JMY600 Series IC Card Module

MIFARE Plus Card Operation Guide

（Revision 1.22）

Jinmuyu Electronics Co., LTD

Oct. 11, 2019

Please read this manual carefully before using. If any problem, please feel free to contact us, we will offer a satisfied answer ASAP.

Contents

1 Overview

This file describes how to operate MIFARE Plus X 4K card and the sequence via using JMY600 Series RFID module. It is suitable for the programmers who are using it to do the development.

Any questions during the programming, please feel free to contact our technical support via jinmuyu@vip.sina.com.

2 Features

- 2 or 4 KB EEPROM
- Simple fixed memory structure compatible with MIFARE Classic 1 K (MF1ICS50), MIFARE Classic 4 K(MF1ICS70)
- Migration path from MIFARE Classic to MIFARE Plus security level supported
- Open standard AES crypto for authentication, integrity, and encryption
- Common Criteria certification: EAL4+ for IC HW and SW
- Complies with ISO/IEC 14443-A
- 7-Byte Unique Identifier (UID) or 4-Byte Non Unique Identifier(NUID) and random IDs
- Multi-sector authentication, multi-block read and write
- Anti-tear function for writing AES keys
- Keys can be stored as MIFARE Classic CRYPTO1 keys(2 x 48 bit per sector) or as AES keys (2 x 128 bit sector)
- Supports virtual card concept
- High data rates up to 848 kbit/s
- Available in MOA4 modules or 8-inch sawn bumped wafer

3 General Description

NXP MIFARE Plus is based on open global standards both for air interface and cryptographic methods. It is available in two versions: MIFARE Plus S, the Slim version, for straightforward migration of MIFARE Classic systems, and MIFARE Plus X, the eXpert version, which offers more flexibility to optimize the command flow for speed, privacy, and confidentiality.

MIFARE Plus X offers a rich feature set, including proximity checks against relay attacks.

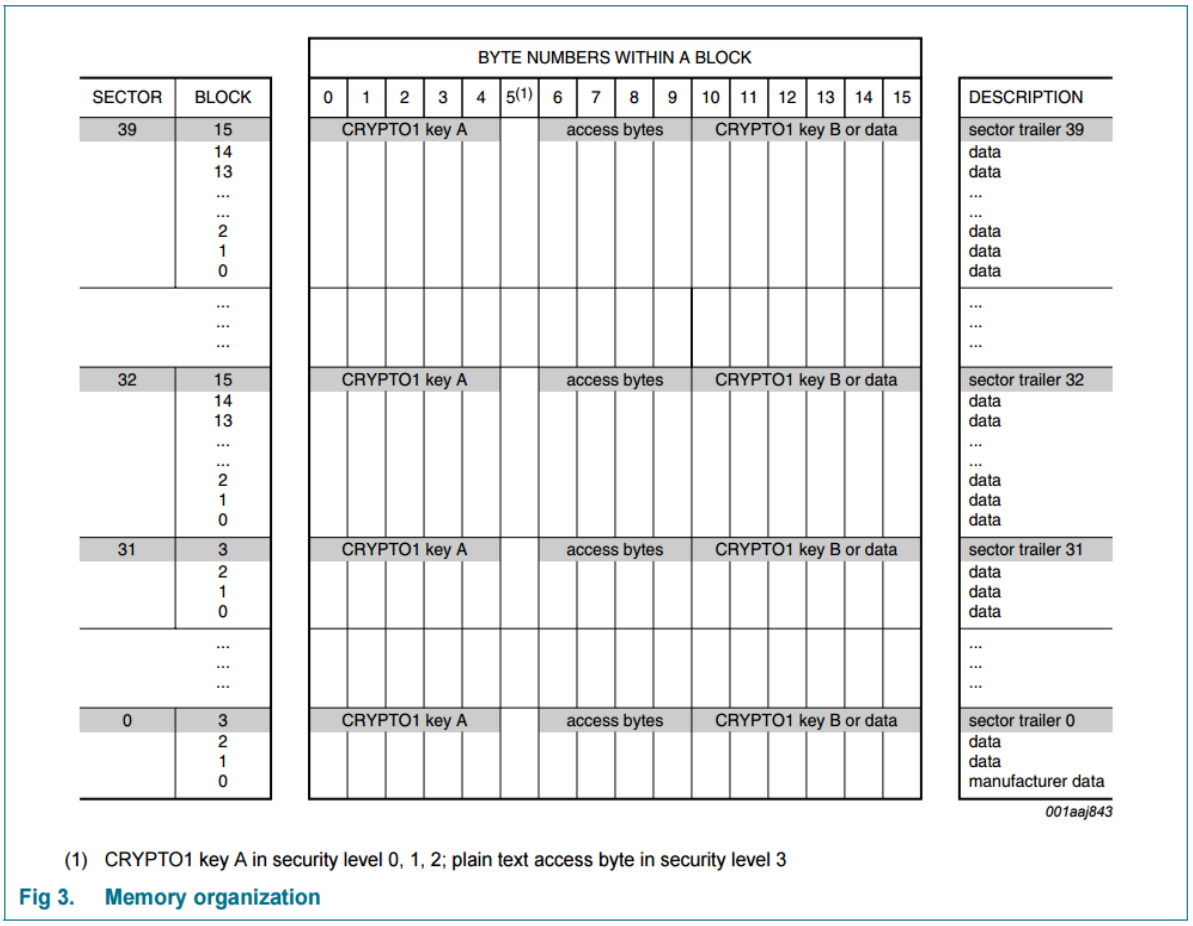
MIFARE Plus is fully functional backwards compatible with MIFARE Classic 1 K / 4 K. Interoperability with MIFARE Classic has been verified by the independent MIFARE Certification Institute. MIFARE Plus offers the possibility to issue cards seamlessly into existing MIFARE Classic applications, before the infrastructure is upgraded. Once the infrastructure security upgrades are in place, MIFARE Plus cards can be switched to a more secure mode in the field with no customer interaction necessary.

