

MR Manual – MF Desfire

Visit us at www.mylab.my

Email: sales@mylab.my

Please email to us, to get a copy of the MR Program.



MR Manual – MF Desfire

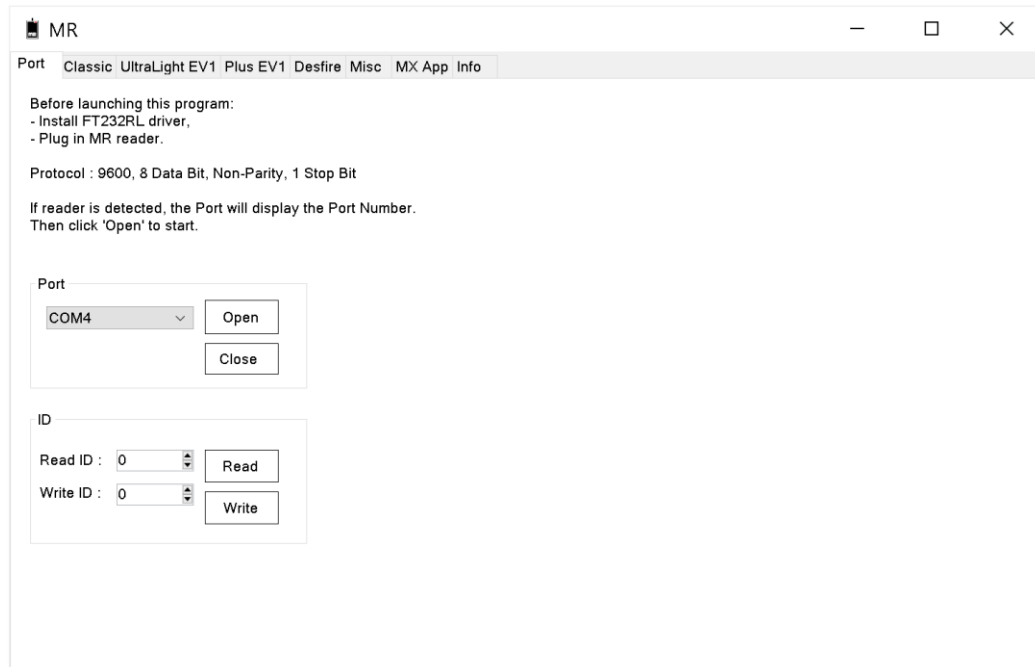
Contents

1. General.....	3
2. How to set to Read Serial Number mode	9
3. How to set to Read / Write mode.....	12
4. Mifare Desfire	13
5. Create Application	15
6. Standard / Backup File	19
7. TMAC.....	25
8. Value File.....	29
9. Linear Record File.....	33
10. Cyclic Record File	38
11. Change File Setting.....	44
12. Roll Key.....	48
13. Delegated Application (DAM)	49
14. Card Info.....	61
15. Change PICC Key	62
16. Change Application Key	64
17. AppDefaultKey	67
18. Proximity Check	69
19. Virtual Card	73
20. Random ID.....	76
21. ISODFName or VCIID	79
22. More on DAM Application	86
23. TroubleShooting.....	87
24. Important Summary of Keys	88
25. End	89

MR Manual – MF Desfire

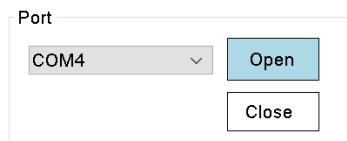
1. General

Plug in MR Reader then launch the MR Software.



Main screen.

If Serial Com Port available, or USB Virtual Com available, it will be shown on screen.



Select the port where reader is connected, then click  to open port.

Upon open port, reader will send command to get reader ID, and turn on the RF. Getting reader ID should be the first command to execute, because if the ID is not matched, reader will not response.

1.0 Protocol

To ease development, sending and receiving protocols are recorded and saved in the **C:\Mylab\MR** folder, as shown below:

Function : Open Port

6:47:51 PM, TX : 02 00 00 01 50 53 03

6:47:51 PM, RX : 02 00 00 02 00 00 00 03

6:47:51 PM, TX : 02 00 00 02 54 01 55 03

MR Manual – MF Desfire

They are briefly explained as below:

Communication Protocol:

Item	Value
Baud rate	9600
Data bit	8
Parity	None
Stop bit	1

For card related command:

TX : 02 / 00 / Reader ID / No of byte / Command / PICC Command / Data / BCC / 03

RX : 02 / 00 / Reader ID / No of byte/ Message / CSN length / Card Serial Number / Card Type / PICC Message / Data / BCC / 03

For hardware setting related command:

TX : 02 / 00 / Reader ID / No of byte / Command / Data / BCC / 03

RX : 02 / 00 / Reader ID / No of byte/ Message / Data / BCC / 03

Item	Length	Meaning
STX (Start of Text)	1	02 Hex
Master ID/MID	1	00 Hex
Reader ID/RID	1	00 – FF hex
No of byte/NOB	1	No of byte in TX Data or RX Data
Command/CMD	1	Refer manual or sending protocol 0 = none 15 hex = dfpicc_df_changemlk2 16 hex = dfpicc_df_mlk2 17 hex = change_vciid 18 hex = dfpicc_change_vciid 19 hex = dfpicc_changekey 1A hex = dfpicc_mylabkey 1E hex = dfpicc 2D hex = aesloadkey 2E hex = desloadkey 48 hex = areadsnr 49 hex = areadsnrsize 4A hex = rats 4B hex = pcdtopicc 4D hex = picctransparent 50 hex = read_id 51 hex = write_id 54 hex = control_rf 6A hex = read_setting 6B hex = write_setting 6D hex = control_beep_led 6E hex = control_beep 6F hex = control_led F0 hex = read_version FC hex = DFDirectKey2

MR Manual – MF Desfire

		FD hex = DFDirectKey
PICC Command	1	Refer manual or sending protocol 0A hex = authenticate 1A hex = authenticateiso AA hex = authenticateaes 54 hex = changekeysettings 55 hex = rollkeyset 56 hex = initializekeyset 57 hex = finalizekeyset 5C hex = setconfiguration C4 hex = changekey C6 hex = changekeyev2 64 hex = getkeyversion C9 hex = createdelegatedapplication CA hex = createapplication DA hex = deleteapplication 69 hex = getdelegatedinfo 6A hex = getapplicationsids 6E hex = freememory 6D hex = getdfnames 45 hex = getkeysettings 5A hex = selectapplction FC hex = formatpicc 60 hex = getversion 51 hex = getcarduid 6F hex = getfileids F5 hex = getfilessettings 5F hex = changefilessettings CE hex = createtransactionmacfile CD hex = createstddatafile CB hex = createbackupdatafile CC hex = createvaluefile C1 hex = createlinearrecordfile C0 hex = createcyclicrecordfile DF hex = deletefile 61 hex = getisofileids BD hex = readdata 3D hex = writedata 6C hex = getvalue 0C hex = credit DC hex = debit 1C hex = limitedcredit 3B hex = writerecord BB hex = readrecords EB hex = clearrecordfile C7 hex = committransaction C8 hex = commitreaderid A7 hex = aborttransaction AF hex = additional_frame
Message/MESG	1	00 – Success, others – Error
CSN length/CSNL	1	0 or 4 or 7 (when 0, there is no serial number returned, hence the Card Serial Number and Card Type column will not be available in the RX

MR Manual – MF Desfire

		protocol too.)
Card Serial Number/CSN	4 or 7	4B or 7B CSN
Card Type/CT	1	Refer Mifare Card Information 08 hex = Mifare Classic 18 hex = Mifare Plus (SL1 or Mixed mode) 20 hex = Mifare Plus (SL3) 20 hex = Mifare Desfire
PICC Message/PMESG	1	00 hex – Success (CSN length > 0), 0C hex – NO_CHANGE 0E hex – OUT_OF_MEMORY_ERROR, 1C hex – ILLEGAL_COMMAND_CODE, 1E hex – INTEGRITY_ERROR, 40 hex – NO_SUCH_KEY, 7E hex – LENGTH_ERROR, 9D hex – PERMISSION_DENIED, 9E hex – PARAMETER_ERROR, A0 hex – APPLICATION_NOT_FOUND, AE hex – AUTHENTICATION_ERROR, AF hex – ADDITIONAL_FRAME, BE hex – BOUNDARY_ERROR, CA hex – COMMAND_ABORTED, DE hex – DUPLICATE_ERROR, EE hex – MEMORY_ERROR, F0 hex – FILE_NOT_FOUND, others – Error 0B hex – ErrCmdInvalid 07 hex – ErrCmdOverflow 0C hex – ErrFormat 90 hex - OK
Data	variable	Transmit or Received string
DF Name	17	1B length, 16B DF Name (If Virtual Card is enabled)
BCC	1	Exclusive-Or from byte SOF to Last Byte of Data
ETX (End of Text)	1	03 Hex

1.1 Reader ID

The default reader ID is 00, it can be changed to other value. In RS485 or multi-drop application, reader with different ID is needed to ensure proper communication.

To set ID value, enter a value in the Write ID numeric box, and then create 'Write'. After you changed the ID, remember to click Read to get the new reader ID, or manually update the read ID numeric box. If not, communication may be fail because the ID in the program is different from the ID in the reader. Therefore, always get the reader ID first before proceeding further.

The value will be saved in the non volatile memory.

ID

Read ID :

Write ID :

1.2 Beep

There are two beep mode available; beep only and beep with LED. Beep with LED will generate beep sound and trigger the on board LED. Multiple beeps can be generated by setting the 'No of beeps' and 'Beep length'.

The screenshot shows the MR software interface with the 'Beep' section selected. The 'No of beeps' is set to 3 and 'Beep Length' is set to 2. The 'Beep' button is highlighted. The 'Auto Read Setting' section is also visible, showing various checkboxes for settings like 'Set to Read CSN mode', 'Blink LED after CSN detected', etc. The 'RF' section at the bottom shows 'RF ON' and 'RF OFF' buttons.

Click will generate 3 beeps.

1.3 RF

No communication between card and reader is possible when the RF is turned off. Therefore, it is important to ensure the RF is turned on when accessing the card. By default, the RF is on.

Sometimes it may be necessary to control the RF to reset the card in the field.

RF

To reset RF in the reader field, click , and then click .

1.4 Reader Internal EEPROM

The hardware settings, and the authentication keys are saved into the internal EEPROM by using instruction. This is a non-volatile memory, the content will be kept even though power is removed.

Due to security reason, the authentication keys are not readable.

- Please bear in mind that EEPROM is intended to provide nonvolatile storage for configuration data and settings that do not need to change frequently. If an application program were to write to an EEPROM cell frequently it would quickly wear it out, shorten the lifetime of the product.

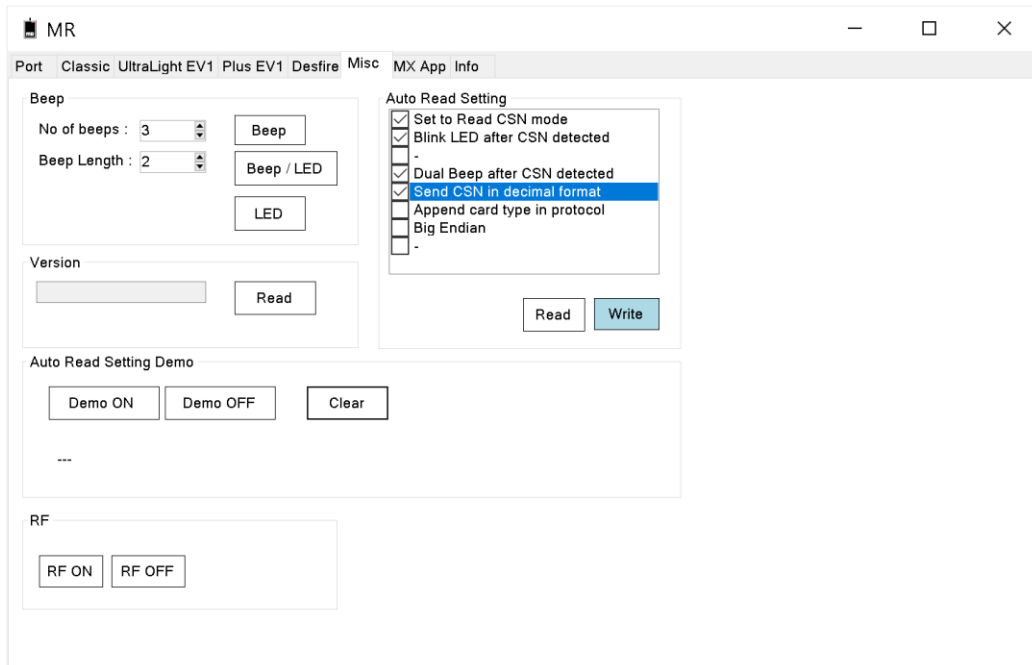
1.5 Remark

After a Mifare card's sector has been authenticated successfully, the sector will be opened, and read or write is permitted. The card will remain in the 'Open' state until the RF field is reset, or the card is removed from the RF area, then a new authentication is needed.

In the examples given below, the testing result may be different if the RF reset is not performed after changing Key or changing authentication method. Therefore, if the testing result is different from the given answer, kindly reset the RF by calling command 'RF Off' and 'RF On', or merely remove the card from reader, and then put back the card on the reader. The author has omitted this, to avoid duplicated words and for easy reading. It is also recommended to perform RF reset prior to create new application or new file.

2. How to set to Read Serial Number mode

By default the reader is in Read/Write mode. User can switch the reader to work on Auto Read Serial Number mode by checking the following box. Both 4B and 7B serial number lengths are supported.



The above setting will switch the reader to work on Read Serial Number mode. When a valid card is detected, it will blink LED, sound two beeps, and send the serial number to Host in decimal and Little Endian format.

Available functions:

- Set to Read Card SNR mode – Enable Read Serial Number mode, default is Read / Write mode.
- Blink LED after SNR detected – Blink LED when a valid card is detected.
- Dual Beep after SNR detected – Sound dual beep when a valid card is detected.
- Send SNR in Decimal format – Send Serial Number in decimal format, default is sending Serial Number in Hex format.
- Append Card Type in protocol – Append card type in the protocol. Only if Hex format is enabled, or 'Send SNR in Decimal format' is unchecked.
- Big Endian – Send Serial Number in Big Endian format, default is sending Serial Number in Little Endian format.

We will try it now by setting the check box as shown below:

MR Manual – MF Desfire

Auto Read Setting

☒	Set to Read CSN mode
☒	Blink LED after CSN detected
☐	-
☒	Dual Beep after CSN detected
☒	Send CSN in decimal format
☐	Append card type in protocol
☐	Big Endian
☐	-

Read Write

Click **Write** to send the check box setting to reader.

We will see how it works now by turning on the Demo mode.

Auto Read Setting Demo

Demo ON Demo OFF Clear

33 36 31 33 33 33 31 37 33 36 34 35 36 36 32 37 36 0D 0A

Click **Demo ON** to detect any valid card in the RF field. If available, display the Serial Number in decimal format, blink LED, and sound dual beep.

You may refer Activity text file in C:\Mylab\MR, for detailed protocol received string.

Function : Write Card Setting

12:08:47 PM, TX : 02 00 00 02 6B 1B 70 03

12:08:47 PM, RX : 02 00 00 01 00 03 03

Function : Demo On

12:08:55 PM, RX : 32 34 31 38 31 34 32 31 39 30 0D 0A

12:08:57 PM, RX : 33 36 31 32 35 32 32 36 33 32 33 38 30 31 38 36 30 0D 0A

12:09:07 PM, RX : 33 36 31 33 33 33 31 37 33 36 35 35 34 39 33 31 36 0D 0A

Turn off the demo now by clicking **Demo OFF**, and try another setting as shown below:

Auto Read Setting

☒	Set to Read CSN mode
☒	Blink LED after CSN detected
☐	-
☒	Dual Beep after CSN detected
☐	Send CSN in decimal format
☒	Append card type in protocol
☒	Big Endian
☐	-

Read Write

Click **Write** to send the check box setting to reader. This setting will include the card type in protocol.

MR Manual – MF Desfire

Auto Read Setting Demo

02 00 00 09 00 04 49 12 8A 0F 5F 80 20 2E 03

Click to detect any valid card in the RF field. If card available, it will return the Serial Number in Hex format, append the card type in the protocol, blink LED, and sound beep. As shown in the protocol 02 00 00 09 00 04 49 12 8A 0F 5F 80 20 2E 03, the card type is 20 hex. Refer Chapter 1-0 Protocol, we know that the card is Mifare Desfire or Mifare Plus (SL3).

Always remember to turn off the demo by clicking .

The setting will be stored as non volatile in the reader's memory.

3. How to set to Read / Write mode

By default the reader is in Read/Write mode. If the reader has been set to Auto Read Serial Number mode, we can switch it back to Read/Write mode by un-checking all the items in the following box, then click .

Auto Read Setting

☐ Set to Read CSN mode

☐ Blink LED after CSN detected

☐ -

☐ Dual Beep after CSN detected

☒ Send CSN in decimal format

☐ Append card type in protocol

☐ Big Endian

☐ -

Read

Write

The reader is now in Read/Write mode.

The reader must be in the Read/Write mode in order to follow the examples in the chapters that follow.

The setting will be stored as non volatile in the reader's memory.

4. Mifare Desfire

Click the Desfire tab now to enter the page. This program will show you how to access Mifare Desfire card.

