Hand Held Terminal Application Specifications
DL/RC ENDORSEMENT

Pre-Condition

A terminal with two card reader slots will be needed. EA card and the DL/RC card are also required.

The user of this application will be the Endorsing Authority.

Application Specifications

1. The application starts.

2. A screen appears asking the EA to insert the EA card in slot 1.

INSERT EA CARD IN SLOT 1

3. The EA inserts the EA card in the respective slot.

4. **DL**-EA-DF (DF ID: 4300) is selected on the EA card using **SELECT FILE** command.

5. EA is prompted for the DL-PIN and the same is verified using the **VERIFY** command with PIN number 1 in the EA card.

   Three cases arise:

   ?? PIN Verified
   ?? Incorrect PIN
   ?? PIN Block

6. If the PIN is verified then go to step 9.

7. If the PIN is not verified, i.e., the PIN is incorrect then the EA is prompted with the message **"Wrong PIN"**.

WRONG DL-EA-PIN. REENTER CORRECT PIN

8. If all the attempts are exhausted then the PIN is blocked and the same is conveyed to the EA and go to Step 2.

DL-EA-PIN BLOCKED Send the Card to SKMA for Unblocking.

9. DL-EA id is read from the EA info file (File ID: 4304) from EA card using **READ BINARY** command.

   The contents of the file will include the following as simple TLV data. (The entries in the Max size column are in shown in decimal numbers. All other entries are in hexadecimal number representation.)

Field	Tag	Max Size	Data Format	Example
Version	C0	4 bytes	String	C0 03 "1.00"
EA Name	C1	40 bytes	String	C1 10 "S Shiva Sundaram"
EA id	C2	16 bytes	String	C2 10 "KA003ST00124428Y"

10. RC-EA-DF (DF ID: 5300) is selected on the EA card using SELECT FILE command.

11. EA is prompted for the RC-EA-PIN and the same is verified using the VERIFY command with PIN number 1 in the EA card.

    Three cases arise:

    ??PIN Verified
    ??Incorrect PIN
    ??PIN Block

12. If the PIN is verified then go to step 15.

13. If the PIN is not verified, i.e., the PIN is incorrect then the EA is prompted with the message "Wrong PIN".

WRONG RC-EA-PIN. *REENTER CORRECT PIN*

14. If all the attempts are exhausted then the PIN is blocked and the same is conveyed to the EA and go to Step 2.

RC-EA-PIN BLOCKED *Send the Card to SKMA* *for Unblocking.*

15. EA is prompted to enter the Location of Endorsement.

Enter Location:

16. This location is stored for further use in the application.

17. EA id is read from the EA info file (File ID: 5304) using READ BINARY command.

    The contents of the file will include the following as simple TLV data. (The entries in the Max size column are in shown in decimal numbers. All other entries are in hexadecimal number representation.)

Field	***Tag***	***Max size***	***Data format***	***Example***
Version	*C0*	*4 bytes*	*String*	*C0 03 "1.00"*
EA Name	*C1*	*40 bytes*	*String*	*C1 10 "Abcdefghijk Lmno"*
EA id	*C2*	*16 bytes*	*String*	*C2 10 DL12345678901234"*

18. EA is prompted to insert the DL/RC card into the second slot.

INSERT DL/RC CARD
IN SLOT 2

19. The EA inserts the DL/RC card in the respective slot.

20. DL-DF (DF ID: 4000) is selected on DL card using the **SELECT FILE** command.

21. If SELECT FILE fails, then go to Step 52.

22. Personal Info file (File ID: 4004) is selected on the DL card using **SELECT FILE** command.

23. DL Number is read from DL personal info file (File ID: 4004) using **READ BINARY** command.

24. DL-EA-DF (DF ID: 4300) is selected on the EA card using SELECT FILE command.

25. MSE: **RESTORE** command is sent to EA card to restore SE#3.

26. MSE: **SET** command is sent to EA card to set DL Number for key derivation.

27. **GET CHALLENGE** command is sent to EA card to get a challenge of 8 bytes.

28. The challenge is passed as an argument to **INTERNAL AUTHENTICATE** (Key 84) command to the DL card.

29. Response from INTERNAL AUTH is passed to the EA card as an argument to the **EXTERNAL AUTHENTICATE** (key 82) command.

30. If EXTERNAL AUTH fails, then display a message that the DL card is not valid and go to step 18. Otherwise proceed to step 31.

31. Read Chip Serial Number from DL Card using GETDATA.

32. MSE: **RESTORE** command is sent to EA card to restore SE#2.

33. MSE: **SET** command is sent to EA card to set DL Number as the data for key derivation.

34. **GET CHALLENGE** command is sent to DL card to get a challenge of 8 bytes.

