

MIFARE® PLUS DEMO MANUAL Version 1.0

GUI examples:

C#:

https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-mfp-examples-csharp-gui.git C++:

https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-mfp-examples-cpp-gui.git

Console examples:

C:

https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-mfp-examples-c.git

C#:

https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-mfp-examples-csharp-console.git

1



Table of contents

About Mifare® Plus cards	3
Application demo	3
Revision history	14



About Mifare® Plus cards

- Keys can be stored as MIFARE® CRYPTO1 keys (6 bytes per sector) and AES keys (16 bytes per sector) - Memory structure identical to MIFARE® Classic 4K (sectors, blocks)

Application demo

When you simply double click on the .exe and the program starts, you shall see that we have option of Reader Open the usual way, with our ReaderOpen() function, or you can check the "Use Advanced options" and use our Advanced options parameters to open communication port with ReaderOpenEx function, provided you input correct parameters in Advanced options fields (reader type, port name, port interface and additional argument). When the port has been successfully open, it will print out "ReaderOpenEx was successful" in lower left corner and reader description in the text box on the bottom of the application. After successful port open, it will start continuous search for card in its NFC field. If found – it will print out cards type and UID in upper left corner. If not, it will show UFR_NO_CARD in the same place where cards type would be. For example:

🛃 Mifare Plus example				- 0 >	<
Reader Open					
Reader Open	Advanced options Reader type:	Port name	Poit interface. arg		
Card information Card type: DL_MIFARE	_PLUS_S_4K_SL1 Card UID: 04:30	0.69:04:78:23:80:00:00:00	Auth mode Provided AES key	O Reader AES key	
Personalization Auth SL1	Switch to SL3 Change Master Key Chang	e Conlig Key Change Sector key	Field Config Set Get UID	Change VC poling f	•
Card master key:	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	SL1 card authentication key:	FFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFF	
Card configuration key:	FFFFFFFFFFFFFFFFFFFFFFFFFFFFF	Select VC key:	FFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFF	
Level 2 switch key:	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	Provimity check key:	FFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFF	
Level 3 switch key	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	VC polling ENC keys	FFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFFFF	
VC polling MAC key	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	1	Personalize card		
All keys must be 16 byte	s long.				
leaderOpen was succes	ssful.				3



From the above picture, we can see all of the tabs dedicated to working with MIFARE® Plus cards. Keep in mind that not all functions mentioned in this demo work with all three cards security levels. Also, all functions on these tabs, except for the last three – "Data read, data write, Write keys into reader" depend on Authentication mode that can be chosen in upper right corner. If we check "Provided AES key" then we will use functions with provided key required. And vice versa, if we check "Reader AES key" then our functions will use reader key that we select on our tabs.

🖳 Mifare Plu	us example						-		×
Card informatio	n DL_MIFARE	_PLUS_S_4K_S	L1 Card U	D: 04.45:91:0A.78:2	3:80:00:00:00	Auth mode Provided AES key	O R	leader AE	Skey
Personalization	Auth SL1	Switch to SL3	Change Master Ke	y Change Config Key	Change Sector k	ey Field Config Set Get U	ID Chang	e VC pollir	ng E 🔹 🕨

Personalization Auth SL1 Switch to SL3 Change Master Key Change Config Key Change Sector key Field Config Set Get UID Change VC poling [FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF SL1 card authentication key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF Card master key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF Select VC key: Card configuration key: Level 2 switch key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF Proximity check key: Level 3 switch key VC polling ENC key: FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF Personalize card VC polling MAC key FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

Let's start from Personalization tab:

All keys must be 16 bytes long.



On this tab we have 9 keys that the card uses for its intended use and purpose. Inputting all of them and clicking the "Personalize card" button will have our card set up for future use. All of these keys have their use explained in their names. For example "Card configuration key" is used for changing cards configuration settings, such as Field configuration settings, authorization of changing VC polling ENC/MAC keys, reader AES keys, etc.. Cards default security level is Security Level 0. Cards security level automatically updates to level 1 as soon as we complete card Personalization. On this level we can also choose AES authentication, which is by default used on SL3. We accomplish that on the next tab.

Personalization	Auth SL1	Switch to SL3	Change Master Key	Change Config Key	Chan
Provided AES	key		10		
Enter SL1 card	l authentica FFFFFFFFF	tion key: FFFFFFFFFFFFF]		
Reader AES k	ey ev index for	SL1 card auther	tication (0 - 15);		
0 ~					
	AES authe	ntication on SL1			

On this tab, depending on what authentication mode we selected in the upper right corner, we use one of these keys to enable MIFARE® Plus authentication with AES keys instead of CRYPTO1 while it's in SL1 mode. MIFARE® Plus supports all MIFARE® Classic value-block operations either in SL1 or SL3 mode. After security upgrade to SL3 mode, MIFARE® Plus uses Advanced Encryption Standard (AES) for authentication, data integrity and encryption. In our demo we switch to SL3 on the next tab – "Switch to SL3".