The screenshot shows the MR software interface with the Desfire tab selected. The interface is divided into several sections: Application, Directory, File, Key, PICC, Roll Key (EV2), and Misc. The Application section contains fields for App ID, App Type, Current PICC KeyType, Current PICC Key, Default App Key, Old VCCConfig Key, New VCCConfig Key, File Type, DF Name, Key 0, and Key 1. The Directory section contains a DAM Slot field and a KeySet dropdown. The File section contains KS0 Key 0, KS0 Key 1, KS1 Key 0, KS1 Key 1, KS2 Key 0, and KS2 Key 1 fields. The Key section contains buttons for Create App and Files, Delete App, Save New PICC, DAM, and Current Active Keys to Reader, and Create Files Only. The Access Method section at the bottom shows ProximityCheck, VirtualCard, PICC, and AES EV1 options.

Desfire main screen.

4.0 Access Method

To access the MF Desfire card content, a successful authentication is necessary. The card is protected by 16B AES Key, and by default they are all 00 hex. If the Key does not match, an error code will be returned. Before authentication can be successful, a Save Key command to load the authentication key to the reader is required. The key will be stored in non volatile memory.

When the card is new, it is in DES mode. For higher security, we will switch it to AES mode, and then the authentication will be done in AES key. We will use AES mode in all our examples below.

Since many applications can be created in a Mifare Desfire card, so when accessing the card, it is necessary to specify the application, the authentication key, and whether ProximityCheck, or VirtualCard is enabled. The access will fail if the selection is not correct.

The screenshot shows the Access Method section of the MR software interface. It includes a dropdown menu for PICC with the following options: PICC, Conventional 100, Conventional 101, Conventional 102, DAM 110+, DAM 111, Conventional 1, and Conventional 2. The current selection is App 1, Key0.

The info label shows the current selected application, and the authentication key. When accessing an application in the card, if the selected application in the info label is different from the application you want to access, you may

see different result. So make sure you specify the application, and the informations shown in the info label are correct.

4.1 Load Key 16B or 24B

Since we are going to use 16B AES key for authentication throughout our examples, our UI will show only 16B key data in 'Load Key' or 'Save Key' portion. Due to card compatibility to the old DES format, the protocol will display 24B data. The preceding 16B are the real AES Key, and the succeeding 8B are dummies.

4.2 Before we start

As mentioned, authentication is required before you can perform any read and write access. If you want to access certain file, and the file requires certain key for authentication, then first you need to load the key to reader. If both the reader's key and the card's key are matched, authentication will be successful. Else an error will be returned.

Some features described in this document may not available in Desfire EV1 card.

MR Manual – MF Desfire

5. Create Application

We will use a new Mifare Desfire EV2 card in the examples below.

The default card type for a new card is DES, and the default PICC key is 16B 00 hex.

We will create a simple application on the card. The application will have the following spec:

Item	Value	Remark
App ID	1	Cannot be 0, as 0 is reserved for PICC level.
App Type	Conventional	Either Conventional or DAM.
Current PICC Key Type	DES (New)	If the card is in AES mode, select AES.
Current PICC Key	24B 00 hex	Default value. For New card, the DES key is 24B. If the Key Type is AES, enter 16B.
Default App Key	00000000000000000000000000000000	Can be other value, or user define.
Old VConfig Key	00000000000000000000000000000000	Default value
New VConfig Key	00000000000000000000000000000000	Can be other value, or user define.
File Type	Standard [1], Backup [2], Value [3], Linear [5], Cyclic [6], TMAC [7].	Select the file that you want to create. We select 5 files for demo purpose. The more file you select, the more space it will occupy.
DF Name	Conventional 1	Auto generated.
New App KS0 Key 0	A0000000000000000000000000000000	Can be other value, or user define.
New App KS0 Key 1	A1000000000000000000000000000000	Can be other value, or user define

Before we click the button to start, it is good to know what this process does. It involves the following:

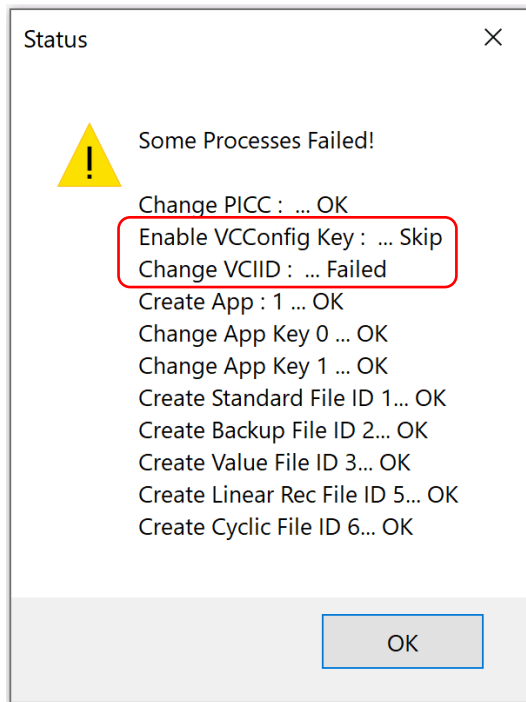
- Change the PICC Key and switch the KeyType from DES to AES. (It is OK if the card is already in AES mode.),
- Enable the VConfigKey with new VConfig key,
- Change the VCIID to 'PICC',
- Create App,
- Change the App Key,
- Create the file(s).

This Conventional application will create 5 files;

- Standard file (File ID 1), 32Byte,
- Backup file (File ID 2), 32 Byte,
- Value file (File ID 3), Free Get Value,
- Linear file (File ID 5), Max 4 Records,
- Cyclic file (File ID 6), Max 4 Records,
- TMAC file (File ID 7).

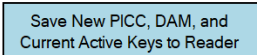
The app will have two keys; Key 0, and Key 1. Key 0 will be used as authentication key when we perform Read. Key 1 is mainly for Write and Change Key.

Set the fields as shown in the diagram below, select PICC in the application field, and uncheck all the items in the Access Method:

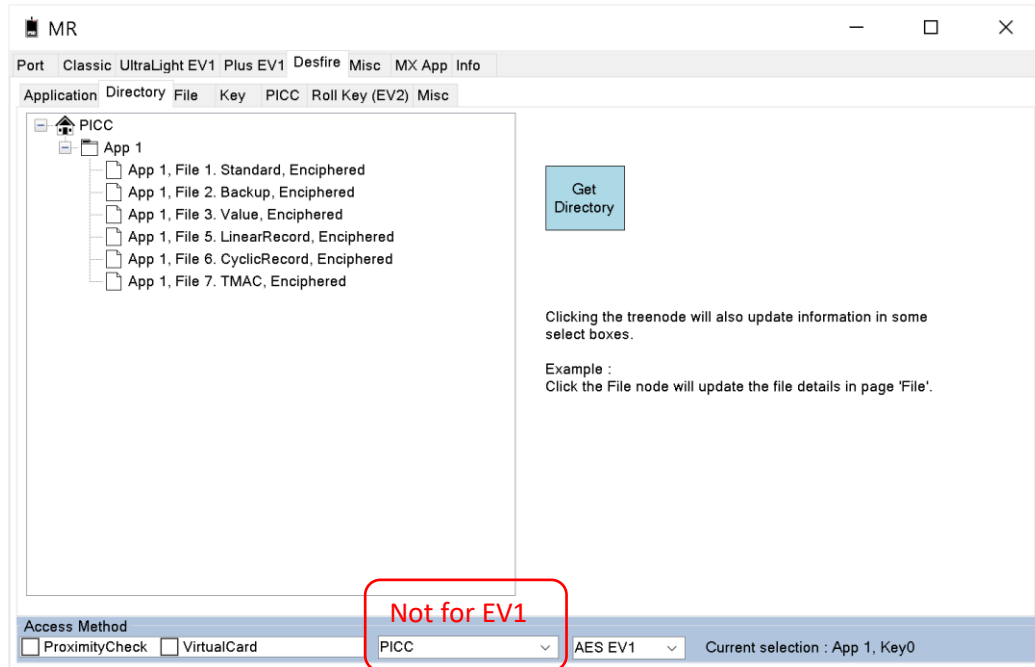


But you will still be able to access most of the features describe in this manual later. So it is okay to use EV1 card.

Now, we save the new PICC key, the Register keys, and the App keys to the reader. The keys are stored in non-volatile memory. We will use the stored key for authentication when we access the card later.

Click  button to save the key now.

Go to page Directory and click  to view the card contents.



The card has one app and six files now.

Please note that Desfire EV1 card does not support DFNames. You will see PICC only in this field.

Before we leave this chapter, we update the details of our newly created app.

Item	Value	Remark
App ID	1	
App Type	Conventional	
Current PICC Key Type	AES	Newly change.
Current PICC Key	00000000000000000000000000000000	
VCCConfigKey	00000000000000000000000000000000	Enabled.
New App KS0 Key 0	A0000000000000000000000000000000	
New App KS0 Key 1	A10000000000000000000000000000000	
File Type	Standard [1], Backup [2], Value [3], Linear [5], Cyclic [6], TMAC [7]	
DF Name	Conventional 1	

We will show you how to use the files that we just created in the following chapters.

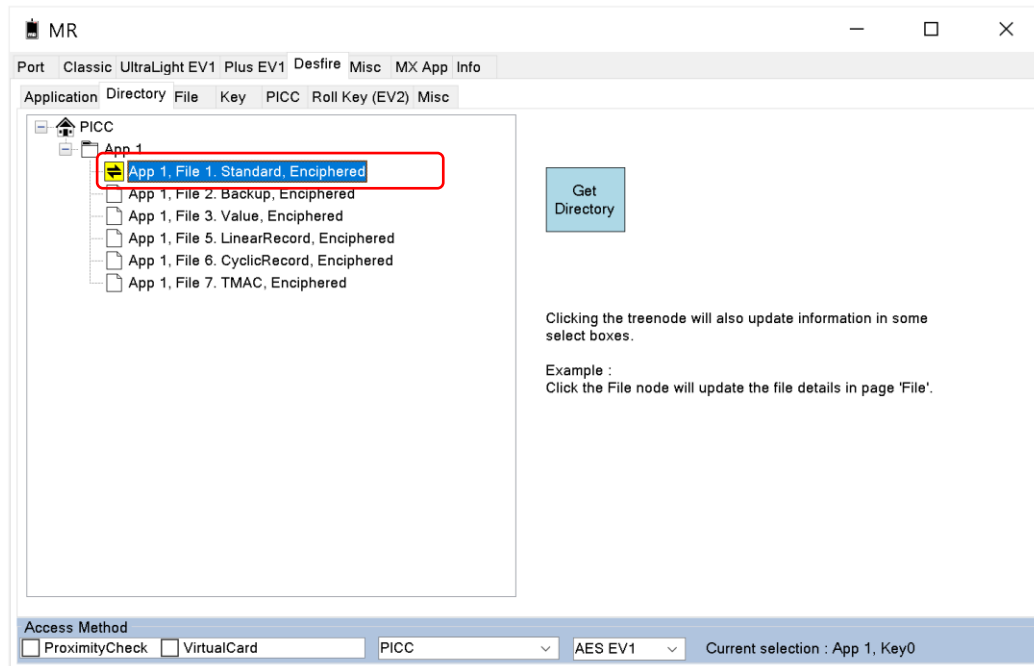
Please refer <C:\Mylab\MR> for details communication flow.

6. Standard / Backup File

In the previous chapter, we have created a Standard and a Backup file in App 1. Now we will write few data to the file, and then read them back to verify.



Go to page Directory, and click button. The card content will appear as shown below:



Click on File 1, then go to page File, page Data.

Some file details are shown in the screen; the current app (App 1), the File ID (1), File Type (Standard), and File Option (Enciphered).

The screenshot shows the MR software interface with the following settings:

- App ID: 1
- App Key: Default Key
- File ID: 1
- File Type: Standard
- File Option: Enciphered
- Offset: 0
- Length: 5 (highlighted with a red box)
- Data: 0011223344 (highlighted with a red box)
- Value: 0
- Commit: No
- TMC / TMV: No

The 'Write Data/Rec' button is highlighted in the 'Standard / Backup / Cyclic / Linear File' section. The 'Current selection : App 1, Key1' label is also highlighted in the bottom right corner.

Set the field Length to 5, and enter five byte data 0011223344 (hex) in field Data. Select No in field Commit. Click **Write Data/Rec**, to write 5B data to the Standard file.

When we created the app in the previous chapter, we have set Key 0 for Read, and Key 1 for Write and Change Key. So when performing Write function, the reader will authenticate with Key 1, not Key 0, as can be seen in the info label.

Now we click **Read Data/Rec** to read 5B of data from Standard File.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 1

File Type : Standard

File Option : Enciphered

Offset : 0

Length : 5

Data : 0011223344

Value : 0

Commit

No

TMC / TMV

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1 Current selection : App 1, Key0

The data was written successfully. Both Read and Write work, there is no need for Commit, to update the memory to card.

Now we will try Backup File. Go to the page Directory, and click on File 2. The Backup file details are shown as follow:

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

PICC

App 1

App 1, File 1. Standard, Enciphered

App 1, File 2. Backup, Enciphered

App 1, File 3. Value, Enciphered

App 1, File 5. LinearRecord, Enciphered

App 1, File 6. CyclicRecord, Enciphered

App 1, File 7. TMAC, Enciphered

Get Directory

Clicking the treenode will also update information in some select boxes.

Example :
Click the File node will update the file details in page 'File'.

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1 Current selection : App 1, Key0

MR Manual – MF Desfire

The screenshot shows the MR application window with the 'Data' tab selected. The 'Length' field is set to 5 and the 'Data' field contains '0011223344'. The 'Write Data/Rec' button is highlighted. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' as options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

Click button **Write Data/Rec** to write 5B of data to the file, and then click button **Read Data/Rec** to read.

The screenshot shows the MR application window with the 'Data' tab selected. The 'Length' field is set to 5 and the 'Data' field contains '0000000000'. The 'Read Data/Rec' button is highlighted. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' as options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

But the returned data shows the previous data was not updated.

Now we will perform Commit Transaction after the write command.

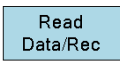
MR Manual – MF Desfire

The screenshot shows the MR software interface with the 'Data' tab selected. The 'Length' field is set to 5 and the 'Data' field contains '0011223344'. The 'Commit' button is highlighted. The interface includes various tabs like Port, Classic, UltraLight EV1, Plus EV1, Desfire, Misc, MX App, and Info. The 'Data' tab has sub-tabs for Add/Delete, File, Key, PICC, Roll Key (EV2), and Misc. The 'Data' section has fields for App ID, App Key, File ID, File Type, File Option, Offset, Length, and Data. The 'Commit' section has buttons for Commit, Abort, and Commit (TMAC). The 'Access Method' section at the bottom has checkboxes for ProximityCheck and VirtualCard, and dropdowns for PICC and AES EV1.

Enter 5B data into Data field, click  button, and then click  button to update the changes to card.

We read the Back up file again.

The screenshot shows the MR software interface with the 'Data' tab selected. The 'Length' field is set to 5 and the 'Data' field contains '0011223344'. The 'Read Data/Rec' button is highlighted. The interface is identical to the previous screenshot, but the 'Read Data/Rec' button is now highlighted instead of the 'Commit' button.

Click  to read the Backup file. This time, the Write function was successful.

MR Manual – MF Desfire

Therefore, the Backup file requires an extra Commit transaction command, in order to update the data to card.

Function : Desfire Get Directory

Please refer [C:\Mylab\MR](#) for details communication flow.

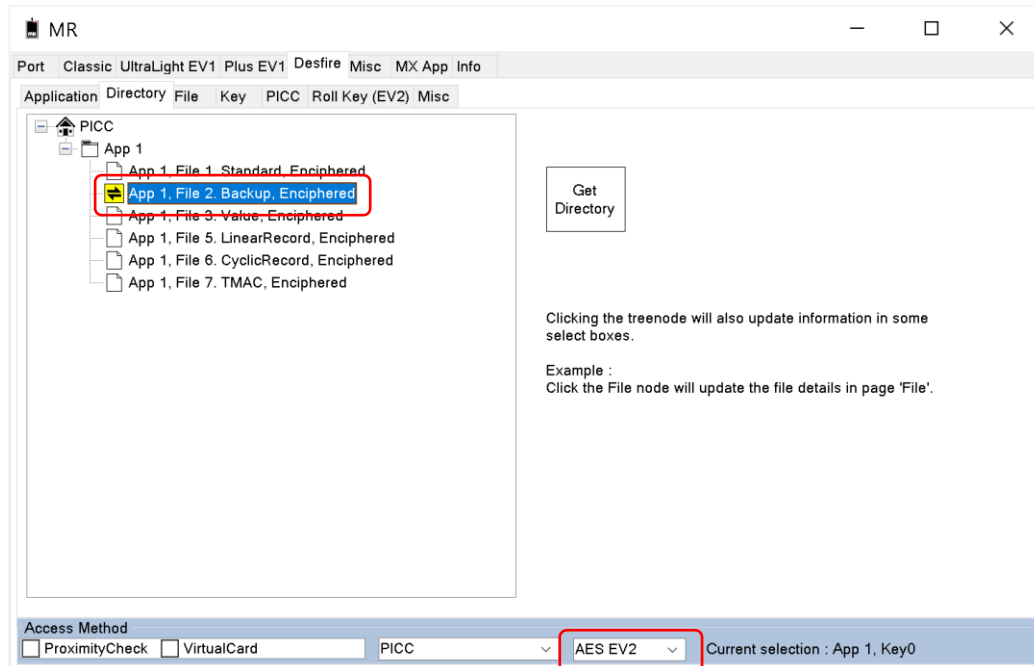
7. TMAC

This feature is not available in EV1 card.

This feature allows a third party to check the authenticity of a transaction and to detect fraudulent scenarios, using the returned TMC/TMV after every transaction.

In the previous chapter, we have created a TMAC file in App 1 application. We will see how it works now.