AES (advanced encryption standard) is then used for authentication, encryption, and data

integrity. MIFARE Plus supports high-speed communication between the card and terminal at up to 848 kbps/s, for time critical services. The read range of up to 10 cm increases the convenience of the touch-and-go experience.

4 Memory Organization

The 4 kB EEPROM memory (MF1PLUS80x) is organized in 32 sectors of 4 blocks and in 8 sectors of 16 blocks. The 2 kB EEPROM memory (MF1PLUS60x) is organized in 32 sectors of 4 blocks. One block consists of 16 bytes.



(1) CRYPTO1 key A in security level 0, 1, 2; plain text access byte in security level 3

Fig 3. Memory organization

Command	HEX Address	Description
Blocks and Data		
MIFARE Data/Value Blocks MIFARE Sector Trailers	00 00h to 00 7Fh	Sector 0 to 31
MIFARE Data/Value Blocks MIFARE Sector Trailers	00 80h to 00 FFh	Sector 32 to 39
MFP Configuration Block	B0 00h	Defines the number of unmaced commands as well as if plain communication is possible.
Installation Identifier	B0 01h	Installation identifier as used in VC concept. The installation Identifier can be requested from NXP.
ATS information	B0 02h	The 'Answer To Select' Information
Field Configuration Block	B0 03h	Defines if Proximity Check is mandatory and if RandomID shall be enabled.
Key		
AES Sector Keys	40 00h to 40 3Fh	AES Sector Key**s** from Sector 0 to 31. The second byte defines the sector number and which key (Key A or Key B) is used. KEY A = sector number muitiplied by 2 KEY B = sector number muitiplied by 2 + 1 E.g. Key A for sector 2 has the number: 40 04
AES Sector Keys	40 40h to 40 4F	AES Sector Key**s** from Sector 32 to 39. The second byte defines the sector number and which key (Key A or Key B) is used. KEY A = sector number muitiplied by 2 KEY B = sector number muitiplied by 2 + 1
Originality Key	80 00h	The originality is personalised by NXP to the IC and cannot be changed. As the value of the key is not distributed outside of NXP, the authentication with this key is only possible with a special prepared SAM, supplied by NXP.
Card Master Key	90 00h	Can be used to change the Level Switch Keys as well as the MFP Configuration key.
Card Configuration Key	90 01h	Can be used to change the Field Configuration Block
Level 2 Switch Key	90 02h	Key to switch from Level 1 to Level 2
Level 3 Switch Key	90 03h	Key to switch from Level 2 to Level 3
SL1 Card Authentification Key	90 04h	Key to do one additional AES authentification in security level 1
Select VC Key	A0 00h	Key to perform Select VC
Proximity Check Key	A0 01h	Key to verify the Proximity Check
VC Polling ENC Key	A0 80h	Select VC Polling ENCKey
VC Polling MAC Key	A0 81h	Select VC Polling MAC Key