3 switch key (0) - 15)	
	3 switch key (l	3 switch key (0 - 15)

Usage of this tab is same for the previous. We check the authentication mode in the upper right corner, enter or select key that we will use to authenticate this process and click on the button.

On next tab, we can change cards Master key. To do so, we must enter previous, old master key so we can authorize usage of the new key that we enter.





The same principle goes for all of the key changes mentioned in our demo with an exception of changing sector key - where we have to specify for which sector we shall be changing AES key.

As for the Field configuration settings, in other words use choice of Random UID that Desfire cards have or regular UID, we authorize that setting with our cards Configuration key and select one of our options on top: Use random UID or standard UID:

Personalization	Auth SL1	Switch to SL3	Change Master Key	Change Config Key	Change Sector key	Field Config Set	Get UID
Random ID or	otion						
O use randor	n ID						
0							
use UID							
Provided AES	kev						
Configuration	key: FFFF	FFFFFFFFFFFFF	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF				
				1			
D-1-1501	Sec.						
Enter reader	configuratio	n key index (0 - 1	15):				
	coningeratio	intel index (0	1.57.				
0 ~			_				
F	ield configur	ation set					
	and the second second second						

The random UID feature means that the cards UID is new every time it is powered on, which means every time it is used. To randomise the UID means that everytime the card is used, a new UID is recorded. This each activity of the card cannot be linked to the user, and he chain of activity cannot be traced to the card. Card needs to be in SL3 mode to use this feature. Only way to get cards true UID with this feature enabled is to get UID with usage of VC polling ENC & MAC keys. We will demonstrate this in next tab "Get UID".

For example, our card generates a random UID like this:

	Digita	al Logic	
#1			
🖳 Mifare P	lus example		
Card informat	on		
Card type:	DL_MIFARE_PLUS_S_4K_SL3	Card UID:	08:9C:C7:37:00:00:00:00:00:00
#2			
NAT A	lus evample		

Each time our card gets into NFC field and gets powered on - it shall get new randomized UID. To see cards true/factory UID, we enter ENC and MAC key or select them by their index if they are stored in the reader.

Mitare Plus exa	mple						- U X
Reader Open	_						
Reader Open	Advanced options	Reader type:	Port name		Polt interface:	ag	
Card information				_	Auth mode		
Card type: DL_M	IFARE_PLUS_S_4K_SL3	Card UID: 04:9	1 60:0A 78:23:80:00:0	0:00	Provided AES	key	O Reader AES key
Personalization Aut	h SL1 Switch to SL3 Cha	nge Master Key Chang	ge Conlig Key Chang	e Sector key	Field Config Set	Get UID	Change VC poling [
Random ID option							
O use random UID)						
(a)							
use UID							
use UID Provided AES key							
use UID Provided AES key							
use UID Provided AES key Contiguration key:	FFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Configuration key:	FFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Conliguration key: Reader AES key	FFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi	FFFFFFFFFFFFFFFFFFFFFFF guration key index (0 - 15);	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi	FFFFFFFFFFFFFFFFFFFFFFFFF guration key index (0 - 15):	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi 0 Field c	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi 0 Field c	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi 0	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF						
use UID Provided AES key Configuration key: Reader AES key Enter reader confi 0 ~ Field c	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFFFFFFFFF					
use UID Provided AES key Configuration key: Reader AES key Enter reader confi 0 Field c Field c	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF						
use UID Provided AES key Configuration key: Reader AES key Enter reader confi 0	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF						

From the image above we can see that UID has changed and will be so until we enable random UID again. From the text box below we can see that our settings were set successfully.

Now we shall demonstrate Data reading and writing. This section has an exception of different authentication modes and different reading/writing modes influenced by our choice of previously mentioned authentication modes.

Here we have Key A and Key B authentication modes, as for the modes of reading/writing we have Provided key mode, Reader key mode, AKM1 mode and AKM2 mode. For reference of these settings such as KeyA/B authentications and AKM1/2 mode, you can find explanations in our UFR Series NFC reader API here: <u>https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-doc</u>



Example for Block read:

eader Open					
Reader Open	Advanced options	Advanced options Reader type: P	ort name: P	ort interface	ag []
ard information			A	uth mode	
Card type: DL_MI	FARE_PLUS_S_4K_SL1	Card UID: 04:30.6	9:04 78:23:80:00:00:00) Provided AES key	 Reader AES key
ange Config Key	Change Sectorkey Field (Config Set Get UID Cha	nge VC poling ENC key Change	VC polling MAC key D	ata read Data write W
Block read Block i	n sector read Linear read				
Provided key			Reader key		
Authentication n	node		Authentication mode		
Key A	🔘 Кеу В	Block: 0 v	● Key A 🛛 Key B	Blo	ck: 0 ∨
Key: FFFFFFF	FFFFFFFFFFFFFFFFFFFFF	FFF	Readerkeyindex 0 v	0 - 31 for CRYPTO	1) and
Block read pro	vided key		Block read reader key		
AKM1 key			AKM2 key		
Authentication	mode		Authentication mode		
Key A	⊖ KeyB	Block: 0 V	🖲 Кеу А 🔘 Кеу	B Bi	ock: D 🗸
Block read Al	:M1 key		Block read AKM2 key		
Block: (0 - 128 for	2K cards) and (0 · 255 for 4	k cards)			
ck read was si	uccessful.				
ck data: 04:30	0:69:0A:78:23:80:18	:42:00:04:01:11:00	:39:11		

