked but not completed transactions initiated at the hospital where transaction is currently being carried out for the selected patient are displayed.
- RSBY-027** The reason for unblocking or treatment cancellation is captured for the selected transaction
- RSBY-028** After unblocking, display the available balance on the card.
- RSBY-029** The transaction history on the card shall store all these details and display it on the next insertion of the card.
- RSBY-030** Store all these transaction details as a log into the local database.

2.5.5 Pay Bill on Patient getting Discharged (Transaction completion)

SRS ID	RSBY_004
SRS Description	Debit package amount from card

While discharging, beneficiary should approach help desk and all the discharge details will be captured and the blocked amount can be claimed for insurance.

- RSBY-031** In case of new session, repeat steps RSBY-01 – RSBY-05.
Repeat steps RSBY-06 – RSBY-09
- RSBY-032** All blocked transactions for the current hospital for the selected patient are displayed
- RSBY-033** At time of discharge, a debit transaction shall be created on the card. The transaction should also display the travel amount is to be paid to the beneficiary in case a balance exists in the travel amount.
- RSBY-034** The transaction details shall also be stored to the local database.
- RSBY-035** Three (3) transaction slips are printed to complete this transaction (1-for the patient, 2-for hospital records, 3 – Insurance company)

RSBY-036 In case of mortality, the Beneficiary Name is recorded along with the short summary for the cause of death into the local database or transaction description is recorded into the local database.

2.5.6 Non Surgical (Medical) Treatment in General Ward or ICU

SRS ID	RSBY_005
SRS Description	In case the treatment prescribed by the doctor falls under the non surgical item, the package amount shall be multiplied by no of days treatment is expected to go on

RSBY-037 In case of new session, repeat steps RSBY-01 – RSBY-05.

RSBY-038 Repeat steps RSBY-06 – RSBY-09

RSBY-039 In case Non Surgical Medical treatment is selected, the application shall allow for entry of no. of days expected for admission.

RSBY-040 The application shall calculate the package amount as package amount from database x no of days entered

RSBY-041 Repeat steps RSBY -019 – RSBY-025

2.5.7 In Case Treatment required is not covered under the prescribed list of packages

SRS ID	RSBY_005
SRS Description	In case treatment required is not covered under the list of prescribed packages

RSBY-042 If treatment is not covered under the list of packages the system shall provide an option as "UNSPECIFIED". The amount to be charged for this option would be entered manually based on authorization from the Insurance Service Provider. The Insurance Provider will generate and provide a unique Authorization Number for the accepted transaction. The process of blocking and payment is similar to a normal transaction as specified under the scheme.

RSBY-043 In case of new session, repeat steps RSBY-01 – RSBY-05.

RSBY-044 Repeat steps RSBY-06 – RSBY-09

RSBY-045 A manual process outside the purview of this software application shall be carried out to get authorization from the Insurance Company. The authorization received would carry Authorization ID as per format and the amount to be charged. Provision will be there in the application to capture the Authorization ID and amount. The transaction shall be created on the card based on these along with the information on Insurance company, date, etc. Remarks for the treatment being given may also be captured if required.

RSBY-046 Save the transaction details to the local database.

2.6 Hardware and System Software requirement:

2.6.1 Hardware Components:

- Fingerprint Scanner/ Reader Module – 1 Per Helpdesk
 - 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
- Smartcard Reader – 2 Per Helpdesk (1 each for HAC & Beneficiary Cards)
 - 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
- Printer
 - Printer with Device Drivers
- Modem

2.6.2 Software components

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

2.6.3 Smart card

The Transaction system shall be able to read / write on 16 / 32KB SCOSTA Smart issued by the Ministry for the RSBY scheme.

3. Data elements of Transaction System:

The following data elements are mandatorily to be maintained by the Transaction system.

3.1 Package Details:

This would contain the list of the packages along with cost for the package which would be used during the transaction. This data has to be communicated to the Transaction device at the hospital from the State server and CANNOT be modified at the hospital.

Sl. No.	Field Name	Data Type	Length	Description
1	Package Category Code	Text	3	Procedure code as per list. Eg. 001- Dental
2	Package ID	Text	10	First 3 digit shall be the package category code and the preceding will the codes as per the list
3	Package Name	Text	100	As per the list
4	Amount	Text	8	Last 2 digits would be paise
5	Type (Fixed / Variable)	Text	1	FP – Fixed package VP- Variable package based on No. of days.

Eg: Package ID for the Package category code Ear (03) sub category Fenestration with serial No.of 5 will be denoted as:

Package Type	Package Category	Sub Category Code
FP	003	00005

Note: Package Mater would be provided by the State Nodal agency.

3.2 Insurance Company Details:

This would contain the list of Insurance companies whose card is accepted at the transaction terminal. This list would be fixed for the Insurance Company's centrally

SI No.	Field Name	Data Type	Length	Description
1	Insurance Company Code	Text	12	As per the code allotted by the Ministry
2	Insurance Company Name	Text	30	
3	Activated Date	Text	8	Date of activation.