There are four security levels for MIFARE Plus.

Security level 0:

Initial delivery configuration initial, used for card personalization.

Security level 1:

Functional backwards compatibility mode (with MIFARE 1K/4K/Mini) with an optional AES authentication.

Security level 2:

3Pass Authentication based on AES followed by MIFARE CRYPTO1 authentication, communication secured by MIFARE CRYPTO1. The MIFARE CRYPTO1 uses session keys derived from the AES and MIFARE CRYPTO1 authentication.

Security level 3:

3Pass Authentication based on AES, new data manipulation commands secured by encryption and MAC-ing method, using AES.

JMY600 serise RFID read and write module support Security level3 fully; support Security level2 partly.

5 Card Operation

5.1 Active Mode

Under this working mode, the Reader Module just output Card Serial Number. For MIFARE Plus card, we don't recommend to use.

5.2 Passive Mode

5.2.1 MIFARE Plus Initialization Commands

The MIFARE Plus offers a unique feature to support migration from CRYPTO1 based systems to AES based operation. The migration on the card-side is done using different security levels supporting different cryptographic algorithms and protocols. There are four security levels. If the card is a L3 card the Commit Perso command will switch the card directly from security level 0 to security level 3 instead of security level 1. The security level switching (i.e. from security level 1 to security level 3) is performed using the dedicated AES authentication switching keys. The security level can only be switched from a lower to a higher level, never in the opposite direction.

During operating the MIFARE Plus card, the module auto-detecting card function must be shut down. For the multi-card operation function, the user may choose according to the needs.

We provide application commands are based on Level 3. In the card level 3, the authentication use AES encryption algorithm. In the communication process between module and card, all are using encrypted data + command with MAC + response with MAC mode. So the security of RF communication is extremely high.

Put a new MIFARE Plus (L3) card into the antenna field, then to do the test via TransPort test

tool. Please send the commands like the following sequence.

- Request Card according to EMV and PBOC:

  TransPort input: 32

  Host sends: 00 04 00 32 36

  Success: 00 1C 01 32 41 07 04 0C 4D 0A D7 2C 80 42 00 20 0C 75 77 80 02 C1 05 2F 2F 01 BC D6 1C

- Write Perso：

  This command is used to change the data and AES keys from the initial delivery configuration to a customer specific value. The communication is in plain.

  - Write into AES Sector Keys:

  The Key HEX address is 0x4000 ~ 0x403F, 0x4040 ~ 0x404F (MIFARE Plus 4K), 0x9000 ~ 0x9003. For the detailed, please refe to the above"Memory Organization" table. Please write these address values step by step via TransPort. Or you can use MR780 to write them into MIFARE Plus at one time via TransWin.

  TransPort input: 33 40 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

  Host sends: 00 16 00 33 40 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 65

  Success: 00 05 01 33 90 A7

  In the above command, the starting address is 0x40 00. Please cycling execution "33" this command to write into the address one by one, the address is as 0x4001, 0x4002 until 0x404F, and then write into 0x9000, 0x9001, 0x9002 and 0x9003. For testing convenience, the key value can be 16bytes 0xFF.

