

RASHTRIYA SWASTHYA BIMA YOJNA

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

Pre-Condition

A system with two card reader slots will be needed. The two cards MKC Card and the RSBY card are also required.

User Scenario

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

Application Specifications

1. MKC-MF (MF ID: 3F00) is selected on the MKC card using SELECT FILE command.
(APDU: 00A400023F00).
2. MKC-DF (MF ID: B100) is selected on the MKC card using SELECT FILE command.
(APDU: 00A40002B100).
3. Verify pin number 1 from KIOSK card.
(APDU: 0020008106 & Pin in Hex).
4. READ 16 Most Significant Byte of URN NUMBER FROM RSBY CARD.
5. Send MSE RESTORE Command on MKC Card with SE Reference 02.
(APDU: 0022F302)
6. Send MSE SET Command on MKC Card USING URN NUMBER taken in step 4 FOR EXTERNAL AUTHENTICATION.
(APDU: 002281A4129410 & URN No. in Hex)
7. Send Get Challenge Command on MKC Card.
(APDU: 0084000008)
8. Send INTERNAL AUTHENTICATION Command ON RSBY CARD USING CHALLENGE from step 8 and using key reference 81.
(APDU: 0088008108 & Challenge in Hex)

9. Send Command to get Response of length 8 bytes from RSBY Card.
(APDU: 00C0000008)
10. Send External Authentication Command on MKC Card using the response received in step 10 with key reference 81.
(APDU: 0082008108 & Response in Hex).

Successful External Authentication command verifies the keys on RSBY Card.

11. Send Select file Command with file ID E000 on RSBY Card.
(APDU: 00A40002E000)
12. Send Get Challenge Command on RSBY Card.
(APDU: 0084000008)
13. Send MSE RESTORE Command on MKC Card with 08.
(APDU: 0022F308)
14. Send MSE SET Command on MKC Card USING URN NUMBER FOR INTERNAL AUTHENTICATION
(APDU: 002241A4129410 & URN No. in Hex)
15. Send INTERNAL AUTHENTICATION Command ON MKC CARD USING CHALLENGE from step 13 with key reference 87.
(APDU: 0088008708 & Challenge in Hex)
16. Send Command to get Response from MKC Card.
(APDU: 00C0000008)
17. Send External Authentication Command on RSBY Card using the response received in step 17 with key reference 83.
(APDU: 0082008308 & Response in Hex).

Successful External Authentication command will now facilitate updation of EF's E005, E006, E007 & E008 on the RSBY Card