Go to the page Directory, and click on File 2. The Backup file details are shown as follow:



Since TMAC is not available in EV1, we will select AES EV2, in the Access Method select box, then Commit (TMAC) button will be enabled.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 5

Data : 0123456789

Value : 0

Commit

No

TMC / TMV

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard ☐ PICC ☐ AES EV2

Current selection : App 1, Key0

Input data in the Data field, and click button **Write Data/Rec** to write them to the file.

Recall from the previous chapter that Backup file requires a Commit transaction command before the written data can be updated to card. But this time, instead of Commit, we will click **Commit (TMAC)** button.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 5

Data : 0123456789

Value : 0

Commit

No

02000000 DCC0E4DC48D77473

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard ☐ PICC ☐ AES EV2

Current selection : App 1, Key0

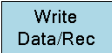
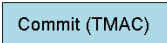
If the command is successful, the written data will be updated to card memory, and the reader will return 4B TMC, and 8B TMV, as shown above.

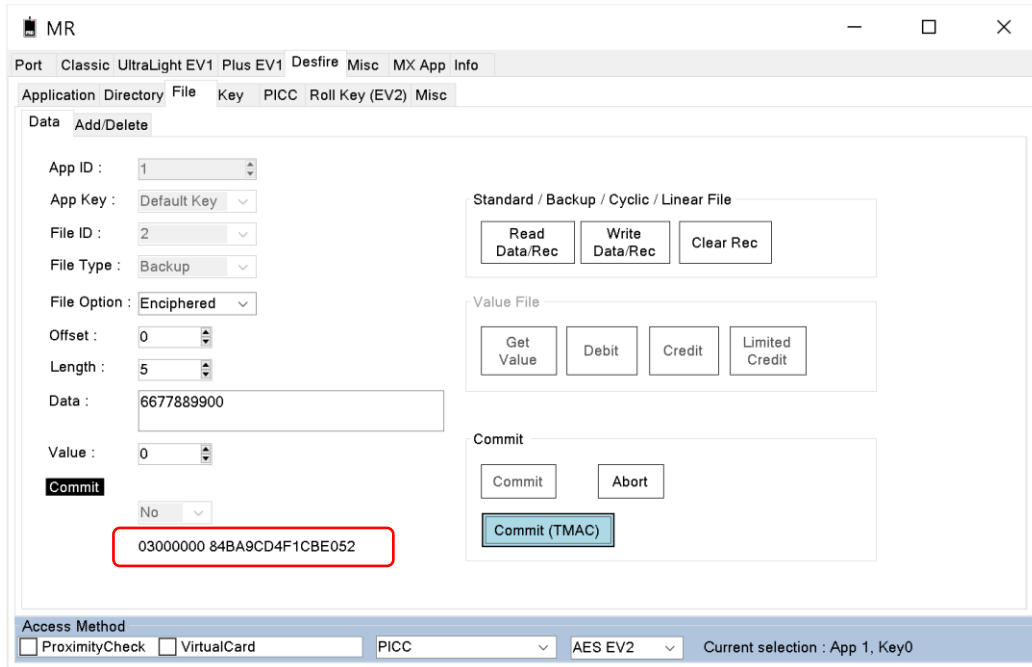
MR Manual – MF Desfire

After adding TMAC file in the application, the reader will return TMC/TMV after every successful update of memory.

The TMC (TMAC Counter) is 02000000 hex (LSB to MSB), means the card memory has been updated two times. This counter will increase every time when we perform memory update to card.

TMV, stands for TMAC value, is an encrypted value of the TMAC operation. Please refer manual for details.

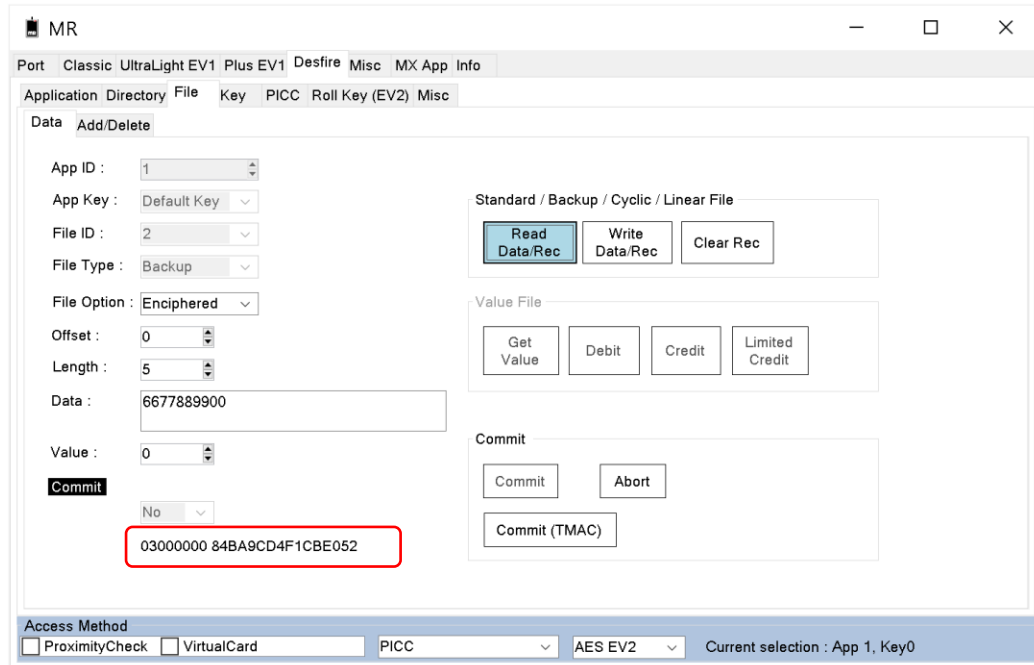
Try input data '6677889900', click , and then click  again.



The screenshot shows the MR application window with the following details:

- Port:** Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info
- Application:** Directory File Key PICC Roll Key (EV2) Misc
- Data Add/Delete:**
 - App ID: 1
 - App Key: Default Key
 - File ID: 2
 - File Type: Backup
 - File Option: Enciphered
 - Offset: 0
 - Length: 5
 - Data: 6677889900
 - Value: 0
 - Commit** button
 - Value field: 03000000 84BA9CD4F1CBE052 (highlighted with a red box)
- Standard / Backup / Cyclic / Linear File:**
 - Read Data/Rec
 - Write Data/Rec
 - Clear Rec
- Value File:**
 - Get Value
 - Debit
 - Credit
 - Limited Credit
- Commit:**
 - Commit
 - Abort
 - Commit (TMAC)** button
- Access Method:**
 - ☐ ProximityCheck ☐ VirtualCard
 - PICC
 - AES EV2
 - Current selection : App 1, Key0

Please note that the TMC has incremented by 1 to 03000000 hex, and the TMV has changed to 84BA9CD4F1CBE052 hex.



But there is no TMC/TMV returned when we do 'Read', as this command does not involve update memory.

Same as 'Write', TMC will be incremented when we perform Value operation, like 'Debit', and 'Credit'.

The advantage of TMAC file is the ability to keep track of the number of memory update the application has been accumulated since its creation. It may be necessary for some offline applications where real time tracking is not available.

But if TMC/TMV is not required, then it is not necessary to create TMAC file in the application.

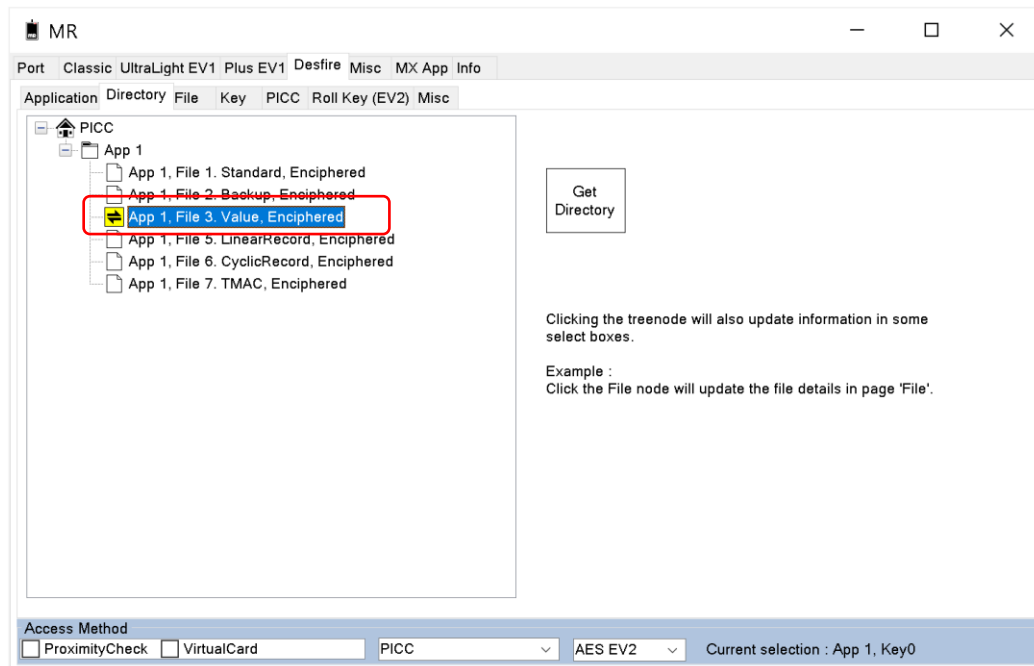
Please refer <C:\Mylab\MR> for details communication flow.

8. Value File

Value file stores data as 4B signed integer. It implements backup mechanism. All operation requires Commit Transaction in order to update the value to file, just like the Backup file we discussed in the last chapter.

In the previous chapter, we have created a Value file in App 1. Now we will perform Credit, Debit to the file, and then read them back to verify.

Go to page Directory, and click  button. The card content will appear as shown below:



Click on File 3 to select Value file, and then go to page File, page Data.

Some file details are shown in the screen; the current app (App 1), the File ID (3), File Type (Value), and File Option (Enciphered).

When we create the Value file, we have set the register so that Plain read is allowed. That means we can read out the data in Value file without any encryption.

The screenshot shows the MR software interface with the 'Data' tab selected. The 'App ID' is set to 1, 'App Key' to Default Key, 'File ID' to 3, 'File Type' to Value, and 'File Option' to Plain. The 'Data' field is highlighted with a red box and contains the hex value 00000000. The 'Value' field is set to 0. The 'Commit' button is visible. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

Click  to read data from Value file. The returned 4B data is 00000000 hex.

Now we will Credit a value of 10 to the file, and then click  again to verify.

Remember that Value file implements backup mechanism, so after clicking  or , Commit is required to update data to memory.

MR Manual – MF Desfire

The screenshot shows the MR software interface with the 'Data' tab selected. The 'File Option' dropdown is set to 'Enciphered' and the 'Value' dropdown is set to 10. The 'Data' field displays '00000000'. The 'Commit' button is highlighted. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' checkboxes, 'PICC' selected in the dropdown, and 'AES EV1' selected in the dropdown. The 'Current selection' is 'App 1, Key0'.

Set the File Option to Enciphered, click , and then click  button.

The screenshot shows the MR software interface with the 'Data' tab selected. The 'File Option' dropdown is set to 'Plain' and the 'Data' field displays '0A000000'. The 'Value' dropdown is set to 10. The 'Commit' button is highlighted. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' checkboxes, 'PICC' selected in the dropdown, and 'AES EV1' selected in the dropdown. The 'Current selection' is 'App 1, Key0'.

Click button  to read the Value file, the returned data 0A000000 hex, which is equivalent to 10 decimal.

Now we try Debit a value of 4 to the file, and then Get Value to read the balance.

MR Manual – MF Desfire

The screenshot shows the MR application window with the 'Data' tab selected. The 'File Option' is set to 'Enciphered' and the 'Value' is set to 4. The 'Data' field shows '0A000000'. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' as options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

Click  and then  to debit value 4.

The screenshot shows the MR application window with the 'Data' tab selected. The 'File Option' is set to 'Plain' and the 'Data' field shows '06000000'. The 'Value' is set to 4. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' as options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

Click , the returned 4B data shows the file balance is 06000000 hex.

Please refer <C:\Mylab\MR> for details communication flow.

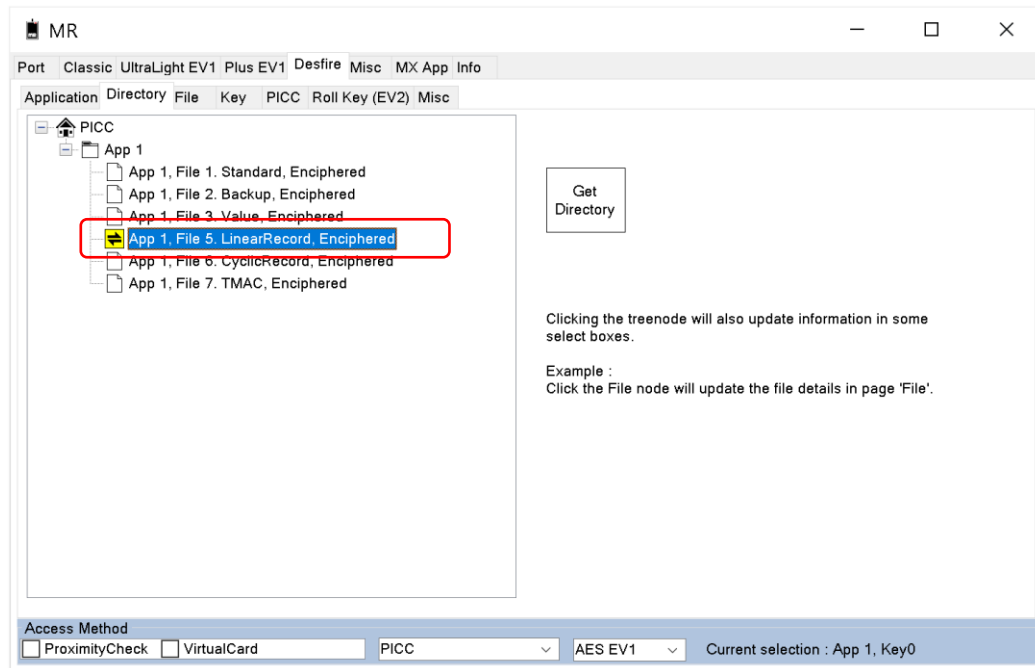
9. Linear Record File

Linear Record file add records to file. It implements backup mechanism. Commit Transaction is required in order to update the record to file.

In the previous chapter, we have created a Linear Record file in App 1. Now we will add few records to the file, and then read them back to verify.

Get
Directory

Go to page Directory, and click . The card content will appear as shown below:



Click on File 5 to select LinearRecord file, and then go to page File, page Data.

Some file details are shown in the screen; the current app (App 1), the File ID (1), File Type (Standard), and File Option (Enciphered).

Now we will add two records to the file, each 16B:

1. 11111111111111111111111111111111 hex,
2. 22222222222222222222222222222222 hex.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 5

File Type : LinearRecord

File Option : Enciphered

Offset : 0

Length : 16

Data : 11111111111111111111111111111111

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard ☐ PICC ☐ AES EV1

Current selection : App 1, Key1

Click **Write Data/Rec** and then **Commit** to add first 16B record to Linear file.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 5

File Type : LinearRecord

File Option : Enciphered

Offset : 0

Length : 16

Data : 22222222222222222222222222222222

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard ☐ PICC ☐ AES EV1

Current selection : App 1, Key0

Click **Write Data/Rec** and then **Commit** to add second 16B record to Linear file.

After writing two records to the file, now we click **Read Data/Rec** to read them out to verify.

The screenshot shows the MR software interface with the 'Data' tab selected. The 'Length' field is set to 2, and the 'Data' field contains two lines of hex data: 11111111111111111111111111111111 and 22222222222222222222222222222222. A red box highlights the 'Offset', 'Length', and 'Data' fields. The 'Commit' button is visible at the bottom left of the interface.

Set the Length to 2, which means 2 records. Only when reading record, the Length means no of records. All other scenario, the Length means no of byte.

As can be seen, the card returned two records 11111111111111111111111111111111 hex, and 22222222222222222222222222222222 hex.

Try adding two more records to the file:

1. 33333333333333333333333333333333 hex,
2. 44444444444444444444444444444444 hex.

And read them out. Please note that, the reader supports only maximum 2 records per string. In order to view more than two records, please adjust the offset value.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 5

File Type : LinearRecord

File Option : Enciphered

Offset : 0

Length : 2

Data : 3333333333333333333333333333333444444444444444444444444444444444

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1

Current selection : App 1, Key0

Read the first two records, set the offset value to 0.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 5

File Type : LinearRecord

File Option : Enciphered

Offset : 2

Length : 2

Data : 1111111111111111111111111111111122222222222222222222222222222222

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1

Current selection : App 1, Key0

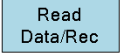
Read the subsequent two records, set the offset value to 2.

You may continue to add more records, but it will show failed. Maximum this file can store is 4 records only. We have limited the number of records to be written to the card, while creating this file.

If the records are not needed, we can remove them by clicking  and then .

The screenshot shows the MR software interface with the 'Desfire' tab selected. The interface includes a menu bar with 'Port', 'Classic', 'UltraLight EV1', 'Plus EV1', 'Desfire', 'Misc', 'MX App', and 'Info'. Below the menu bar, there are tabs for 'Application', 'Directory', 'File', 'Key', 'PICC', 'Roll Key (EV2)', and 'Misc'. The 'Data' tab is active, showing a 'Data' section with fields for 'App ID' (1), 'App Key' (Default Key), 'File ID' (5), 'File Type' (LinearRecord), 'File Option' (Enciphered), 'Offset' (2), 'Length' (2), and 'Data' (a long hexadecimal string). There is a 'Commit' button and a 'Value' dropdown set to 'No'. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' checkboxes, a 'PICC' dropdown, and an 'AES EV1' dropdown. The 'Current selection' is 'App 1, Key0'.