4	Expiry Date	Text	8	Date up to which card could be accepted.
---	-------------	------	---	--

3.3 Transaction details:

The following transaction details are to be maintained mandatorily by the transaction system. These transactions details are to be transferred to the District server periodically as per the format defined below. The details will have a composite TLV Structure with Tag C0, the two byte length of this Tag will be calculated dynamically based on the overall size of the transaction record as per the structure below. The Value field shall be a sequence of TLV structures for respective data elements with the tags as defined below. The length field of these tags shall be of one byte for all data elements. The overall record size shall be the length of C) tag plus 3 byte (One byte for Tag Code C0 and two bytes of length field)

SI No.	Field Name	Data Type	Tag	Length	Description
A. Transaction Reference					
1	Transaction ID	AutoNum	C1	8	System generated
2	Terminal ID	Text	C2	8	ID allotted to the Terminal by the server.
3	Batch No	Text	C3	6	Batch No. reference for the transactions stored.
4	Invoice No	Text	C4	6	Running serial number under a batch
B. Beneficiary Card / Patient details					
5	Unique Relationship Number (URN)	Text	C5	17	
6	Chip Serial Number	Text	C6	64	
7	Card Type	Text	C7	1	Main or Split
8	Insurance Policy No	Text	C8	20	
9	Insurance Co Code	Text	C9	12	
10	State Code (Customer Card)	Text	CA	2	
11	District Code (Customer Card)	Text	CB	4	
12	Member ID	Text	CC	1	
13	FP Verifier ID	Text	CD	1	Member ID of the person whose finger was verified.
C. Transaction Details					
14	Hospital Code	Text	CE	10	As per Hospital Authority card
15	Hospital Authority ID	Text	D0	8	As per Hospital

					Authority card
16	Transaction Code	Text	D1	4	As per transaction code list defined below. Eg: 0300 denotes registration
17	Transaction Type	Text	D2	1	As per transaction type list code defined below Eg: 01- Cashless
18	Transaction Date	Text	D3	8	
19	Transaction Time	Text	D4	6	
20	Package code / Authorization Code	Text	D5	10	
21	Total Amount Claimed	Text	D6	8	
22	Total Amount Blocked	Text	D7	8	
23	In-sufficient funds (Y/N)	Text	D8	1	
24	Insufficient Amount	Text	D9	8	
25	No of Days (in case of variable type of package)	Text	DA	3	
26	Date of Admission	Text	DB	8	
27	Date of discharge	Text	DC	8	
28	Mortality (Yes / No)	Text	DD	1	Y - Yes N - No
29	Transaction Description	Text	DE	30	
D. Card Balance Details after Transactions					
30	Amount Claimed for Treatment	Text	E0	8	
31	Travel Amount Claimed till date	Text	E1	8	
32	Current total Amount Blocked in Card	Text	E2	8	
33	RFU *	Text	TBD	25	

*** Note: RFU of 25 bytes is reserved for any application specific future requirements. Any information written in this field shall have the approved TLV structure.**

3.4 Hotlist Card Details:

The transaction system shall maintain the list of cards which have been hot listed by the District server. In case of Hotlist card details coming into contact the transaction system shall ONLY display an appropriate message and should not allow to transaction to proceed further. No deactivation shall be performed on the card.

SI No.	Field Name	Data Type	Length	Description
1	Chip Serial Number	Text	64	Hex value of Card Serial Number would be stored in Text format. SCOSTA cards have CSN of maximum 32 bytes
2	Download Date /Time	Text	14	
3	Status (Pending / Applied / Sent)	Text	2	RFU
4	Applied Date /Time	Text	14	RFU

3.5 Hospital Code and Hospital Authority ID format:

This would contain the list of the hospitals which would be used during the transaction. The Hospital code has to be communicated to the Transaction device at the hospital from the District server and CANNOT be modified at the hospital.

Sl. No.	Field Name	Data Type	Length	Description
1	Hospital Code	Text	8	First 2 digits shall be State code, next 3 digits shall be district code with leading 0's and the next 3 digits shall be a running serial No with leading 0's.
2	Hospital Authority ID	Text	8	As per DKMA software. (1-2 bytes for State Code, 3-4 bytes for District code and the next 4 digits will be running serial No.)

Note: Insurance Company shall take necessary approval from the Ministry before assigning the Hospital code and the Hospital authority ID to maintain uniqueness in the system.