  - Write into MFP Configuration Block:

  TransPort input: 33 B0 00 00 0F FF FF FF FF FF FF FF FF FF FF FF FF FF

  Host sends: 00 16 00 33 B0 00 00 0F FF FF FF FF FF FF FF FF FF FF FF FF FF 9A

  Success: 00 05 01 33 90 A7

- Commit Perso：

  Level 0 command, to switch Level 0 to Level 1 or Level 3. Target Level depends on the card. If need switch to Level 1 or Level 3, please tell the suppliers when purchasing. Before using this command, please use MIFARE Plus Write Perso command to write all AES key and the initial value of all the blocks, then make the changed data effect.

  TransPort input: 34

  Host sends: 00 04 00 34 30

  Success: 00 05 01 34 90 A0

  Note: At this point, the card level has been switched, but switch to which level rely on card factory settings.

- MIFARE Plus Switch to Level 3

  If the card is in Level 1, then you need further switch to next level until to be in Level 3. If MIFARE Plus is in Level 1, that is compatible with MIFARE 1. In the returned SAK, it doesn't support ISO14443-4, so need to execute "ISO14443 TYPE A Request" and "ISO14443-4 TYPE A Card Reset (RATS)" commands.

  ISO14443 TYPE A Request:

  TransPort input: 20 00

  Host sends: 00 05 00 20 00 25

  Success: 00 0E 01 20 04 34 5F 0A D7 2C 80 42 00 18 6B

ISO14443-4 TYPE A Card Reset (RATS):

TransPort input: 30

Host sends: 00 04 00 30 34

Success: 00 10 01 30 0C 75 77 80 02 C1 05 2F 2F 01 BC D6 02

- Switch to Level 3:

TransPort input: 35 03 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Host sends: 00 15 00 35 03 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 23

Success: 00 05 01 35 90 A1

Now the MIFARE Plus card is in Level 3. Please move it away, and then put it into antenna RF field again.

5.2.2 MIFARE Plus Application Layer Commands

- MIFARE Plus Request and RATS according to EMV and PBOC:

TransPort input: 32

Host sends: 00 04 00 32 36

Success: 00 1C 01 32 41 07 04 0C 4D 0A D7 2C 80 42 00 20 0C 75 77 80 02 C1 05 2F 2F 01 BC D6 1C

- MIFARE Plus Application Layer Commands:

TransPort input: 36 00 00 05 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

Host sends: 00 17 00 36 00 00 05 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 25

Success: 00 05 01 36 90 A2

- MIFARE Plus Data Block Write:

TransPort input: 38 00 05 01 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Host sends: 00 17 00 38 00 05 01 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 2B

Success: 00 05 01 38 90 AC

- MIFARE Plus Data Block Read:

TransPort input: 37 00 05 01

Host sends: 00 07 00 37 00 05 01 34

Success: 00 15 01 37 90 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F B3

- MIFARE Plus Purse Create:

TransPort input: 39 00 04 00 01 00 00

Host sends: 00 0A 00 39 00 04 00 01 00 00 36

Success: 00 05 01 39 90 AD

- MIFARE Plus Purse Read:

TransPort input: 3A 00 04

Host sends: 00 06 00 3A 00 04 38

Success: 00 09 01 3A 90 00 01 00 00 A3

- MIFARE Plus Purse Increment:

TransPort input: 3B 00 04 00 01 00 00

Host sends: 00 0A 00 3B 00 04 00 01 00 00 34

Success: 00 05 01 3B 90 AF

- MIFARE Plus Purse Read:

TransPort input: 3A 00 04
Host sends: 00 06 00 3A 00 04 38
Success: 00 09 01 3A 90 00 02 00 00 A0