All the records are cleared.

You may click  to verify.

Function : Desfire Write Data/Rec

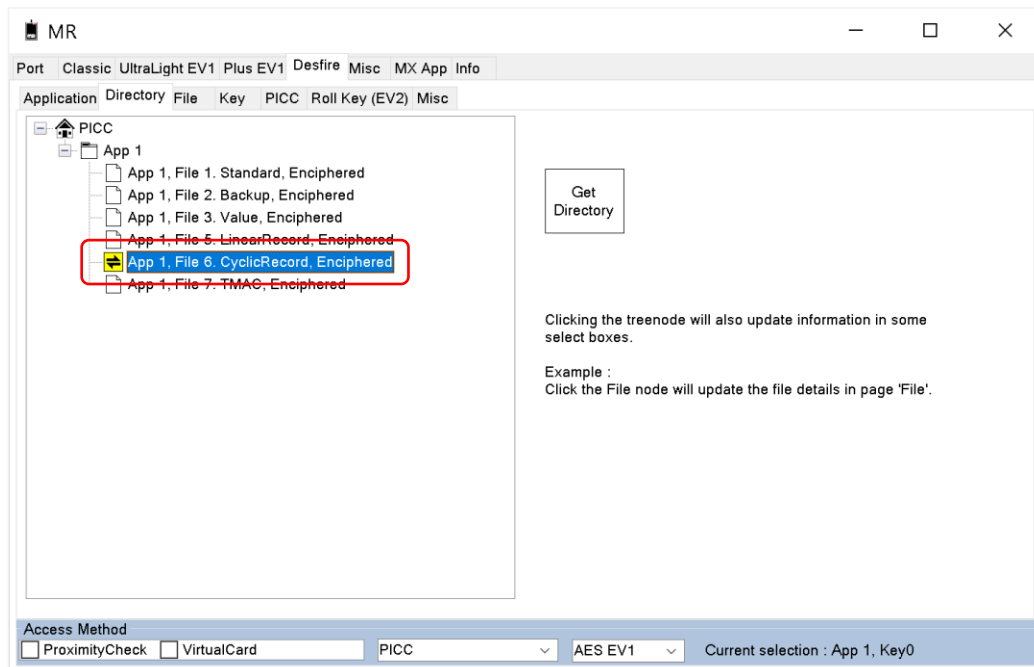
Please refer <C:\Mylab\MR> for details communication flow.

10. Cyclic Record File

Cyclic Record file add records to file. The new record will overwrite the oldest record. Total number of record it can be added is the assigned maximum number of record minus one, as one record space is needed for temporary storage. It implements backup mechanism. Commit Transaction is required in order to update the record to file.

In the previous chapter, we have created a Cyclic Record file in App 1. Now we will add few records to the file, and then read them back to verify.

Go to page Directory, click  .



Click on File 6 to select CyclicRecord file, and then go to page File, page Data.

Some file details are shown in the screen; the current app (App 1), the File ID (1), File Type (Standard), and File Option (Enciphered).

Now we will add one record to the file: 80000000000000000000000000000000 hex.

MR Manual – MF Desfire

The screenshot shows the MR software interface with the 'Data' tab selected. The 'Offset' is set to 0 and the 'Length' is set to 16, both highlighted with a red box. The 'Data' field contains a long hexadecimal string: 80000000000000000000000000000000. The 'Commit' button is highlighted. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' as options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

Click **Write Data/Rec** and then **Commit** to add a 16B record to file. The length stands for number of byte.

The screenshot shows the MR software interface with the 'Data' tab selected. The 'Offset' is set to 0 and the 'Length' is set to 1, both highlighted with a red box. The 'Data' field contains a long hexadecimal string: 80000000000000000000000000000000. The 'Read Data/Rec' button is highlighted. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' as options, with 'PICC' selected. The 'Current selection' is 'App 1, Key0'.

Click **Read Data/Rec** to read out one record from file. When read record, the length means number of record, not number of byte.

Since the file has only one record, attempt to read more than one record will show error.

MR Manual – MF Desfire

Continue to add the following records:

- 81000000000000000000000000000000 hex,
- 82000000000000000000000000000000 hex.

And read them out.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 6

File Type : CyclicRecord

File Option : Enciphered

Offset : 0

Length : 1

Data : 82000000000000000000000000000000

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1 Current selection : App 1, Key0

Set offset to 0, click **Read Data/Rec** to retrieve the latest record.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 6

File Type : CyclicRecord

File Option : Enciphered

Offset : 2

Length : 1

Data : 80000000000000000000000000000000

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1 Current selection : App 1, Key0

MR Manual – MF Desfire

Set offset to 2, click  to retrieve the oldest record.

So total there are 3 records in the file now. Maximum number of records it can store is $4 - 1 = 3$, so we have reached the maximum number now.

Continue to add one more record, and then read out the oldest record.

MR

Port

Classic

UltraLight EV1

Plus EV1

Desfire

Misc

MX App

Info

Application

Directory

File

Key

PICC

Roll Key (EV2)

Misc

Data

Add/Delete

App ID :

1

App Key :

Default Key

File ID :

6

File Type :

CyclicRecord

File Option :

Enciphered

Offset :

0

Length :

16

Data :

83000000000000000000000000000000

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec

Write Data/Rec

Clear Rec

Value File

Get Value

Debit

Credit

Limited Credit

Commit

Commit

Abort

Commit (TMAC)

Access Method

ProximityCheck

VirtualCard

PICC

AES EV1

Current selection : App 1, Key0

Click **Write Data/Rec** and then **Commit** to add add one more record.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 6

File Type : CyclicRecord

File Option : Enciphered

Offset : 2

Length : 1

Data : 81000000000000000000000000000000

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard ☒ PICC AES EV1 Current selection : App 1, Key0

Click **Read Data/Rec** to read out the oldest record found that it has been replaced second oldest record previously.

If the records are no longer needed, you may remove them by clicking **Clear Rec** and then **Commit**.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 6

File Type : CyclicRecord

File Option : Enciphered

Offset : 2

Length : 1

Data :

Value :

Commit

No

03000000 84BA9CD4F1CBE052

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

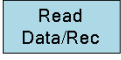
Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard ☒ PICC AES EV1 Current selection : App 1, Key0

All records are gone now.

MR Manual – MF Desfire

You may click  to verify.

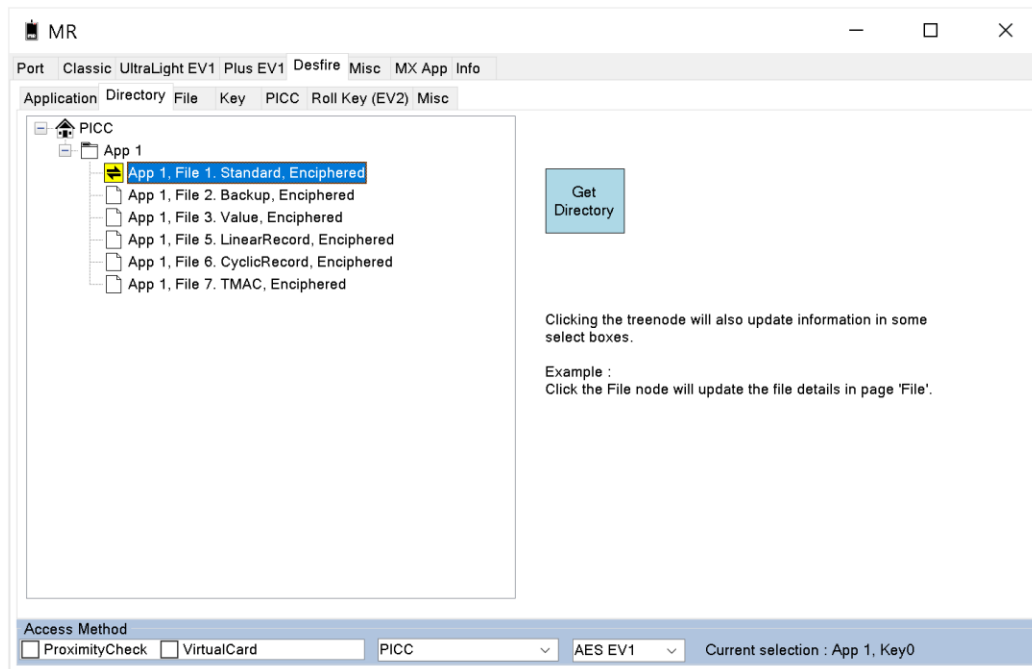
Please refer <C:\Mylab\MR> for details communication flow.

11. Change File Setting

The file option of our files in application App 1, are all Enciphered. It is possible to change the file setting, say we want to change the file option of File ID 1 from Enciphered to Plain, you can call Change File command.

Before we change anything, we read out the current file setting:

First, select File 1 from Directory,



Then go to page File, page Add/Delete.

The screenshot shows the MR software interface with the following settings:

- File Type:** Standard
- File ID:** 1
- File Options:** Enciphered
- ISO File:** Yes
- ISO File ID:** 1
- File Size:** 32
- Value File:**
 - Lower Value: 0
 - Upper Value: 0
 - Value: 0
 - Limited Credit: No
 - Free Get Value: No
- Key Options:**
 - Read Key: 0
 - Write Key: 1
 - Read/Write Key: 1
 - Change Key: 1** (highlighted with a red box)
- Linear / Cyclic Record File:**
 - Rec Size: 16
 - Max No Of Rec: 1
 - Total Rec Saved: 0
- T-MAC File:**
 - Key Type: AES
 - Key Ver: 0
 - Key: (empty field)

Buttons: Create File, Delete File, Get File, Change File.

Access Method: ProximityCheck, VirtualCard, PICC, AES EV1. Current selection: App 1, Key0.

Click , to retrieve the file details.

As shown in the Key Options, the key for change file setting is Key 1.

We will change the following items:

Item	Old	New
File Options	Enciphered	Plain

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

File Type : Standard Value File

File ID : 1 Lower Value : 0

File Options : Plain Upper Value : 0

ISO File : Yes Value : 0

ISO File ID : 1 Limited Credit : No

File Size : 32 Free Get Value : No

Create File Delete File Get File Change File

Key Options

Read Key : 0

Write Key : 1

Read/Write Key : 1

Change Key : 1

Linear / Cyclic Record File

Rec Size : 16

Max No Of Rec : 1

Total Rec Saved : 0

T-MAC File

Key Type : AES

Key Ver : 0

Key :

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1

Current selection : App 1, Key1

Change the File Options to Plain, and click

Change File

We go back to the page Directory and click

Get Directory

to view the file system.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

PICC

App 1

App 1, File 1. Standard, Plain

App 1, File 2. Backup, Enciphered

App 1, File 3. Value, Enciphered

App 1, File 5. LinearRecord, Enciphered

App 1, File 6. CyclicRecord, Enciphered

App 1, File 7. TMAC, Enciphered

Get Directory

Clicking the treenode will also update information in some select boxes.

Example :
Click the File node will update the file details in page 'File'.

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1

Current selection : App 1, Key0

Note that the file option for File 1 is now Plain.

We will access Standard file now. Click on File 1, then go to page File, page Data.

The screenshot shows the MR software interface with the 'Data' tab selected. The 'File Option' is set to 'Plain' and the 'Data' field contains the hexadecimal string '00112233440DFAF097D3F7752B'. The 'Read Data/Rec' button is highlighted. The interface also includes fields for App ID, App Key, File ID, File Type, Offset, Length, Value, and buttons for Read, Write, Clear, Get Value, Debit, Credit, Limited Credit, Commit, and Abort. The bottom status bar shows the Access Method as ProximityCheck, VirtualCard, and PICC, with the current selection being App 1, Key0.

Click **Read Data/Rec** to read 5B data from this file. Please note that the reader return extra information; the first 5B is the real data, and the 8B data following it is the MAC data. You may ignore it.

You may change other file setting according to your needs. But remember to read the details first, by clicking

Get File, before you change anything. This is to avoid you accidentally modify some important settings.

You may change the File Options, and Key Options only. The rest are unchangeable.

Please refer <C:\Mylab\MR> for details communication flow.

12. Roll Key

This feature is not available in EV1 card.

Roll key is important for smart card application, because it enhances security. If a card key is accidentally leaked or hacked, then the whole system will be unsafed. But if a smart card has roll key feature built in, then the system can switch to the next level key, and the system can still maintain its security.

We will explain the concept of Roll Key here. Let say we create 3 KeySets in an application, KS0 KS1, and KS2.

Default is KeySet 0

KeySet 0, 1, 2

KeyVer 0, 1, 2

We use Keyset 0 's Key to access card

Then we roll 1 step, the pattern now becomes:

KeySet 1, 2, 0

KeyVer 1, 2, 0

We now use KeySet 1 's Key to access card

Then we roll 1 step again, the pattern now becomes:

KeySet 2, 0, 1

KeyVer 2, 0, 1

We now use KeySet 2 's Key to access card

If we roll 1 step again, it will show 'Permission Denied', because the next KeyVer (0) is lower than the current KeyVer (2). That means, for roll key to be successful, the next Keyset's Version, must be higher than the current active Keyset Version.

We will create a new application to show this feature now.

13. Delegated Application (DAM)

This feature is not available in EV1 card.

To create Delegated Application, we need to enable the PICCDAMAUTHKEY, PICCDAMMACKEY and PICCDAMENCKEY, at PICC level, in the card.

We will enable these keys when we create DAM application later. After enabled, the keys still hold their default value. We will change the value later, or when necessary.

Item	Value (hex)
PICCDAMAUTHKEY	00000000000000000000000000000000
PICCDAMMACKEY	00000000000000000000000000000000
PICCDAMENCKEY	00000000000000000000000000000000

Before we create the DAM application, let's understand the three DAM parameters.

DAM parameters:

DAM Slot Number – it allows the user to target a specific slot of the application memory space. It is also associated with the requested quota limit (max size that can be used by the application). After an application has been deleted, the memory space will be released, and it is possible to reuse the memory slot, if the new slot number and the new quota limit are same as the old application.

DAM Slot Version – when a delegated application becomes obsolete, another delegated application can be created in the slot with the same DAM slot number but using a higher DAM slot version. The only exception is the DAM slot version set to 0xFF or 255. This means that the targeted slot can be used over and over again.

Quota Limit – it indicates the maximum memory the application can consume in number of 32B blocks. If quota limit is set to 32, then the total memory size will be $32 \times 32 = 1024B$.

In our DAM applications, we have fixed the DAM parameters value as follow:

- DAM quota = 28 ($28 \times 32=896$ bytes)
- DAM Version = 0xFF
- Max 3 KeySets
- All keysets will be roll key ready.

Now go to page Application, and we will create a DAM application on the card. The DAM will have the following spec:

Item	Value	Remark
App ID	2	Cannot be 0, as this is reserved for PICC level.
App Type	DAM	Either Conventional or DAM.
Current PICC Key Type	AES	
Current PICC Key	00000000000000000000000000000000	
Default App Key	00000000000000000000000000000000	
DAM Slot	2	Can be other value, or user define.
New App KS0 Key 0	20000000000000000000000000000000	Can be other value, or user define.
New App KS0 Key 1	21000000000000000000000000000000	Can be other value, or user define.
New App KS1 Key 0	20000000000000000000000000000000	Can be other value, or user define.

MR Manual – MF Desfire

New App KS1 Key 1	23000000000000000000000000000000	Can be other value, or user define
New App KS2 Key 0	20000000000000000000000000000000	Can be other value, or user define.
New App KS2 Key 1	25000000000000000000000000000000	Can be other value, or user define
File Type	Standard [1], Backup [2], Value [3], Cyclic [6], TMAC [7].	These file(s) will be created.
DF Name	DAM 2	Auto generated

Since there are 3 keysets, and each keyset has 2 keys (Key 0 and Key 1), so total we need to set 6 keys. We define the KeySets's Key when we create the application. All the keys in the keysets will be initialized, finalized, and ready to be rolled.

Please note that the Key 0 is same for all the keysets. We will explain it later.

Before we click the button to start, it is good to know the whole process:

- Change the PICC Key and switch the KeyType from DES to AES. (It is OK if the card is already in AES mode.),
- Enable DAMAuth Register with default key,
- Enable DAMMAC Register with default key,
- Enable DAMENC Register with default key,
- If same DAM already exist, delete it,
- Create DAM,
- Initialize, Change, and Finalize keysets's App Key,
- Create the file(s).

Select PICC in the application field, and enter the values to the field, as shown below:

The screenshot shows the MR software interface with the following configuration:

- App ID:** 2
- App Type:** DAM
- Current PICC Key Type:** AES
- Current PICC Key:** 00000000000000000000000000000000
- Default App Key:** 00000000000000000000000000000000
- Old VCCongig Key:** 00000000000000000000000000000000
- New VCCongig Key:** 00000000000000000000000000000000
- File Type:**
 - ☒ Standard [1]
 - ☒ Backup [2]
 - ☒ Value [3]
 - ☒ Cyclic [6]
 - ☒ TMAC [7] (EV2)
 - ☐ Value2 [4]
 - ☐ Linear [5]
- DF Name:** DAM 2
- DAM Slot:** 2
- KeySet:** 3 Keysets
- KS0 Key 0:** 20000000000000000000000000000000
- KS0 Key 1:** 21000000000000000000000000000000
- KS1 Key 0:** 20000000000000000000000000000000
- KS1 Key 1:** 23000000000000000000000000000000
- KS2 Key 0:** 20000000000000000000000000000000
- KS2 Key 1:** 25000000000000000000000000000000
- Access Method:**
 - ☒ ProximityCheck
 - ☐ VirtualCard
 - ☐ PICC
 - ☒ AES EV2
- Current selection:** App 2, Key0

This DAM application will have 5 files;

- Standard file (File ID 1), 32 Byte,
- Backup file (File ID 2), 32 Byte,
- Value file (File ID 3), Free Get Value,

MR Manual – MF Desfire

- Cyclic file (File ID 6), Max 4 Records,
- TMAC (File ID 7).