35. The response is sent to EA card as an argument to **INTERNAL AUTHENTICATE** (Key 81) command.

36. The response of the **INTERNAL AUTHENTICATE** is sent to DL Card as an argument to the **EXTERNAL AUTHENTICATE** command (Key 82).

37. If the External Auth is successful, then the EA is prompted to make a choice between viewing all the endorsement/review records and booking a new endorsement.

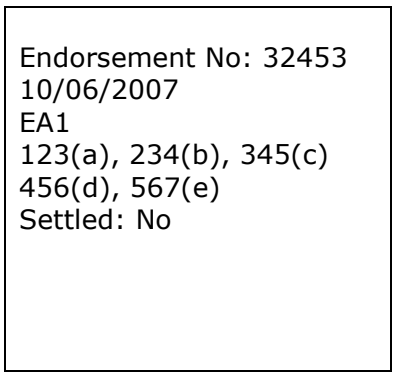
1. View all endorsements 2. Book an endorsement 3. Exit

38. If the EA selects to view the records then:

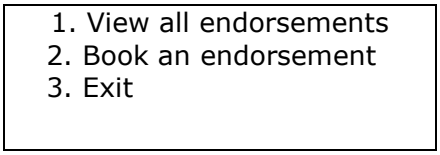
    All the Endorsements records are read from the DL card and displayed on the terminal as follows:

    The unsettled endorsements are displayed first. After all the unsettled endorsements are displayed, the settled ones are displayed. By matching the tags from 01 to 0A in the review file, all the settled records can be found out corresponding to each of the tags 01 to 0A in endorsement file. If the review date in the review file corresponding to an endorsement in the endorsement file is less than or equal to the endorsement date or zeroes, then that endorsement record is treated as unsettled one.

    These records can be scrolled to view one by one.



39. After viewing all the records, the previous screen is displayed.



40. If the EA chooses to book an endorsement then the following steps are carried out, otherwise the application stops.

41. Endorsement number file (ID: 4306) which is a Transparent working EF with 4 bytes file size is selected on EA card using SELECT FILE command. The file contains the endorsement number counter in 4 bytes (packed BCD format).

42. The last endorsement number used is read from this file using READ BINARY command.

Endorsement on DL Card

43. If there is any blank record (record with a tag value from 01 to 0A and length 0x5A and value all zeroes) out of 10 endorsement records on the DL Endorsement file on DL Card then:

    a. Endorsement EF (ID: 4006) is selected on the DL card by issuing the **SELECT FILE** command.

    b. The section and rule are required to be entered by the EA:

```
ENTER
SECTION/RULE/
PROCEEDING
SECTION: 454(1)

Enter 0 to exit.
```

A maximum of 10 sections/rules of 6 bytes each can be entered one by one. 43(b) is repeated till the EA enters 0 for exit.

c. A new record, in the form of a data object which includes endorsement number (the number read on step 42 plus one), current date, EA-ID read on step 9 and the sections entered in step 43(b) are written to the record found on step 43 on the DL-Endorsement file on DL Card using UPDATE BINARY. Go to Step 45.

44. If there are 10 endorsement records already present in the DL card's endorsement file then:

a. The earliest record, i.e., the endorsement record with the earliest endorsement date is searched. Then this record is checked for being a settled one or an unsettled one from the Review file.

b. If the earliest record is an unsettled one then the following screen is displayed:

```
NO MORE
ENDORSEMENTS
CAN BE MADE.

PLEASE SEIZE THE
CARD
```

And go to Step 18.

c. If the selected endorsement record is a settled one then this endorsement record is overwritten with the new endorsement record similar to Step 43 c. using **UPDATE RECORD** command**.**

EA Card Updation

45. Select the Endorsement File (ID: 4305) on EA Card using SELECT FILE command. This is a Transparent working EF with file size 2400 bytes. The file structure is as follows:

Field	**Tag**	**Max Size**	**Data Format**	**Example**
Version	C0	4 bytes	String	C0 03 "1.00"
Date	C1	4 bytes	Date	C1 08 23 02 19 99
DL Endorsement	C2	84 bytes	String	See explanation below

The version record will be the first record in the file. The DL endorsement record will have C2 as tag. There will be as many DL endorsement records as the number of endorsements made since last upload to the backend. Each endorsement will have the following format.

The version record will be the first record in the file. The DL endorsement record will have C2 as tag. There will be as many DL endorsement records as the number of endorsements made since last upload to the backend. Each endorsement will have the following format.

- DL number (16 characters)
- Endorsement Number (4 bytes in packed BCD format)
- ~~DL Card Chip Number (16 Bytes))(Do Not consider Now)~~
- 4 MSB (Most Significant Bytes) of MD5 hash of DL Card Chip No.
- Information for as many sections as the DL is booked for. Max 10 sections of 6 bytes each.

All endorsements made on a particular date will start with a date record followed by the DL endorsement records, one for each DL. A maximum of 66 endorsements can be made using an EA card in a day.