- MIFARE Plus Purse Decrement:
  TransPort input: 3C 00 04 00 01 00 00
  Host sends: 00 0A 00 3C 00 04 00 01 00 00 33
  Success: 00 05 01 3C 90 A8
- MIFARE Plus Purse Read:
  TransPort input: 3A 00 04
  Host sends: 00 06 00 3A 00 04 38
  Success: 00 09 01 3A 90 00 01 00 00 A3
- MIFARE Plus Purse Copy:
  TransPort input: 3D 00 04 00 05
  Host sends: 00 08 00 3D 00 04 00 05 34
  Success: 00 05 01 3D 90 A9
- MIFARE Plus Purse Read:
  TransPort input: 3A 00 05
  Host sends: 00 06 00 3A 00 05 39
  Success: 00 09 01 3A 90 00 01 00 00 A3

5.2.3 Modify card key

Function: In security level 3, a mandatory AES authentication between PICC and reader is conducted, where two keys are generated as a function of the random numbers from the PICC and the reader as well as of the shared key. These two session keys are used to secure the data which is exchanged on the interface between the card and reader. One of the two keys is used to ensure the confidentiality of the command and the response while the other key ensures the integrity of the command and the response.

- MIFARE Plus Request and RATS according to EMV and PBOC:
  TransPort input: 32
  Host sends: 00 04 00 32 36
  Success: 00 1C 01 32 41 07 04 0C 4D 0A D7 2C 80 42 00 20 0C 75 77 80 02 C1 05 2F 2F 01 BC D6 1C
- MIFARE PlusFirst Authenticate:
  TransPort input: 3E 40 02 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  Host sends: 00 16 00 3E 40 02 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 6A
  Success: 00 05 01 3E 90 AA
- MIFARE PlusFollowing Authenticate:
  TransPort input: 3F 40 02 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
  Host sends: 00 16 00 3F 40 02 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 6B
  Success: 00 05 01 3F 90 AB
- MIFARE Plus Key Write:
  TransPort input: 38 40 02 01 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
  Host sends: 00 17 00 38 40 02 01 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 6C

Success: 00 05 01 38 90 AC

- The above operation has already modified the card key, and verifies it at this time. Remove the card and put it back.
- MIFARE Plus Request and RATS according to EMV and PBOC:

  TransPort input: 32

  Host sends: 00 04 00 32 36

  Success: 00 1C 01 32 41 07 04 0C 4D 0A D7 2C 80 42 00 20 0C 75 77 80 02 C1 05 2F 2F 01 BC D6 1C
- Authorize data blocks with new keys:

  TransPort input: 36 00 00 05 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

  Host sends: 00 17 00 36 00 00 05 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 24

  Success: 00 05 01 36 90 A2
- MIFARE Plus Data Block Read:

  TransPort input: 37 00 05 01

  Host sends: 00 07 00 37 00 05 01 34

  Success: 00 15 01 37 90 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F B3

5.2.4 Modify the card configuration block

To modify the card configuration block (address: 0xB000) at LEVEL 3, please proceed as follows:

- MIFARE Plus Request and RATS according to EMV and PBOC:

  TransPort input: 32

  Host sends: 00 04 00 32 36

  Success: 00 1C 01 32 41 07 04 0C 4D 0A D7 2C 80 42 00 20 0C 75 77 80 02 C1 05 2F 2F 01 BC D6 1C
- MIFARE PlusFirst Authenticate:

  TransPort input: 3E 90 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

  Host sends: 00 16 00 3E 90 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF B8

  Success: 00 05 01 3E 90 AA
- MIFARE PlusFollowing Authenticate:

  TransPort input: 3F 90 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

  Host sends: 00 16 00 3F 90 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF B9

  Success: 00 05 01 3F 90 AB
- Write configuration block data:

  TransPort input: 38 B0 00 01 00 0F FF FF FF FF FF FF FF FF FF FF FF FF FF FF

  Host sends: 00 17 00 38 B0 00 01 00 0F FF FF FF FF FF FF FF FF FF FF FF FF FF FF 91

  Success: 00 05 01 38 90 AC