The app will have two keys; Key 0, and Key 1. Key 0 will be used as authentication key when we perform Read. Key 1 is mainly for Write and Change Key.

Create App
and Files

Click the button to create the application.

Please Confirm



This is new DAM application ?

OK

Cancel

If the above message box appears, click OK to confirm.

Status



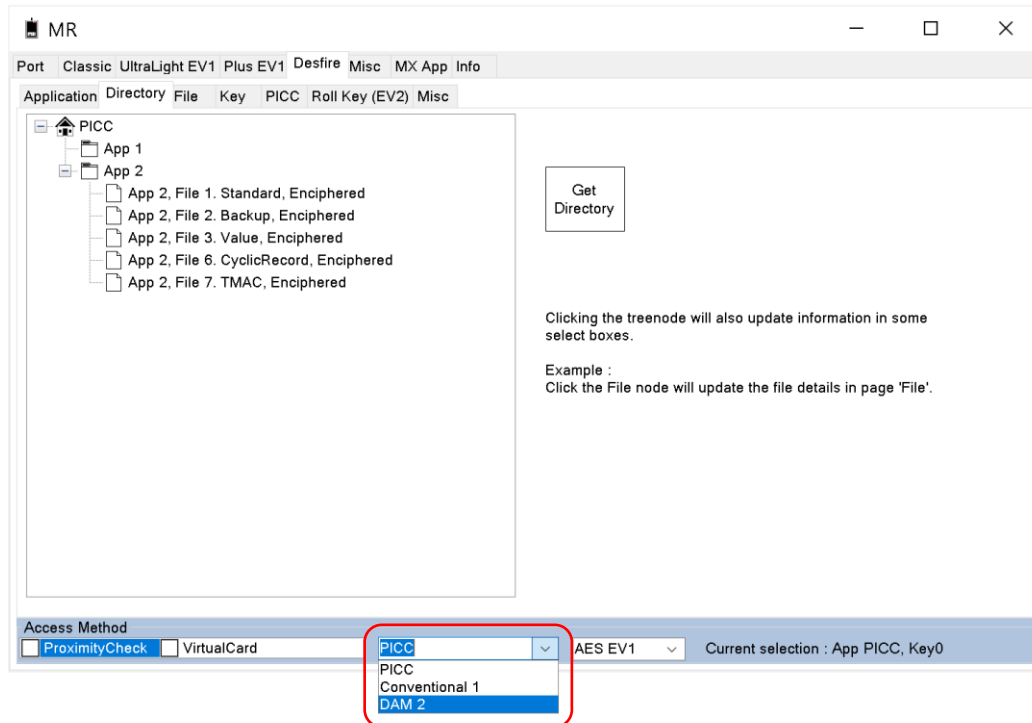
Change PICC : ... OK
Enable DAM Key : ... OK
Create App : 2 ... OK
Init KeySet 1 ... OK !
Init KeySet 2 ... OK !
Change KeySet 2 Key 1 ... OK !
Change KeySet 2 Key 0 ... OK !
Finalize KeySet 2 ... OK !
Change KeySet 1 Key 1 ... OK !
Change KeySet 1 Key 0 ... OK !
Finalize KeySet 1 ... OK !
Change KeySet 0 Key 1 ... OK !
Change KeySet 0 Key 0 ... OK !
Create Standard File ID 1... OK
Create Backup File ID 2... OK
Create Value File ID 3... OK
Create Cyclic File ID 6... OK
Create TMac File ID 7... OK

OK

The DAM 2 app has been created. The keys are enabled, and ready to be rolled, and the files are ready to be used.

Remember to save the PICC Key and the KeySet0's keys to reader, by clicking [Save New PICC, DAM, and Current Active Keys to Reader](#). So the active key in the reader now is App 2 KS0's key.

Go to page Directory, click [Get Directory](#) to view the file system now.



The card has two applications now.

Because the active key in the reader now is the App 2 KS0's key, so you see only files in App 2, and files in App 1 don't show up.

If you want to view App 1's files, load App 1's Keys to reader, and click [Get Directory](#), then the App 1 files will appear.

Click on File 2, and go to page File, page Data, we are going to do read / write to the Backup file. And since we have created TMAC file in this DAM2 application, we will show you the TMC/TMV features too. So, select DAM2 and AES EV2 in the Access Method.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 2

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 16

Data : 01234567890123456789012345678901

Value : 0

Commit

No

TMC / TMV

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

ProximityCheck VirtualCard

DAM 2 AES EV2

Current selection : App 2, Key1

Click **Write Data/Rec** to write 16B data to the file, and then click **Commit (TMAC)** to update the data to memory.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 2

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 16

Data : 01234567890123456789012345678901

Value : 0

Commit

No

01000000 7A1E4E9675E167C1

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

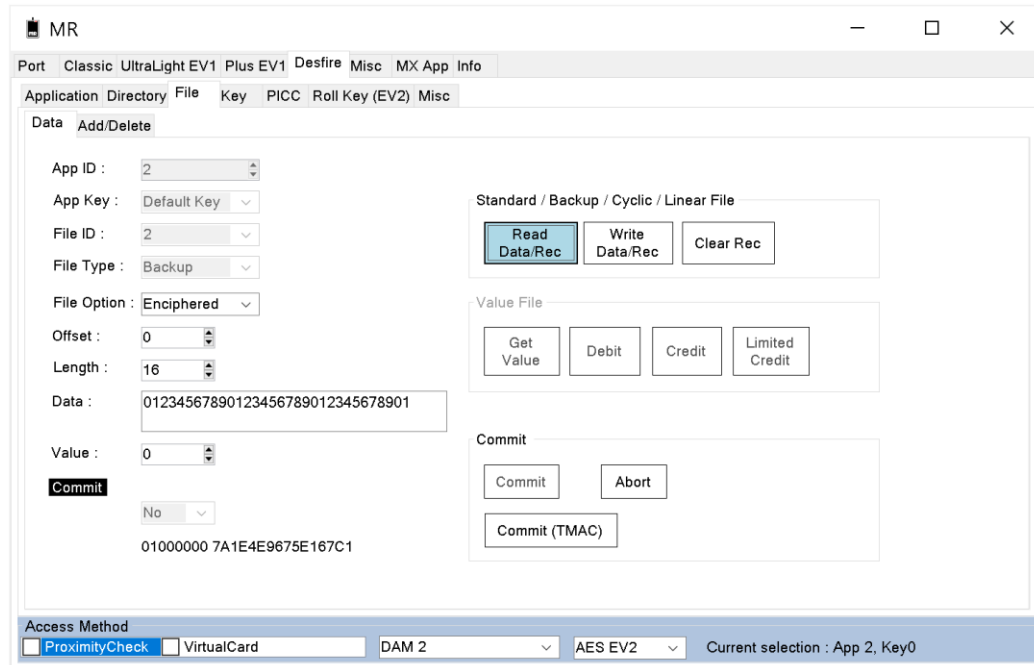
ProximityCheck VirtualCard

DAM 2 AES EV2

Current selection : App 2, Key0

Recall from chapter TMAC, after adding TMAC file in an application, the card will return TMC/TMV, after every successful commit transaction.

Click **Read Data/Rec** to read the data to verify the data we have just written.



Therefore, the DAM works just like the conventional application.

We will try the Roll Key feature as we discussed in the previous chapter. We have reserved 3 Keysets when we create this DAM, and we defined the keys as follow:

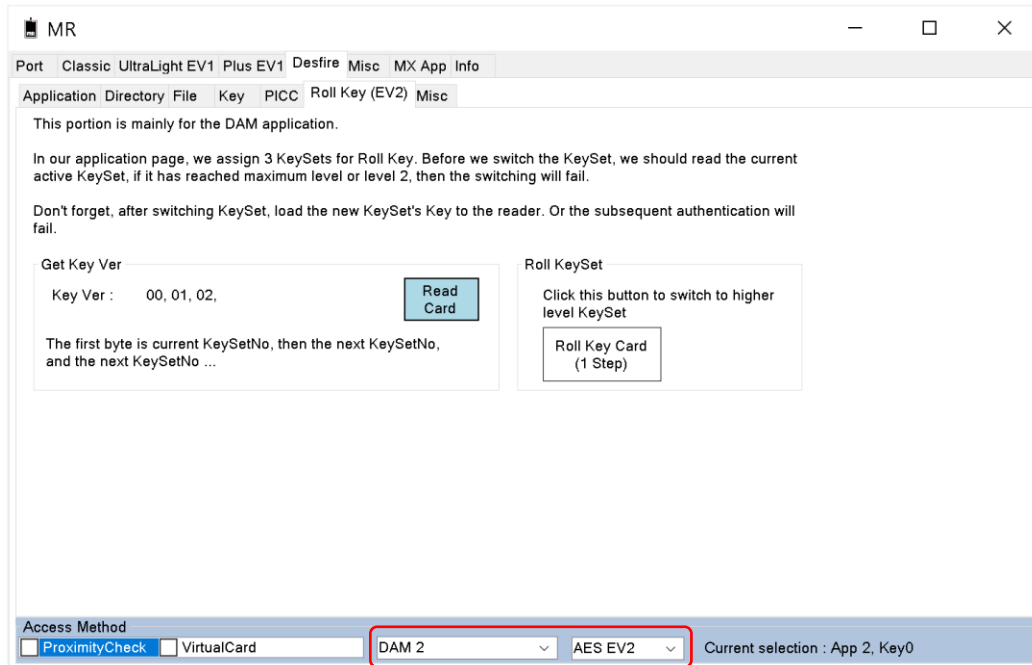
Application ID = 02	Value
KS0 Key0	20000000000000000000000000000000
KS0 Key1	21000000000000000000000000000000
KS1 Key0	20000000000000000000000000000000
KS1 Key1	23000000000000000000000000000000
KS2 Key0	20000000000000000000000000000000
KS2 Key1	25000000000000000000000000000000

The active keyset now is KS0, and the keys loaded to the reader are;

- Key 0: 20000000000000000000000000000000 hex
- Key 1: 21000000000000000000000000000000 hex.

We will verify this. Go to page Roll Key (EV2).

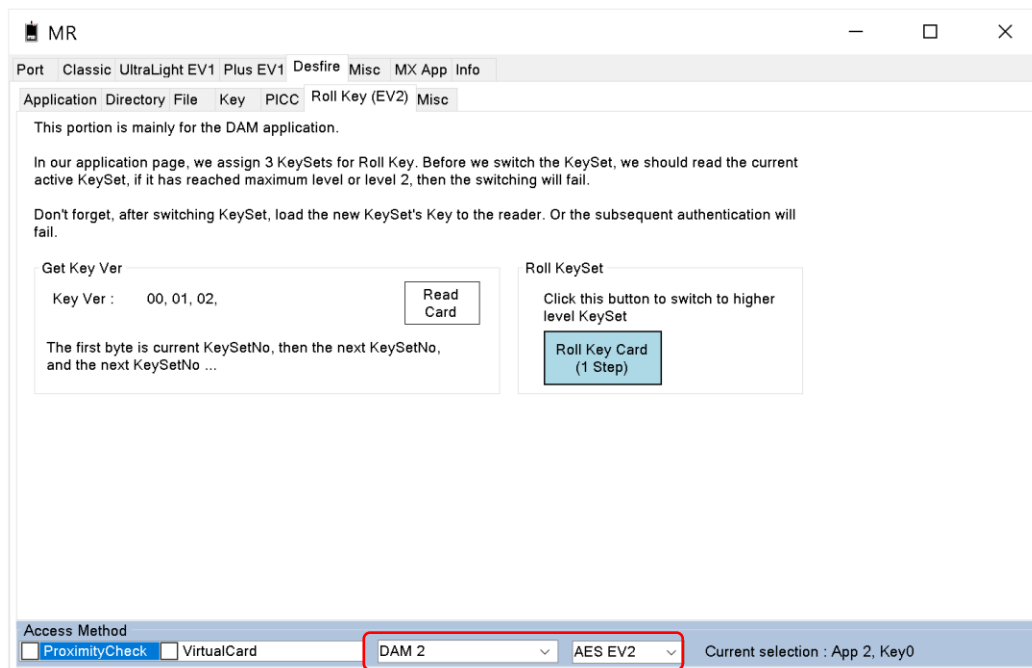
MR Manual – MF Desfire

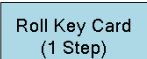


Click  to read the Key Ver. It returned 00, 01, 02, which means KeyVersion for KS0, KS1, and KS2.

So the current active keyset is KS0.

Now we will start to roll the key by one step. When this is done, the active keyset will be KS1.



Click , to start roll key.

MR Manual – MF Desfire

Now we have switched the keyset to KS1, and we can confirm it by reading the Key Ver.

Get Key Ver

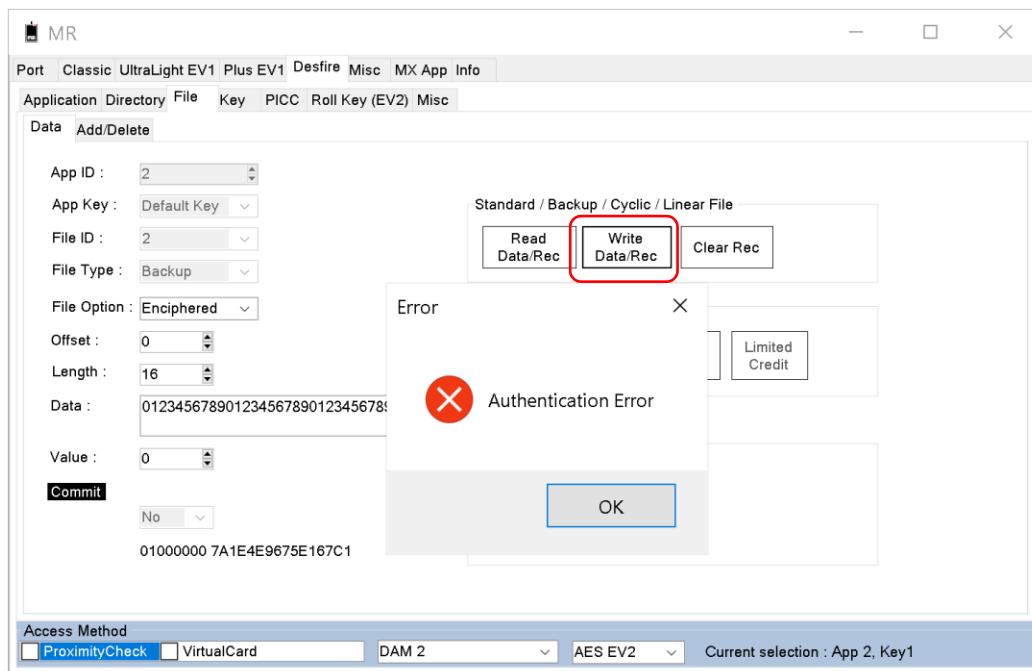
Key Ver : 01, 02, 00,

The first byte is current KeySetNo, then the next KeySetNo, and the next KeySetNo ...

Click to get the current Key Ver. The returned value shows that the active keyset is KS 1.

This is the reason we set the Key 0 same for all the keysets. When the Key 0 same, we can read the Key Ver, does not matter which keyset they are in. If the Key 0 is different for every keyset, then we need to load the correct keyset to the reader, then only we can read the Key Ver. But sometimes we may forget which keyset the card is currently in, and don't know which key should be loaded.

Since the current active key in the reader is still KS0, we will try if we still can write to the file in App 2 using KS0's key. Bear in mind that Write function involve authentication with Key 1, not Key 0, and Key 1 is different for all the keysets.



Click to write data to Standard file in App 2, but it fails. It should be able to read from the file since the Key 0 is same for all keyset. You may try it.

Using KS0's key cannot write to App 2 anymore. We will load KS1's key to reader now, and the keys are:

Application ID = 02	Value
KS0 Key0	20000000000000000000000000000000
KS0 Key1	21000000000000000000000000000000
KS1 Key0	20000000000000000000000000000000
KS1 Key1	23000000000000000000000000000000

MR Manual – MF Desfire

KS2 Key0	20000000000000000000000000000000
KS2 Key1	25000000000000000000000000000000

Go to page Key, page Load Key, and enter the KS1's key to the field below:

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

Load Key to Reader

KeyNr : PICCMasterKey Save Key

KeyData : 00000000000000000000000000000000

Load New KeySet Key To Reader

Key 0 : 20000000000000000000000000000000 Save Key

Key 1 : 23000000000000000000000000000000

Access Method

☒ ProximityCheck ☐ VirtualCard DAM 2 AES EV2 Current selection : App 2, Key0

Click  to load the key to reader. This will be the active key in reader.