46. Check for C0 tag. If it is not present, write the version field with the C0 tag with value as 1.00.

    Search for the last C1 tag and read the value (date).

If this date is equal to today's date, then there is no need to write the date again. Go to the last C2 tag having non zero value. Find the offset of the new C2 tag to be written. Write the new data with a C2 tag, length and then the value containing DL number, endorsement number (in packed BCD), Chip serial number of DL card and Endorsement sections using UPDATE BINARY.

If the date read is not equal to today's date, then

Find the offset of the new C1 tag to be written. The value starts with a C1 tag, length as 4 bytes and value as today's date. Then the C2 tag, length and the value containing DL number, endorsement number (in packed BCD), Chip serial number of DL card and Endorsement sections using UPDATE BINARY.

Store the current offset (offset to write a new endorsement).

47. Endorsement number file (ID: 4306) is selected on EA card using SELECT FILE command.

48. The current endorsement number is padded with as many number of zeroes as required to the left and then written to the file using UPDATE BINARY.

49. Calculate the space remaining in the file = 2400 - Current offset.

    If the space remaining < 104 then a message is displayed as

    "Not enough space on EA Card to store further endorsements. Please upload the data to the backend database and clear the data in the EA card."

50. If the process is successfully completed, then a message is displayed.

DL ENDORSEMENT COMPLETED SUCCESFULLY

51. Remove DL card from the slot and Go to Step 18.

52. RC-DF (DF ID: 5000) is selected on RC card using the **SELECT FILE** command.

53. If SELECT FILE command fails, then a message is displayed as given below and goes to Step 18.

Not a Valid DL/RC Card

54. Personal Info file (File ID: 5003) is selected on the RC card using **SELECT FILE** command.

Field	**Tag**	**Max size**	**Data format**
Vehicle Registration Number	C0	10 bytes	String

55. RC Number is read from RC personal info file (File ID: 5003) using **READ BINARY** command.

56. **RC**-EA-DF (DF ID: 5300) is selected on the EA card using **SELECT FILE** command.

57. MSE: **RESTORE** command is sent to EA card to restore SE#3.

58. MSE: **SET** command is sent to EA card to set RC Number for key derivation.

59. **GET CHALLENGE** command is sent to EA card to get a challenge of 8 bytes.

60. The response from the GET CHALLENGE is passed as an argument to **INTERNAL AUTHENTICATE** (Key 81) command to the RC card.

61. Response from INTERNAL AUTH is passed to the EA card as an argument to the **EXTERNAL AUTHENTICATE** (key 82) command.

62. If EXTERNAL AUTH fails, then display a message that the RC card is not valid and go to step 18. Otherwise proceed to step 63.

63. MSE: **RESTORE** command is sent to EA card to restore SE#2.

64. MSE: **SET** command is sent to EA card to send RC Number as the data for key derivation.

65. **GET CHALLENGE** command is sent to RC card to get a challenge of 8 bytes.

66. The response is sent to EA card as an argument to **INTERNAL AUTHENTICATE** (Key 81) command.

67. The response of the **INTERNAL AUTHENTICATE** is sent to RC Card as an argument to the **EXTERNAL AUTHENTICATE** command (Key 8B).

68. The EA is prompted to make a choice between viewing all the endorsement/review records and booking a new endorsement.

1. View all endorsements
2. Book an endorsement
3. Exit

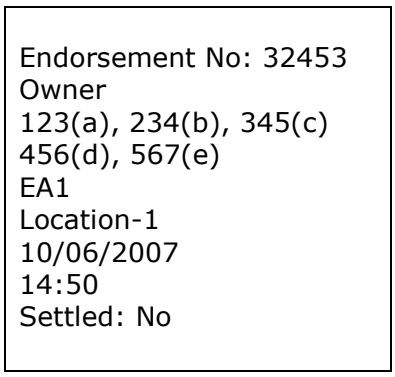
69. If the EA selects to view the records then:

    All the Endorsements records are read from the RC card and displayed on the terminal as follows:

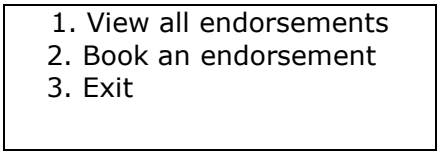
    The unsettled endorsements are displayed first. After all the unsettled endorsements are displayed, the settled ones are displayed. By matching the tags from 01 to 05, all the settled records can be found out corresponding to each of the tags 01 to 05 in endorsement file. If the review date in the review file corresponding to an endorsement in the endorsement file, is less than or equal to the endorsement date or zeroes, then that endorsement record is treated as unsettled one.

    The 'accused' field in the endorsement file will contain either 'D', or 'C' or 'O'. Accordingly Driver, Conductor or Owner is displayed for D, C, or O.