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

4. Standard Codes for Data elements:

4.1 Codes:

SI No.	Data element	Description	Code assigned
1	Relation Code		
		1	Self
		2	Spouse
		3	Father
		4	Mother
		5	Son
		6	Daughter
		7	Brother
		8	Sister
		9	Father In Law
		10	Mother In Law
		11	Grand Son
		12	Grand Daughter
		13	Grand Father
		14	Grand Mother
		15	Brother In Law
		16	Sister In Law
		17	Other
2	Member ID		
		Head of family default	1
		Spouse	2
		Dependent 1	3
		Dependent 2	4
		Dependent 3	5
		Dependent 4 for 32KB card only (RFU)	6
		Dependent 5 for 32 KB card only (RFU)	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
7	Transaction Code		
		Registration	0300
		Blocked	0301
		Unblocked	0302
		Payment of Bill	0303
8	Transaction Type		
		Cashless	0
		Pre-authorization from Insurance company	1

4.2 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

4.3 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

5. Conclusion:

The Insurance Company / Smart card service provider shall develop their Transaction application based on the above specification guideline. The Transaction 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. All documents required for development would be provided by the Ministry based on the written request only.

Appendix 1: RSBY Transaction Data security guidelines:

This document specifies the transaction data security guideline that is to be implemented as part of the Transaction System for the RSBY scheme. The guidelines are being specified for the purpose of maintaining the confidentiality and integrity of the transaction data that is stored in the Terminal and subsequently transferred to the District server.

Transaction Data Authentication:

Transaction Authentication is the process used to ensure that transaction data stored in the terminal is not altered or duplicated in any fashion following the completion of a transaction. The following are the few of the transactions that are to be securely stored in the PC based Terminal:

- a. Amount Blocked for treatment in Smart card.
- b. Amount Paid for treatment using Smart card
- c. Visit details.

Following are the guidelines for the transaction data authentication:

- a. All data elements stored as part of the transaction record should be stored securely.
- b. The transaction application shall ensure that the confidentiality and integrity of the data is maintained.

Transaction Data transfer protocol:

Transaction collection is the process by which all the offline transactions stored in the PC based terminal of the Hospitals during a specified time periods are uploaded to the District server. As the transactions in the RSBY scheme takes place offline the terminal must upload to the District Server all the activities that are carried out at the terminal for the purpose of accounting and settlement purpose. The uploading of the transactions is to be done at scheduled intervals (intervals for the same to be decided by the insurance company, mandatory minimum once per day).

The following are the guidelines for data transfer mechanism between transaction system and the Back end Host (District Server) for secure transfer of transaction record:

- a. Secure session is to be established between the Transaction terminal and the District server.
- b. When the transaction details are received by the district server, the system shall perform a validation check on the transaction records before completing clearing and settlement.

Appendix 2: Specification for authentication between Hospital Authority card (HAC) and RSBY (Beneficiary) card.

Pre-Condition

A system with two card reader slots will be needed. The two cards MHC (HAC) card and the RSBY card are also required.

User Scenario

The user of this application will be the FKO (Hospital).

Application Specifications

1. MHC-MF (MF ID: 3F00) is selected on the MHC (HAC) card using SELECT FILE command.
(APDU: 00A400023F00)
2. Verify pin number 1 from hospital card.
(APDU: 0020008106 & Pin in Hex)
3. READ URN NUMBER FROM RSBY CARD.
4. TAKE 16 Most Significant Byte OF URN.
5. MHC-DF(DF ID: B300) is selected on the MHC (HAC) card using SELECT FILE command.
(APDU: 00A40002B300).
6. MHC SE FILE ID: B303 is selected on the MHC (HAC) card using SELECT FILE command.
(APDU: 00A40002B303).
7. Send MSE RESTORE Command on MHC (HAC) Card with SE Reference 02.
(APDU: 0022F302)
8. Send MSE SET Command on MHC (HAC) card USING URN NUMBER taken in Step 4.
(APDU: 002281A4129410 & URN No. in HEX)
9. Send Get Challenge Command on MHC (HAC) Card.
(APDU : 0084000008)
10. Send INTERNAL AUTHENTICATION Command ON RSBY CARD USING CHALLENGE from step 9 and using key reference 81.

(APDU : 0088008108 & Challenge in Hex)

11. Send Command to get Response of length 8 bytes from RSBY Card.
(APDU: 00C00008)
12. Send External Authentication Command on MHC (HAC) Card using the response received in step 11 with key reference 81.
(APDU: 0082008108 & Response in Hex).

Successful External Authentication Command Verifies the key on RSBY Card.

13. Send Select file Command with file ID E000 on RSBY Card.
(APDU: 00A40002E000).
14. Send Get Challenge Command on RSBY Card.
(APDU: 0084000008).
15. Send MSE RESTORE Command on MHC (HAC) Card with 04.
(APDU: 0022F304).
16. Send MSE SET Command on MHC (HAC) Card USING URN NUMBER
(APDU: 002241A4129410 & URN No. in Hex).
17. Send INTERNAL AUTHENTICATION Command ON MHC (HAC) CARD USING CHALLENGE from step 14 with key reference 81.
(APDU: 0088008308 & Challenge in Hex).
18. Send Command to get Response from MHC (HAC) Card.
(APDU: 00C0000008).
19. Send External Authentication Command on RSBY Card using the response received in step 18 with key reference 82.
(APDU: 0082008208 & Response in Hex)

Successful External Authentication command will now facilitate updation of EF's E009, E010 & E011 on the RSBY Card.