We will try to write to the Standard file in App 2 again, using KS1's key.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 2

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 16

Data : 01234567890123456789012345678901

Value : 0

Commit

No

02000000 C83AB7403DBF7720

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

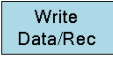
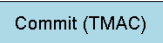
Commit Abort

Commit (TMAC)

Access Method

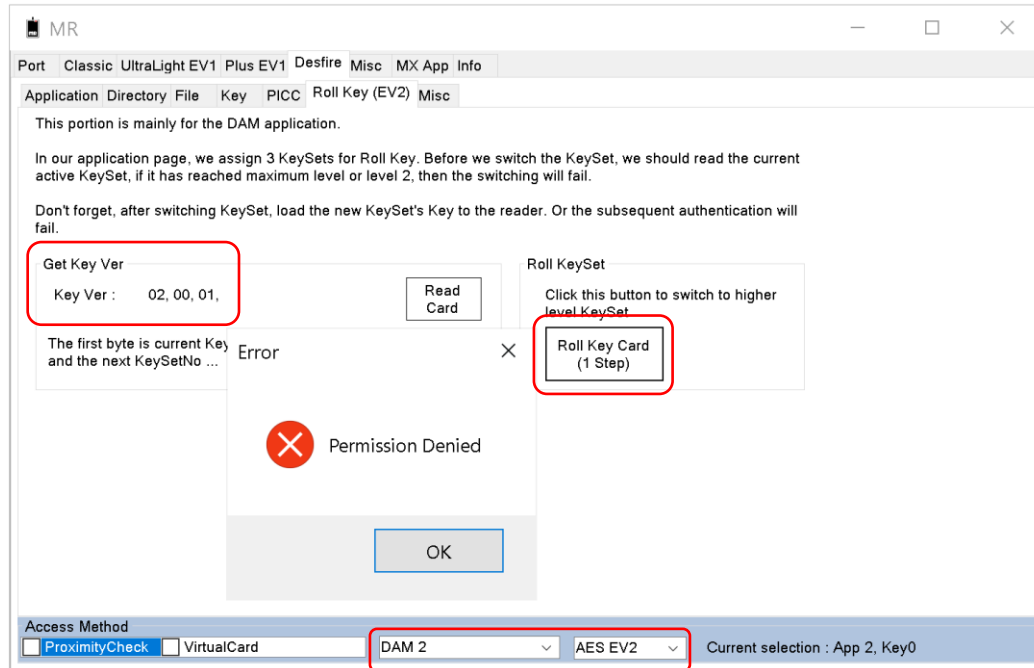
☒ ProximityCheck ☐ VirtualCard DAM 2 AES EV2 Current selection : App 2, Key0

MR Manual – MF Desfire

Click  to write data to DAM 2 application Backup file, and then click . Success!

You may call Roll Key again to switch to KS2. But remember to load KS2's key to reader after the switch.

Since we reserved only 3 KeySets for this App 2, if the current keyset is KS2, then any subsequent Roll Key will be failed, as KS2 is the highest keyset in this application. The picture below shows the scenario.



Since the Key Ver is 02, means the App has reached maximum keyset, and any attempt to roll key again will fail.

Before we end this chapter, we show you how to change the three DAM Registers. We have enabled the registers when we created this DAM 2 application, but we did not change the values. They are still holding the default value which is 16B 00 hex.

We assign the following new values for the three keys:

Item	Value (hex)
PICCDAMAUTHKEY	10101010101010101010101010101010
PICCDAMMACKKEY	11111111111111111111111111111111
PICCDAMENCKEY	12121212121212121212121212121212

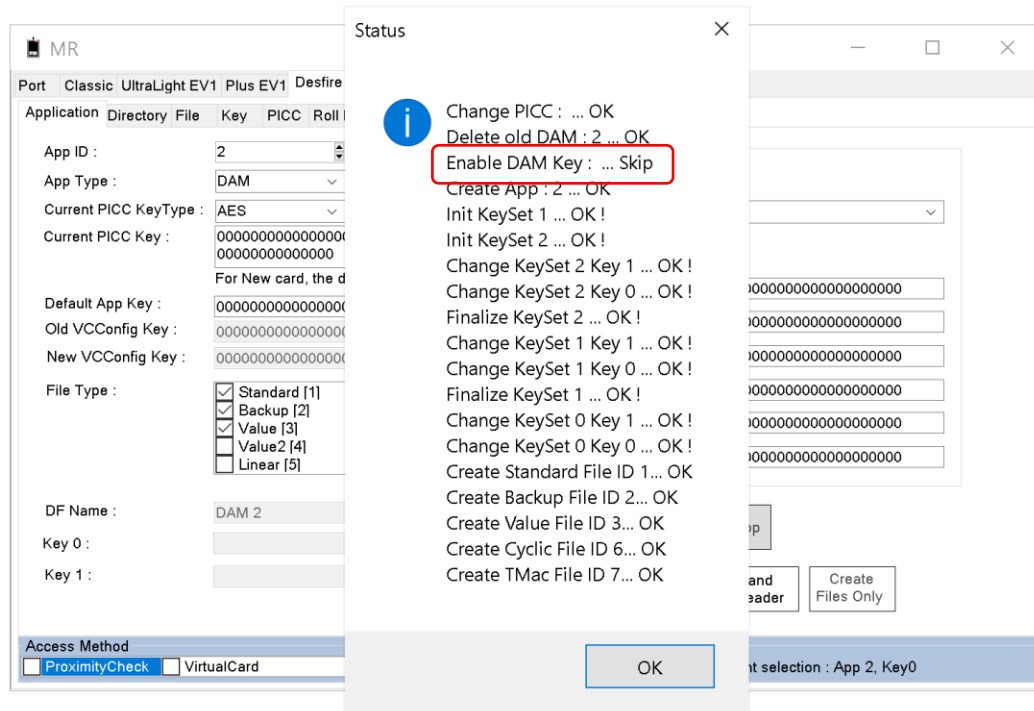
Go to page Key, page DAM Key (EV2). Enter the values to the fields.

The default old key is 16B 00 hex. If you changed the key before, enter the current old keys. Then click  to program the keys to card.

And then click  to save the keys to reader's non volatile memory.

www.mylab.my
Page 59

MR Manual – MF Desfire



You may use the card like normal.

Please refer <C:\Mylab\MR> for details communication flow.

14. Card Info

We will read out the basic info of the card. Go to page PICC, in the Card Info, click

Read Card

The screenshot shows the MR software interface with the following sections:

- Change PICC Key / Switch KeyType:** Includes fields for New KeyType (AES), New Key Ver (0), Old Key (00000000000000000000000000000000), and New PICC Key. Buttons: Write Card, Save Key.
- Options:** AuthKey = PICCKey. Buttons: Write Card. Fields: New App, Default Key.
- Card Info:** Displays SNR (0451453A841390), Free Mem (000E00), and Version (04010112001805, 04010102011805, 0451453A841390, CF7CD259704022). Button: Read Card.
- Key Setting:** AuthKey = PICCKey. Checkboxes: Config Changeable, Free Create / Delete, Free Directory List, MasterKey Changeable. Buttons: Read Card, Write Card. Fields: Access Right (0), No of Keys (0).
- Access Method:** ProximityCheck, VirtualCard, PICC, AES EV1. Current selection: App 1, Key0.

From the screen, we know that the SNR = 0451453A841390 hex, and the free memory size is 0E00 hex or 3584 Bytes. You may refer to the card manufacturer's manual for details about the meaning of other returned string.

Please refer <C:\Mylab\MR> for details communication flow.

15. Change PICC Key

We have switched the key type of PICC from DES to AES when we created App 1, but the value is still the default 16B 00 hex. We will change the PICC value here. Bear in mind that PICC key is the most commonly used key in Desfire card, without the key, we cannot perform any basic function to the card. So, don't lose the key.

We will first read the key info of this card.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Change PICC Key / Switch KeyType

New KeyType : AES Write Card Save Key

New Key Ver : 0

Old Key : 00000000000000000000000000000000

New PICC Key :

Card Info

SNR : 0451453A841390 Read Card

Free Mem : 000E00

Version : 04010112001805
04010102011805
0451453A841390
CF7CD259704022

Options

AuthKey = PICCKey Write Card

New App

Default Key :

Key Setting

AuthKey = PICCKey Read Card

☒ Config Changeable

☒ Free Create / Delete

☒ Free Directory List

☒ MasterKey Changeable

Access Right : 0

No of Keys : 1

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV1 Current selection : App 1, Key0

In the 'Key Setting' section, click  to get the Key info. There are some important points in the Key Info:

- Only one key in the PICC level
- Access Right is Key0, it is the Key required for authentication in order to change key,
- MasterKey is changeable.

From the Key info, we know that MasterKey is changeable, and the Access Right or authentication key is Key0, so we will use Key0 to change the PICC key.

The default PICC key is 16B all 00 hex. Now we want to change it to 01020300000000000000000000000000 hex.

Item	Value
Current PICC Key	00000000000000000000000000000000
New PICC Key	01020300000000000000000000000000

To change the PICC key to other value

MR Manual – MF Desfire

The screenshot shows the MR software interface with the 'PICC' tab selected. The 'Change PICC Key / Switch KeyType' section has 'New KeyType' set to 'AES' and 'New Key Ver' set to '0'. The 'Old Key' and 'New PICC Key' fields are both filled with a long hexadecimal string. The 'Options' section shows 'AuthKey = PICCKey' and a 'Write Card' button. The 'Card Info' section displays SNR, Free Mem, and Version information, with a 'Read Card' button. The 'Key Setting' section shows 'AuthKey = PICCKey' and several checked options: 'Config Changeable', 'Free Create / Delete', 'Free Directory List', and 'MasterKey Changeable'. The 'Access Method' section at the bottom shows 'ProximityCheck' and 'VirtualCard' options, with 'PICC' selected in the dropdown menu. The 'Current selection' is 'App 1, Key0'.

Click  to change PICC key. And then click  to load the key to reader for next authentication.

You may verify the new PICC key by reading the Card Info.

The screenshot shows the 'Card Info' section of the MR software interface. It displays the following information: SNR: 0451453A841390, Free Mem: 000E00, and Version: 04010112001805, 04010102011805, 0451453A841390, CF7CD259704022. A 'Read Card' button is visible next to the information.

Click  to retrieve basic info. It works.

Please refer <C:\Mylab\MR> for details communication flow.

16. Change Application Key

We program the application key when we create the application. The keys for DAM 2 are as shown below:

Item	Value
App ID	2
App Type	DAM
Current PICC Key Type	AES
Current PICC Key	01020300000000000000000000000000
DAM Slot	2
New App KS0 Key 0	20000000000000000000000000000000
New App KS0 Key 1	21000000000000000000000000000000
New App KS1 Key 0	20000000000000000000000000000000
New App KS1 Key 1	23000000000000000000000000000000
New App KS2 Key 0	20000000000000000000000000000000
New App KS2 Key 1	25000000000000000000000000000000
File Type	Standard [1], Backup [2], Value [3], Cyclic [6], TMAC [7]
DF Name	DAM 2

But it can be changed to other value.

If the application has keyset like our DAM 2, it is good to change the key before rolling any keyset. But if you have rolled the key, then you need to get the current Key Version.

Our DAM 2 has reached KS 2, and its Key Ver is 02, but the key is still changeable. We define a new key for KS 2's Key 1 here:

Item	Old Value	New Value
KS 2, Key 1	25000000000000000000000000000000	35000000000000000000000000000000

Go to page Key, then page App Key. Fill the details of the key that we want to change, as shown below:

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

AuthKey = PICCKey or AMKey

Old Key : 25000000000000000000000000000000

New Key : 35000000000000000000000000000000

Current KeyVer : 2

KeyNr : Key1

Is KeySet : Yes

KeySet No : 2

KeySet Ver : 2

Write Card Save Key

Access Method

☐ ProximityCheck ☐ VirtualCard DAM 2 AES EV2 Current selection : App 2, Key0

Click  to change the key. We will verify the new key now.

Recall that the Key 1 is mainly for Write function, we try to write few data to the Backup file now.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 2

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 16

Data : 01234567890123456789012345678901

Value : 0

Commit

No

TMC / TMV

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Error

Authentication Error

OK

Access Method

☐ ProximityCheck ☐ VirtualCard DAM 2 AES EV2 Current selection : App 2, Key1

Click  to write few bytes to the Backup file, but it fails.

Now we load the key that we just changed to the reader.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

Load Key to Reader

KeyNr : Key1 Save Key

KeyData : 35000000000000000000000000000000

Load New KeySet Key To Reader

Key 0 : 00000000000000000000000000000000 Save Key

Key 1 : 00000000000000000000000000000000

Access Method

☐ ProximityCheck ☐ VirtualCard DAM 2 AES EV2 Current selection : App 2, Key1

Enter the new Key 1 and click . You may try the Write function again.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 2

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 16

Data : 01234567890123456789012345678901

Value : 0

Commit

No

02000000 C83AB7403DBF7720

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

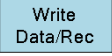
Commit

Commit Abort

Commit (TMAC)

Access Method

☐ ProximityCheck ☐ VirtualCard DAM 2 AES EV2 Current selection : App 2, Key0

Click  and then . Now the Write function works fine.

Please refer <C:\Mylab\MR> for details communication flow.

17. AppDefaultKey

The default Key value for new application is all zeros. But this value can be changed. We will show you how to change the value to 16B FFs in this section. After the change, all the keys in a new application will be 16B FFs, not zeros.

The screenshot shows the MR software interface with the 'PICC' tab selected. The 'Change PICC Key / Switch KeyType' section has 'New KeyType' set to 'AES', 'New Key Ver' set to '0', 'Old Key' set to '00000000000000000000000000000000', and 'New PICC Key' set to '01020300000000000000000000000000'. The 'Options' section has 'AuthKey = PICCKey' and 'New App Default Key' set to 'FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF'. The 'Key Setting' section has 'AuthKey = PICCKey' and 'Config Changeable', 'Free Create / Delete', 'Free Directory List', and 'MasterKey Changeable' all checked. The 'Access Method' section at the bottom has 'ProximityCheck' and 'VirtualCard' unchecked, and 'PICC' selected. The 'Current selection' is 'App 2, Key0'.

Click  to set the default application Key to 16B FF hex.

Now, we have changed the default application key to 16B FF hex, no longer 00 hex. For this card, you need to enter correct default app key to the Default App Key field, whenever you want to create new Application.

18. Proximity Check

This feature is not available in EV1 card.

Proximity Check allows a reader to verify whether a card is within a certain distance. We will enable this feature here.

First we need to enable the VCConfigurationKEY, and VCProximityKEY.

Recall that we have enabled VCConfigurationKey when we created our first application App 1. But we didn't change the value. So the key is still the default key 16B 00 hex. We will show you how to change the value here.

The VCConfigurationKEY is used to enable the VCProximityKEY flag, while the VCProximityKEY is used for Proximity Check, after we have enabled the PCMandatory flag.

We define the two keys as follow:

Item	Value
VCConfigurationKey	02000000000000000000000000000000
VCProximityKey	03000000000000000000000000000000

To enable the VCConfigurationKEY, go to page Key, page PC/VC (EV2), and follow the setting as shown below:

Click  to change the VCConfigurationKEY. Once changed, the key will be enabled. After that, click  to save the key to reader.

Now, we will enable the VCProximityKEY.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

VConfigurationKey

AuthKey = PICCKey

Old : 00000000000000000000000000000000

New : 02000000000000000000000000000000

Write Card

Save Key

VKey (EV2)

AuthKey = VCConfigKey

VCProximityKey

Old : 00000000000000000000000000000000

New : 03000000000000000000000000000000

VCSelectMACKey

Old : 00000000000000000000000000000000

New :

VCSelectENCKey

Old : 00000000000000000000000000000000

New :

PICC Configuration

AuthKey = PICCKey

This is a non reverse process;
Once the flag is turned On, it
cannot be turned Off.
ProximityCheck and VirtualCard
are for EV2 only.

☐ Disable Format PICC

☐ Enable Random UID

☐ Enable PCMandatory

☐ Enable AuthVCMandatory

Write Card

Access Method

☐ ProximityCheck ☐ VirtualCard PICC AES EV2 Current selection : App 2, Key0

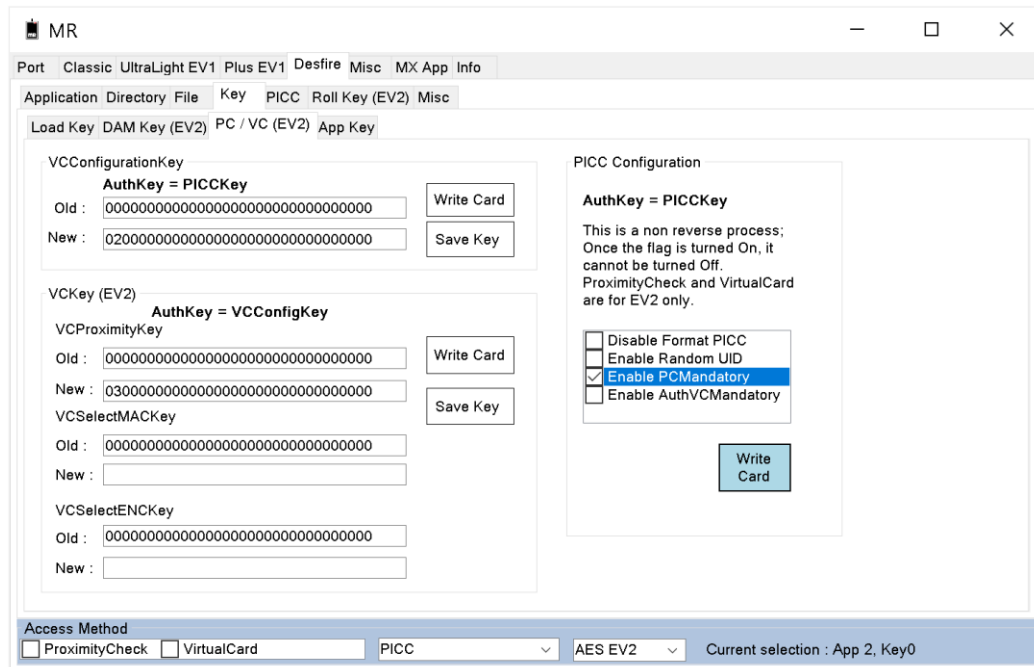
Click  to change the VCProximityKEY. Once changed, the key will be enabled. After that, remember to click  to save the key to reader.

Now we have enabled VConfigurationKEY and VCProximityKEY.

Next we will enable the PCMandatory flag.

Please note that Enable ProximityCheck is a non reverse process; once the flag is turned on, it cannot be turned off.