    These records can be scrolled to view one by one.



70. After viewing all the records, the previous screen is displayed.



71. If the EA chooses to book an endorsement then the following steps are carried out, otherwise the application stops.

72. Endorsement number file (ID: 5306) which is a Transparent working EF with 4 bytes file size is selected on EA card using SELECT FILE command. The file contains the endorsement number counter in 4 bytes (packed BCD format).

73. The last endorsement number used is read from this file using READ BINARY command.

Endorsement on RC Card

74. If there is any blank record (record with a tag value from 01 to 05 and length 0x45 and value all zeroes) out of 5 endorsement records on the RC Endorsement file on RC Card then:

    a. Endorsement EF (ID: 5008) is selected on the RC card by issuing the **SELECT FILE** command.

    b. The section and rule are required to be entered by the EA:

```
ENTER
SECTION/RULE/
PROCEEDING
SECTION: 454(1)

Enter 0 to exit.
```

A maximum of 5 sections/rules of 6 bytes each can be entered one by one. 74(b) is repeated till the EA enters 0 for exit.

c. The EA is prompted to enter the Accused.

```
Enter Accused:
D, C or O

(D – Driver,
 C – Conductor
 O – Owner)
```

d. A new record, in the form of a data object which includes endorsement number (the number read on step 73 plus one), 'D', 'C' or 'O' for Driver, Conductor or Owner, sections entered in step 74(b), EA-ID read on step 17, location entered in step 15 and the current date and time is written to the record found on step 74 on the RC-Endorsement file on RC Card using UPDATE BINARY. Go to Step 76.

75. If there are 5 endorsement records already present in the RC card's endorsement file then:

a. The earliest record, i.e., the endorsement record with the earliest endorsement date is searched. Then this record is checked for being a settled one or an unsettled one from the Review file.

b. If the earliest record is an unsettled one then the following screen is displayed:

```
NO MORE
ENDORSEMENTS
POSSIBLE.

PLEASE SEIZE THE
CARD
```

And go to Step 18.

c. If the selected endorsement record is a settled one then this endorsement record is overwritten with the new endorsement record similar to Step 74 d. using command **UPDATE RECORD.**

EA Card Updation

76. Select the Endorsement File (ID: 5305) on EA Card using SELECT FILE command. This is a Transparent working EF with file size 6350 bytes. The file structure is as follows:

Field	**Tag**	**Max size**	**Data format**	**Example**
Version	C0	4 bytes	String	C0 03 "1.00"
Date	C1	4 bytes	Date	C1 04 23021999
RC Endorsement	C2	60 bytes	String	See explanation below.

The version record will be the first record in the file. The RC endorsement record will have C2 as tag. There will be as many RC endorsement records as the number of endorsements made since last upload to the backend. Each endorsement will have the following format.

- Vehicle registration number (10 characters)
- Endorsement Number (4 bytes) in packed BCD format.
- ~~RC Card Chip Serial No. (16 Bytes)~~(Do Not consider Now~~)~~
- 4 MSB (Most Significant Bytes) of MD5 hash of RC Card Chip No.
- Information for as many sections as the RC is booked for. Max 5 sections each 6 bytes.

  All endorsements made on a particular date will start with a date field followed by the RC endorsement records, one for each RC.

77. Check for C0 tag. If it is not present, write the version field with the C0 tag with value as 1.00.

    Search for the last C1 tag and read the value (date).

    If this date is equal to today's date, then there is no need to write the date again. Go to the last C2 tag having non zero value. Find the offset of the new C2 tag to be written. Write the new data with a C2

tag, length and then the value containing Registration number, endorsement number (in packed BCD), Chip serial number of RC card and Endorsement sections using UPDATE BINARY.

If the date read is not equal to today's date, then

Find the offset of the new C1 tag to be written. The value starts with a C1 tag, length as 4 bytes and value as today's date. Then the C2 tag, length and the value containing Registration number, endorsement number (in packed BCD), Chip serial number of RC card and Endorsement sections using UPDATE BINARY.

Store the current offset (offset to write a new endorsement).

78. Endorsement number file (ID: 5306) is selected on EA card using SELECT FILE command.

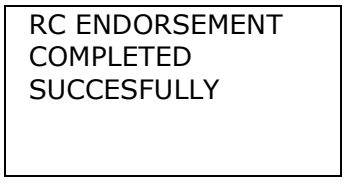
79. The current endorsement number is padded with as many number of zeroes as required to the left and then written to the file using UPDATE BINARY.

80. Calculate the space remaining in the file = 6350 - Current offset.

    If the space remaining < 62 then a message is displayed as

    "Not enough space on EA Card to store further endorsements. Please upload the data to the backend database and clear the data in the EA card."

81. If the process is successfully completed, then a message is displayed.



82. Remove RC card from the slot and Go to Step 18.