

RASHTRIYA SWASTHYA BIMA YOJNA

SPECIFICATION FOR AUTHENTICATION BETWEEN HOSPITAL CARD & RSBY (BENEFICIARY) CARD

Pre-Condition

A system with two card reader slots will be needed. The two cards MHC 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 card using SELECT FILE command.
(APDU: 00A400023F00).
2. MHC-DF (MF ID: B300) is selected on the MHC card using SELECT FILE command.
(APDU: 00A40002B300).
3. Verify pin number 1 from hospital card.
(APDU: 0020008106 & Pin in Hex).
4. READ 16 Most Significant Byte URN NUMBER FROM RSBY CARD.
5. MHC-DF (DF ID: B300) is selected on the MHC card using SELECT FILE command.
(APDU: 00A40002B300).
6. MHC SE FILE ID: B303 is selected on the MHC card using SELECT FILE command.
(APDU: 00A40002B303)
7. Send MSE RESTORE Command on MHC Card with SE Reference 02.
(APDU: 0022F302)
8. Send MSE SET Command on MHC Card USING URN NUMBER taken in step 4.
(APDU: 002281A4129410 & URN No. in Hex)
9. Send Get Challenge Command on MHC 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: 00C0000008)
 12. Send External Authentication Command on MHC Card using the response received in step 11 with key reference 81.
(APDU: 0082008108 & Response in Hex).

Successful External Authentication command verifies the keys 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 Card with 04.
(APDU: 0022F304)
16. Send MSE SET Command on MHC Card USING URN NUMBER
(APDU: 002241A4129410 & URN No. in Hex)
17. Send INTERNAL AUTHENTICATION Command ON MHC CARD USING CHALLENGE from step 14 with key reference 83.
(APDU: 0088008308 & Challenge in Hex)
18. Send Command to get Response from MHC 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 on the RSBY Card