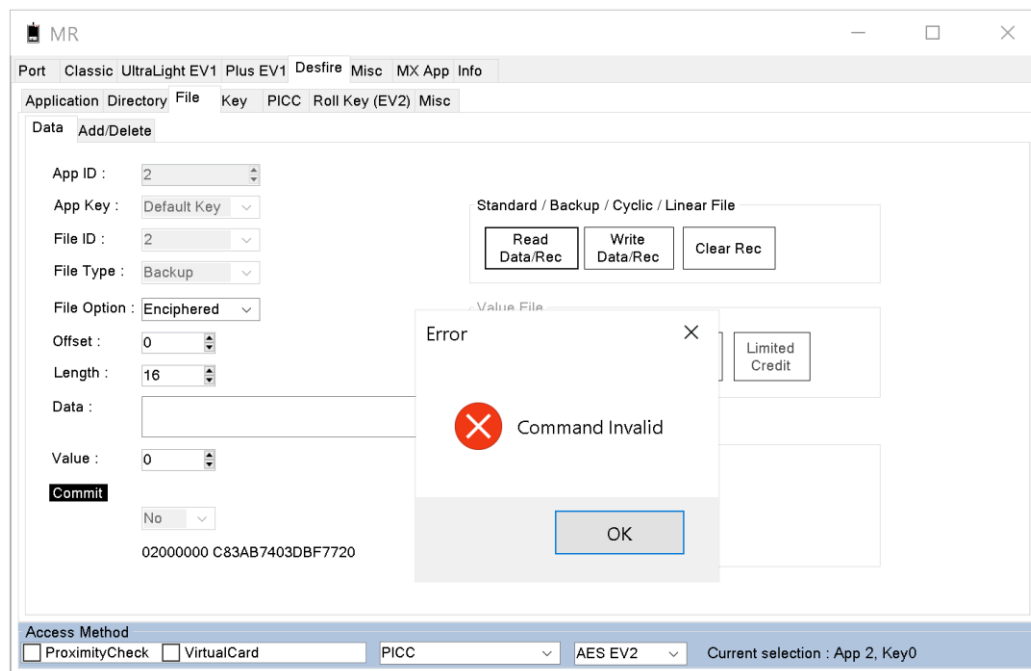
MR Manual – MF Desfire

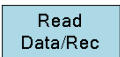


Check Enable PCMandatory, and then click .

Now the Proximity Check flag is enabled.

We will try to read card info now excluding the ProximityCheck in the access method.



Click  to Backup file. Failed! You may need to reset the RF field in order to view this.

MR Manual – MF Desfire

Now we include the ProximityCheck in the access method. We try to read the card again.

The screenshot shows the MR software interface with the 'Access Method' section highlighted by a red box. The 'Access Method' dropdown is set to 'ProximityCheck'. Below it, the 'VirtualCard' dropdown is set to 'VirtualCard', the 'PICC' dropdown is set to 'PICC', and the 'AES EV2' dropdown is set to 'AES EV2'. The 'Current selection' is 'App 2, Key0'. The 'Data' field contains the hexadecimal value '01234567890123456789012345678901'. The 'Value' field contains '0'. The 'Commit' button is highlighted. The 'Data' field is also highlighted. The 'Data' field is also highlighted.

If Proximity Check is included, access is granted.

We have enabled the Proximity Check, and it cannot be disabled.

From now on, we need to include Proximity Check before we can access the card.

Please refer [C:\Mylab\MR](#) for details communication flow.

19. Virtual Card

This feature is not available in EV1 card.

Once this feature is enabled, the reader will need to compare the card's DF Name when accessing the card.

We have enabled the VConfigKey in Chapter Proximity Check. Please refer to the chapter 'Proximity Check' if VConfigKey is not yet enabled.

So, to enable Virtual Card, we first need to enable VCSelectMACKey and VCSelectENCKey.

We define the two keys as follow:

Item	Value
VCSelectMACKey	04000000000000000000000000000000
VCSelectENCKey	05000000000000000000000000000000

Since we have enabled the Proximity Check, we need to set the access method to include the ProximityCheck.

The screenshot shows the MR software interface with the following sections:

- VCConfigurationKey**: AuthKey = PICCKey. Old: 00000000000000000000000000000000. New: [empty]. Buttons: Write Card, Save Key.
- VCKey (EV2)**: AuthKey = VConfigKey. VCProximityKey: Old: 00000000000000000000000000000000. New: [empty]. Button: Write Card. VCSelectMACKey: Old: 00000000000000000000000000000000. New: 04000000000000000000000000000000. Button: Save Key. VCSelectENCKey: Old: 00000000000000000000000000000000. New: 05000000000000000000000000000000.
- PICC Configuration**: AuthKey = PICCKey. Text: This is a non reverse process; Once the flag is turned On, it cannot be turned Off. ProximityCheck and VirtualCard are for EV2 only. Checkboxes: Disable Format PICC, Enable Random UID, Enable PCMandatory, Enable AuthVCMandatory. Button: Write Card.
- Access Method**: ☒ ProximityCheck, VirtualCard, PICC, AES EV2. Current selection : App 1, Key0.

Empty the VCProximityKey field. Click  to program the keys to the card and hence enable the keys. After

that, click  to save the keys to reader.

We have enabled both VCSelectMACKey, and VCSelectENCKey.

So now we will turn on the AuthVCMandatory flag.

Please note that Enable Virtual Card is a non reverse process; once the flag is turned on, it cannot be turned off.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

VCConfigurationKey

AuthKey = PICCKey

Old : 00000000000000000000000000000000 Write Card

New : Save Key

VCKey (EV2)

AuthKey = VCConfigKey

VCProximityKey

Old : 00000000000000000000000000000000 Write Card

New : Save Key

VCSelectMACKey

Old : 00000000000000000000000000000000

New : 04000000000000000000000000000000

VCSelectENCKey

Old : 00000000000000000000000000000000

New : 05000000000000000000000000000000

PICC Configuration

AuthKey = PICCKey

This is a non reverse process;
Once the flag is turned On, it
cannot be turned Off.
ProximityCheck and VirtualCard
are for EV2 only.

☐ Disable Format PICC

☐ Enable Random UID

☒ Enable PGMandatory

☒ Enable AuthVCMandatory

Write Card

Access Method

☒ ProximityCheck ☐ VirtualCard

PICC AES EV2

Current selection : App 1, Key0

Check Enable AuthVCMandatory, and click . Now the Virtual Card flag is enabled.

We will try to read Backup file now excluding the Virtual Card, in the access method.

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 2

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 16

Data :

Value : 0

Commit

No

TMC / TMV

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Error

Failed

OK

Access Method

☒ ProximityCheck ☐ VirtualCard

PICC AES EV2

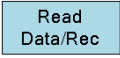
Current selection : App 2, Key0

Click  to read Backup file. Failed! You may need to reset the RF field in order to view this.

Now we include the Virtual Card in the access method.

MR Manual – MF Desfire

The screenshot shows the MR software interface with the 'Data' tab selected. The 'Access Method' section at the bottom is highlighted with a red box, showing 'ProximityCheck' and 'VirtualCard' both checked. Other visible fields include App ID (2), App Key (Default Key), File ID (2), File Type (Backup), File Option (Enciphered), Offset (0), Length (16), Data (01234567890123456789012345678901), Value (0), and a 'Commit' button. The 'Standard / Backup / Cyclic / Linear File' section contains 'Read Data/Rec', 'Write Data/Rec', and 'Clear Rec' buttons. The 'Value File' section contains 'Get Value', 'Debit', 'Credit', and 'Limited Credit' buttons. The 'Commit' section contains 'Commit', 'Abort', and 'Commit (TMAC)' buttons. The bottom status bar shows 'PICC' and 'AES EV2' selected, with 'Current selection : App 2, Key0'.

Click  to get Backup file info. OK.

We have enabled the Proximity Check and Virtual Card. From now on, we need to include these two flags before we can access the card.

Please refer <C:\Mylab\MR> for details communication flow.

20. Random ID

If random UID is necessary in your application, you may enable the Random UID flag in the Configuration Register.

Bear in mind that we have enabled the PCMandatory and AuthVCMandatory flags, we need to include these two flags when we access the card.

Please note that Enable Random ID is a non reverse process; once the flag is turned on, it cannot be turned off.

The screenshot shows the MR software interface with the PICC Configuration window open. The 'AuthKey = PICCKey' section is active. The 'PICC Configuration' section on the right contains the following options:

- ☐ Disable Format PICC
- ☒ Enable Random UID
- ☒ Enable PCMandatory
- ☒ Enable AuthVCMandatory

Below these options is a 'Write Card' button. The 'Access Method' section at the bottom of the window shows 'ProximityCheck' and 'VirtualCard' both checked. The 'Current selection' is 'App 2, Key0'.

Check Enable Random UID, and click

Write Card

We will verify it now.

MR Manual – MF Desfire

MR

Port: Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Load Key

KeyType: Select Save Key

KeyAddr: Select

KeyData:

Access Card

KeyType: Select

KeyAddr: Select

Block: 0

Trans. Block: 0

Trans. Method: Select

Epurse Value:

Data (16B): 08511D45

Halt: No Halt

Read CSN Read Write Value Create Value Block

Access Condition Calculation

Data Blk 0: Select Data Blk 2: Select

Data Blk 1: Select Sec Trailer: Select

DataBlock:	Rd	Wr	Inc	Dec
000	A/B	A/B	A/B	A/B
010	A/B	X	X	X
100	A/B	B	X	X
110	A/B	B	B	A/B
001	A/B	X	X	A/B
011	B	B	X	X
101	B	X	X	X
111	X	X	X	X

SecTrailer:	Key A	Acc Bits	Key B			
Rd	Wr	Rd	Wr	Rd	Wr	
000	X	A	A	X	A	A
010	X	X	A	X	A	X
100	X	B	A/B	X	X	B
001	X	A	A	A	A	A
011	X	B	A/B	B	X	B
101	X	X	A/B	B	X	X

Start

Read CSN

Go to page Classic, click **Read CSN** to read Card Serial Number. The returned data shows the CSN is random. You need to reset the card from the RF field before clicking button Read CSN.

Even though random ID flag is enabled, we can still read the original unique CSN by calling 'Get UID' command, as shown in the Card Info portion.

MR

Port: Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Change PICC Key / Switch KeyType

New KeyType: AES Write Card Save Key

New Key Ver: 0

Old Key: 00000000000000000000000000000000

New PICC Key:

Options

AuthKey = PICCKey Write Card

New App Default Key:

Card Info

SNR: 0451453A841390 Read Card

Free Mem: 000E00

Version: 0401012001805

0401012001805

0000000000000000

CF7CD259704022

Key Setting

AuthKey = PICCKey

Config Changeable

Free Create / Delete

Free Directory List

MasterKey Changeable

Access Right: 0

No of Keys: 0

Access Method

☒ ProximityCheck ☒ VirtualCard

PICC AES EV2 Current selection: App 2, Key0

MR Manual – MF Desfire

Read
Card

Click  to view the real CSN. This command will authenticate the card and return the true unique serial number of the card.

Please take note that after turning on the random ID, the card serial number in the Version info string has become all 00s.

Please refer <C:\Mylab\MR> for details communication flow.

21. ISODFName or VCIID

This feature is not available in EV1 card.

VirtualCard Installation Identifier

The author has fixed the VCIID for picc level as PICC. And we set the name when we created our first application App 1 earlier.

ISODFName

Say we want to change App 1's DF Name to a new name.

Since we are accessing application App 1, load the keys to reader first.

Application ID = 01	Value
Access right	0
DF Name	Conventional 1
Key0	A000000000000000000000000000000000
Key1	A100000000000000000000000000000000

Go to page Roll Key, enter data as shown below, and click

Save
Key

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

Load Key to Reader

KeyNr :

KeyData :

Load New KeySet Key To Reader

Key 0 :

Key 1 :

Access Method

☒ ProximityCheck ☒ VirtualCard Current selection : App 2, Key0

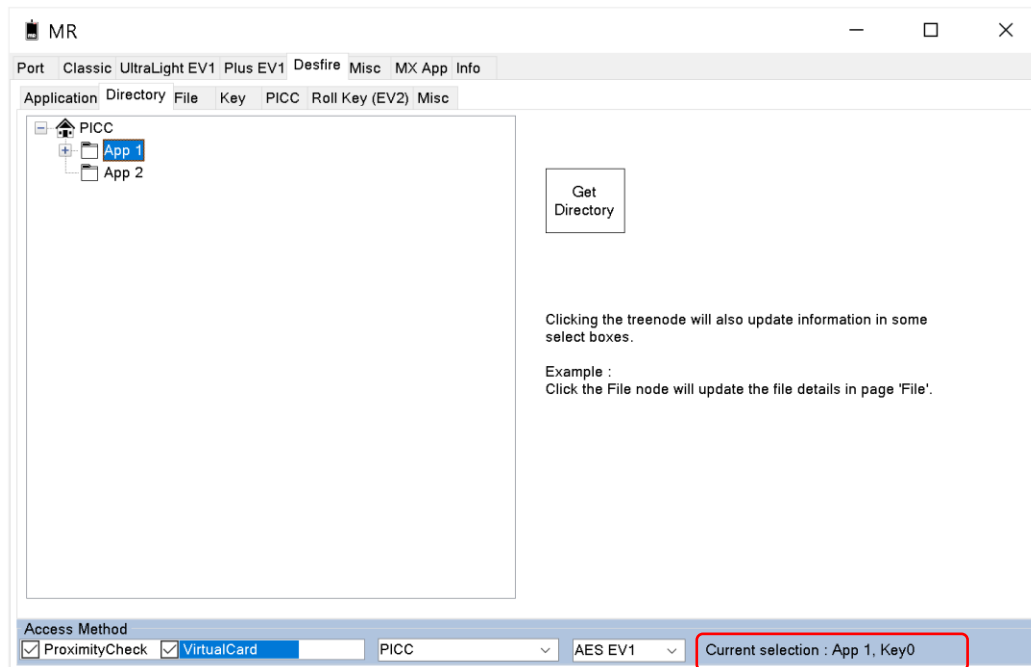
You may load only Key0 as only Key0 (AMK) will be used to change the DF name.

We define the new DF name as below:

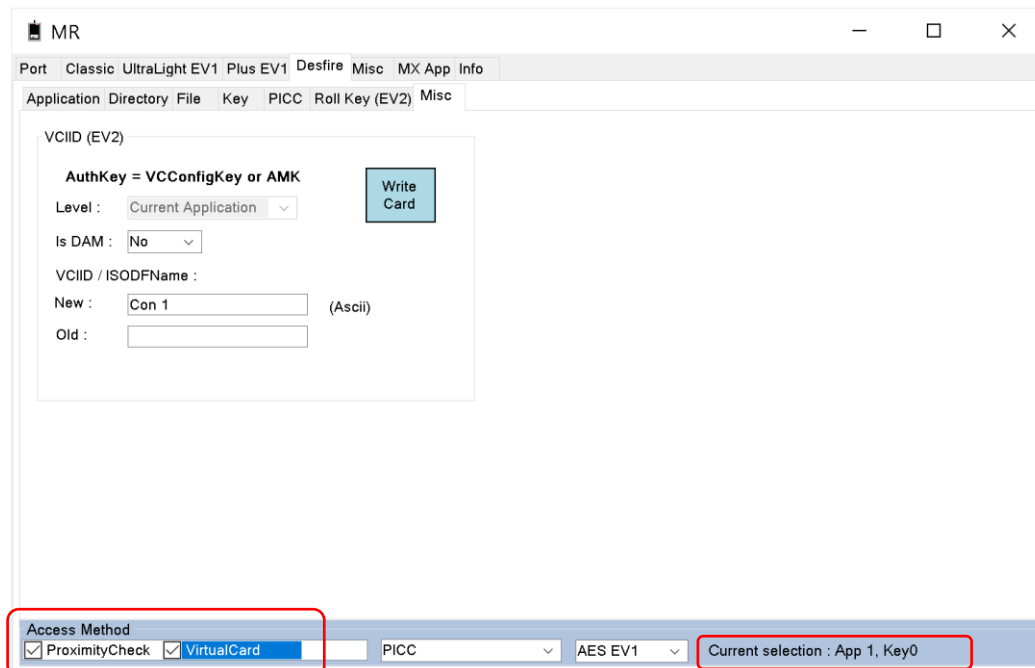
Application ID = 01	Value
Old DF Name	Conventional 1
New DF Name	Con 1

MR Manual – MF Desfire

Go to page Directory, and then select App 1.



Click to select App 1 in page Application.