Here we see that we successfully read block 0 with one of these functions, and block data has been written in the bottom of the screen.



Similar principle goes for Data writing with exception of entering data we wish to write in our card, for example Block write:

ader Upen				
Reader Open	Advanced options Reader type: Po	I name Port inte	eface arg	
d information Card type: DL_MIFARE_PLUS_S_4K_SL3	Card UID: 04:91:60	Auth mo 0A 78:23:80:00:00:00	de ided AES key 🛛 🔿	Reader AES ke
ange Config Key Change Sector key Field C	Config Set Get UID Chang	ge VC poling ENC key Change VC pol	ing MAC key Data read	Data write 🛛 🙀
lock write Block in sector write Linear write				
Authentication mode Key A Key B Block Key: FFFFFFFFFF Block write provided key	ick: 1 v	Authentication mode Key A Key B Key index 0 V (0 - 31 f (0 - 15 f Block write reader key	Block: 8 ~ or CRYPTO 1) and or AES) key	
AKM1 key Authentication mode	ick: 0 ~	AKM2 key Authentication mode Key A Key B Block wille AKM2 key	Block: 0 v	
Block: (0 - 128 for 2K cards) and (0 - 255 for 4	k.cards)			
Data: 000102030405060708090A0B0CI	ID DE OF			
k write was successful.				

We just choose block that we wish to write into, enter or select key if needed and click on the provided button. If we go back to reading, we will see our data written in, for example, block 1 successfully.



	1	Advanced options			
Reader Open	Advanced options	Reader type:	Port name:	Poit interface:	erg
Card information				Auth mode	
Card type: DL_MI	FARE_PLUS_S_4K_SL3	Card UID: 04	91:60:0A:78:23:80:00:00:00	Provided AES ke	y 🔘 Reader AES ke
hange Config Key (Change Sector key Field (Config Set Get UID	Change VC poling ENC key Cha	nge VC polling MAC key	y Data read Data write W
Block read Block i	n sector read Linear read				
Provided key Authentication m Key A	ode O Key B	Block: 0 v	Reader key Authentication mode	(ey B	Block: 8 🗸
Key: FFFFFFFF Block read pro	FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF	FFF	Reader key index 0 Block read reader k	(0 - 31 for CRYF (0 - 15 for AES) ey	2TO 1) and key
AKM1 key			AKM2 key		
Authentication Key A	o KeyB	Block: 0 v	Authentication mode Key A) Key B	Block: 0 v
Block read AK	M1 key		Block read AKM2	key	
Block: (0 · 128 for	2K cards) and (0 · 255 for 4	k cards)			
ock nead was su	rrestul				
sck data: 00:01	:02:03:04:05:06:07	:08:09:0A:08:0C	:0D:0E:0F		
12.25.001.01	R OK				

For storing keys in our reader, we have dedicated tab "Write keys into reader" where we can enter either CRYPTO1 or AES keys, and lock further key input in our device or unlock it.



🛃 Mifare Plus exar	mple				-		×
Reader Open							
Reader Open	Advanced options	Advanced options Reader type: Por	I name	Port interface: arg	r [
Card information Card type: DL_M	IFARE_PLUS_S_4K_SL3	Card UID: 04:91:60:	04.78:23:80:00:00:00	Auth mode Provided AES key	() Re	ader AES	key
Change Sector key CRYPTO 1 Keys CRYPTO 1 key: Enter key index (0 - Write CRYPTO Unlock reader	Field Conlig Set Get UID FFFFFFFFFFFF 31): 0 ~ 01 key into	Change VC poling ENC key	Change VC poling MAC k AES keys AES key FFFFFFF Enter key index (0 - 15) Write AES key into Lock reader	ey Data read Data write	Write keys i	nto reade	,
Password: Unlock I	keys		Password:				
RYPTO 1 key wri	ting was successful	L					
Success: [0:00 (0)] U	FR OK						

As a reminder: CRYPTO1 key is 6 bytes long, AES key is 16 bytes long, and our password input is 8 characters, for the sake of simplicity.

API reference for functions used in this demo: <u>https://www.d-logic.net/code/nfc-rfid-reader-sdk/ufr-doc</u>



Revision history

Date	Version	Comment
2019-04-09	1.0	Base document