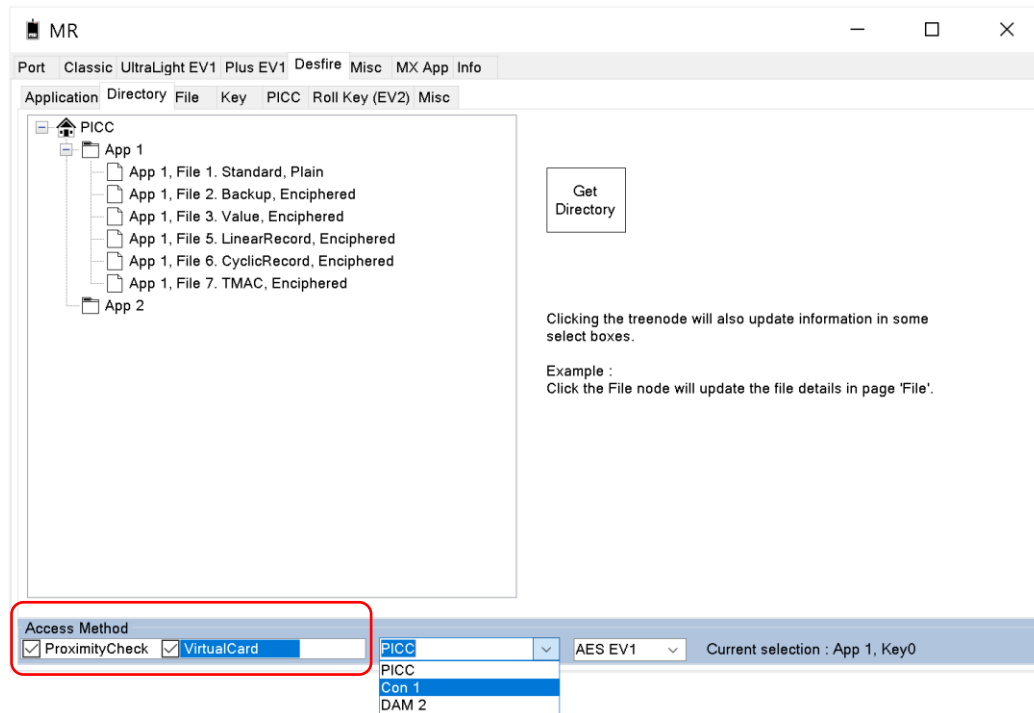


Select Current Application, specify whether it is a DAM application, enter new DF name, and click

Write Card

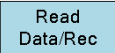
We will verify it now. First go to page Directory, we need to update the Access Method DFName.

MR Manual – MF Desfire



Select PICC in the DFName field, and click . You will see the latest DFName list in the field. You may need to reset RF in order to view this.

Then click to select File 2, Backup in the Directory.

Go to page File, click  to read 10 byte data from the file.

MR Manual – MF Desfire

MR

Port Classic UltraLight EV1 Plus EV1 **Desfire** Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Data Add/Delete

App ID : 1

App Key : Default Key

File ID : 2

File Type : Backup

File Option : Enciphered

Offset : 0

Length : 10

Data : 66778899000000000000

Value : 0

Commit

No

TMC / TMV

Standard / Backup / Cyclic / Linear File

Read Data/Rec Write Data/Rec Clear Rec

Value File

Get Value Debit Credit Limited Credit

Commit

Commit Abort

Commit (TMAC)

Access Method

☒ ProximityCheck ☒ VirtualCard **Con 1** AES EV1

Current selection : App 1, Key0

It works.

To change the DFName for Delegated Application (DAM), you need to enter the old or current DF name, load the current KeySet's Key, and load the DAMMAC Key to the reader before executing the change.

We know that App 2 is a DAM, and its active KeySet is KS2. Therefore, load the following Key to reader:

[illegible]

You may load only Key0 as only Key0 (AMK) will be used to change the DF name.

MR Manual – MF Desfire

And load the DAMMAC Key to the reader. Skip this step if you have previously done this.

Application ID = 02	Value
DAMMAC	11111111111111111111111111111111

MR

Port Classic UltraLight EV1 Plus EV1 Desfire Misc MX App Info

Application Directory File Key PICC Roll Key (EV2) Misc

Load Key DAM Key (EV2) PC / VC (EV2) App Key

AuthKey = PICCKey

DAM is available in EV2 only.

DAM Auth Key

Old : 00000000000000000000000000000000

New :

DAM MAC Key

Old : 00000000000000000000000000000000

New : 11111111111111111111111111111111

DAM ENC Key

Old : 00000000000000000000000000000000

New :

Write Card Save Key

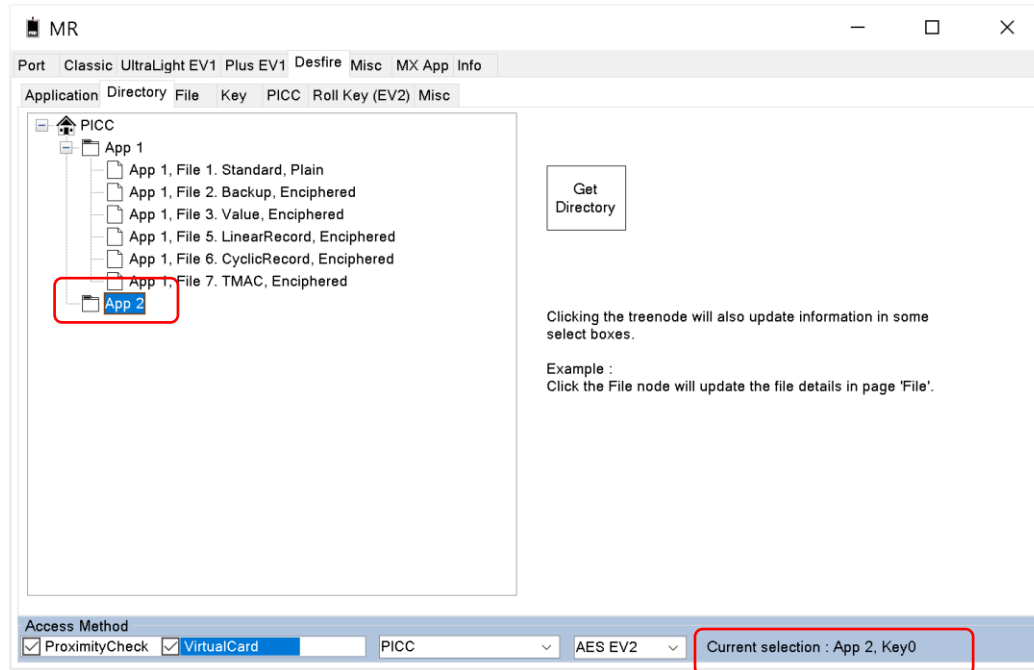
Access Method

☒ ProximityCheck ☒ VirtualCard PICC AES EV1 Current selection : App 2, Key0

Click  to load the DAMMAC key to reader.

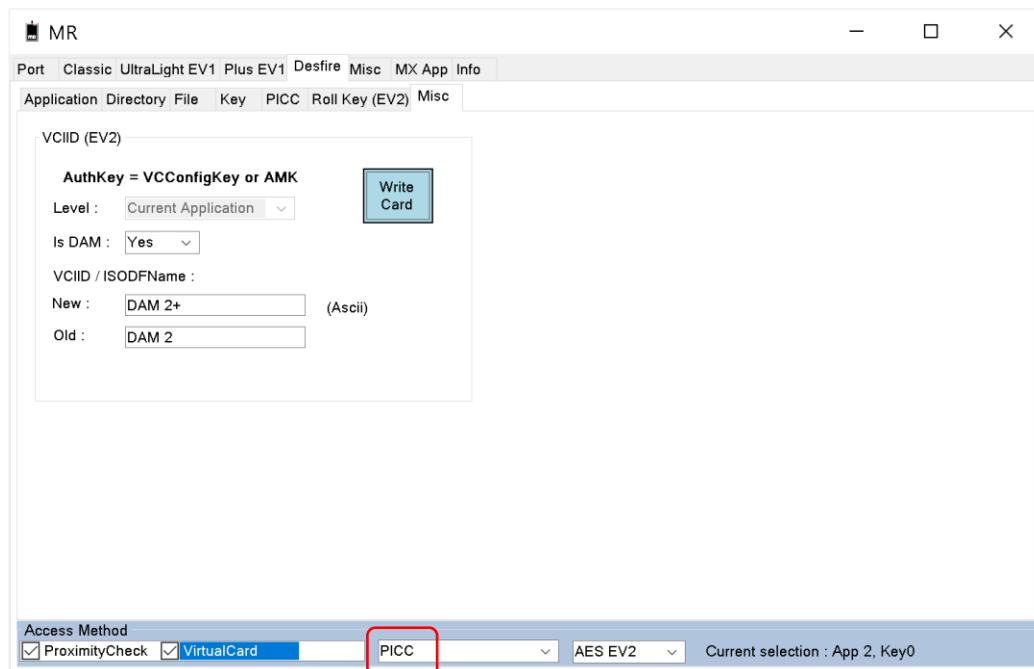
Then select App 2 in the Directory page.

MR Manual – MF Desfire



Now go to page Misc, we are going to change the current App 2 DFName from DAM 2 to DAM 2+.

Application ID = 02	Value
Old DF Name	DAM 2
New DF Name	DAM 2+

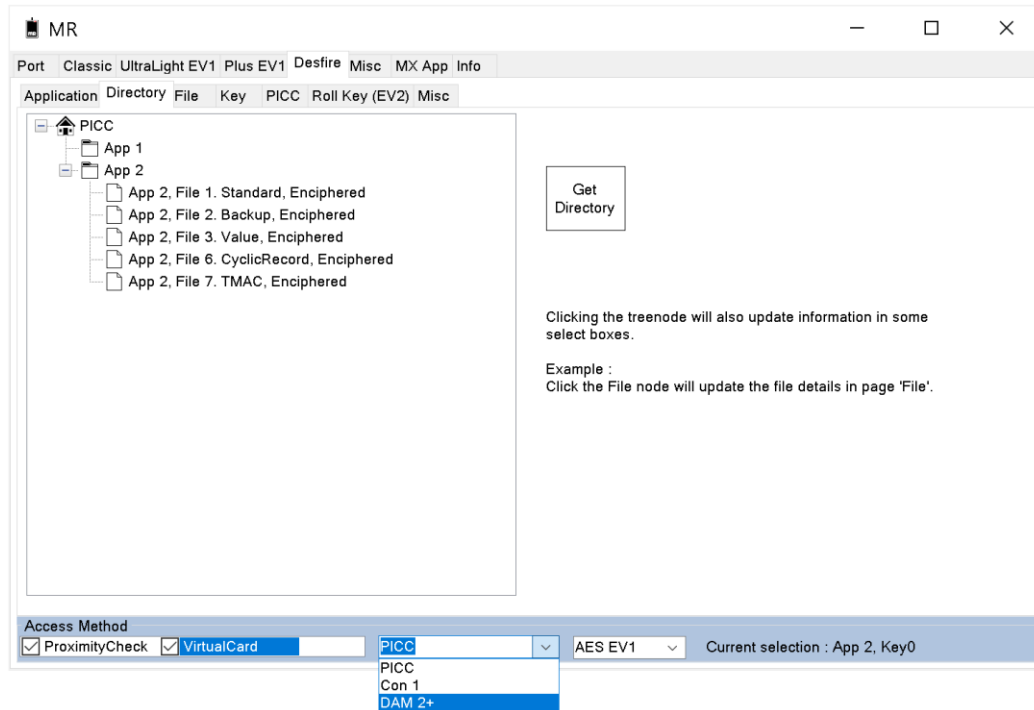


Click  to change the DFName.

MR Manual – MF Desfire

Get
Directory

After this, go to page Directory again, and click .



The DFName list is updated.

Please refer <C:\Mylab\MR> for details communication flow.

22. More on DAM Application

DAM application will be preferred compared to the conventional application, as we can delete the application, and reuse the memory space. Delete DAM application will release the memory space previously occupied by the application. But a conventional application will occupy the space even though it has been deleted.

We enable Keyset in our DAM application, and it is roll-key ready. Key0 are same for all keysets. This means KS0's Key0, KS1's Key0 and KS2's Key0 are same. This is purposely made so that some important feature can still be retrieved after rolling key, using Key0. It is recommended to set Key0 for 'Read' only, 'Write' and other functions that require update, should be set to other keys.

Provided the DAM slot and the DAM ID are same, it is OK to program the card again, as the old application will be formatted, deleted, and recreated at the same slot.

For roll key application, if the card returns error when accessing it, most likely the card's active keyset is different from the reader's. Therefore, we should always get the card's active keyset, before we decide what to do. If the card is running at a higher keyset than the reader's, then the reader should access the card using higher keyset. Whereas if the card's active keyset is lower than the reader, then the reader should perform roll key to the card. So reading 'Current Key Ver' is always necessary in roll key application.

Remember to set the access method correctly when accessing MF Desfire card.

As a last example, consider the following flow:

- Credit an amount (50) to the value file ID 3,
- Save a record to the cyclic file ID 6,
- Read value file balance.

Since value and cyclic files require commit transaction in order to update memory,

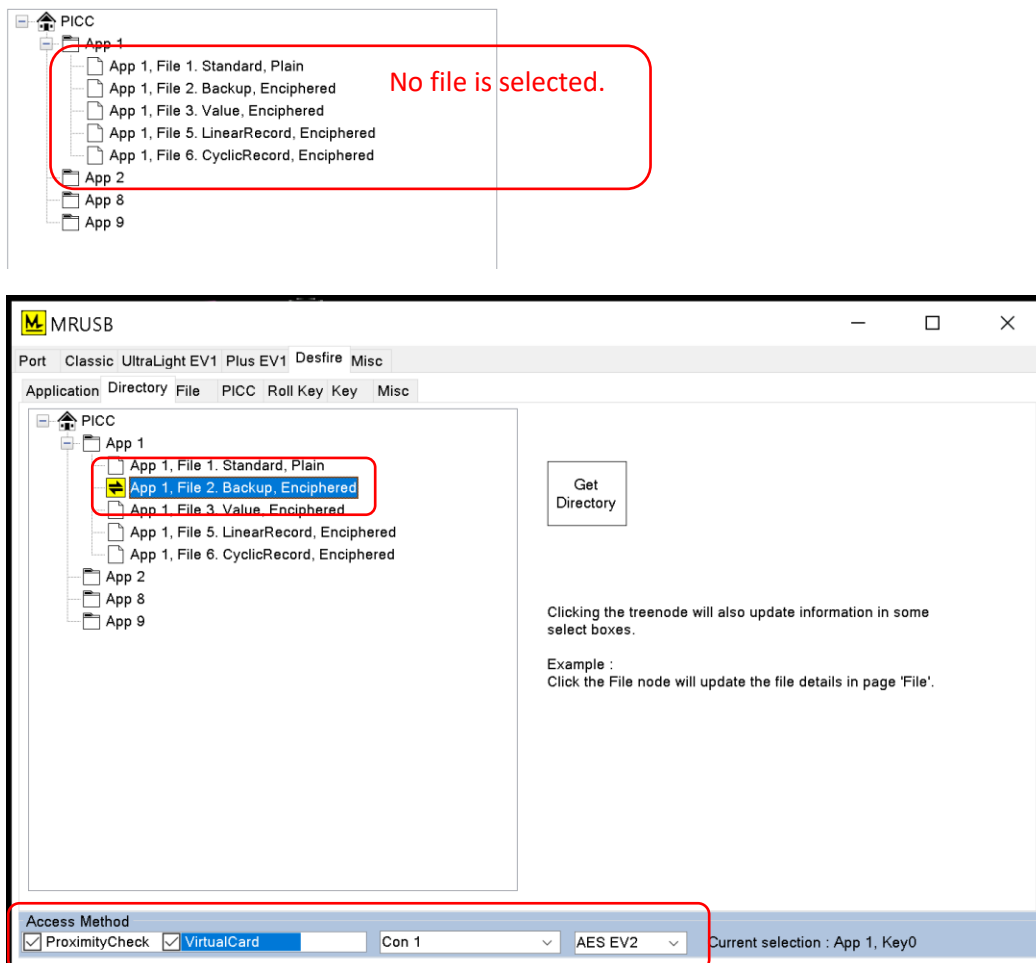
- Credit 50 to value file, but don't call commit now,
- Save a record that include time, location, and action, to cyclic file, and then call the commit transaction. Both value and cyclic files will be updated in one short.
- Send Get Value command to read the value file balance, no update of memory is needed.

23. TroubleShooting

When the reader fails to access the card, most of the time, it is due to the key. As we mentioned before, a successful authentication between reader and card is required before we can access to the card data, and this will only happen if their authentication key are matched. Since the reader can hold only one set of application keys, if the card has more than one application, and each application has different key, then you need to load the right key before you can access the application. Key unmatched is usually the main reason why the authentication fails. So, remember to load the right key.

Another possible common issue is the current active keyset, this is mainly for Roll Key application. The card may have been rolled key, but the system is still using old keyset to access the card, therefore access denied. For Roll Key application, it is necessary to read the card current active keyset version, and load the appropriate key to the reader.

Also, if the targeted file is not selected, and the Access Method is incorrectly set, access to the card will fail too.



Select a file in the directory tree, set the Access Method correctly, in order to access card.

MR Manual – MF Desfire

24. Important Summary of Keys

Card CSN : 04 25 6B CA B1 5D 80

Item	Value
PICC MasterKey (AES)	01020300000000000000000000000000
PICCDAMAUTHKEY	10101010101010101010101010101010
PICCDAMMACKEY	11111111111111111111111111111111
PICCDAMENCKEY	12121212121212121212121212121212
Default App Key	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
VCIID	PICC (PICC DFName)
VCConfigurationKey	02000000000000000000000000000000
VCProximityKey	03000000000000000000000000000000
VCSelectMACKey	04000000000000000000000000000000
VCSelectENCKey	05000000000000000000000000000000
ProximityCheck	Enabled
VirtualCard	Enabled
Random UID	Enabled
Conventional 1	DF name : Con 1 Key 0 = A0000000000000000000000000000000 Key 1 = A1000000000000000000000000000000
DAM 2	Access right 0 DFName: DAM 2+ KS Access Right 0 Slot no = 2 Slot Ver = 255 Quota Limit : 20 KS0 Key0 20000000000000000000000000000000 KS0 Key1 21000000000000000000000000000000 KS1 Key0 20000000000000000000000000000000 KS1 Key1 23000000000000000000000000000000 KS2 Key0 20000000000000000000000000000000 KS2 Key1 35000000000000000000000000000000 Current Key Ver = 02

Notes:

If ProximityCheck or VirtualCard are enabled, remember to load VCProximityKey VCSelectMACKey, and the VCSelectENCKey to reader. Else the authentication will be failed.

If the application is DAM, then loading DAM Auth, DAM MAC, and DAM ENC Keys are necessary.

25. End