Smart Card Script Protocol File

Beijing Jinmuyu Electronics Co., Ltd

(Revision 1.03)
2022/3/30

Document modification record

Date	Version	Content
---	V1.00	New document
2021.03.03	V1.01	Add data encryption and decryption instructions
2021.07.07	V1.02	Modify the SAM card operation command structure. Add MIFAR EPLUS, FeliCa, NFC instruction introduction. Add some script examples. Modify the data output command structure and add LED/buzzer control.
2023.03.30	V1.03	Add support for ISO15693

1 Introduction

In the access control system, an executable script file format is used to authenticate a variety of smart cards.

2 Script data storage structure

The system provides 15 script command storage units. Each command is 32 bytes. The 16 commands are placed in a 512-byte FLASH block, and the "Clear Script" command must be used to clear the FLASH, when the command is updated each time. FLASH data is all 0xFF after being cleared.

Command sequence	Length	Address
0	32bytes	0x0000
1	32bytes	0x0020
2	32bytes	0x0040
3	32bytes	0x0060
4	32bytes	0x0080
5	32bytes	0x00A0
6	32bytes	0x00C0
7	32bytes	0x00E0
8	32bytes	0x0100
9	32bytes	0x0120
10	32bytes	0x0140
11	32bytes	0x0160
12	32bytes	0x0180
13	32bytes	0x01A0
14	32bytes	0x01C0

Other available resources:

The system provides two 32-byte RAMs as intermediate data buffers.

RAM 1	RAM 2
32bytes	32bytes

3 Script commands

No.:	Command	Function
1	0xX1	SAM card operation command
2	0xX2	CPU card operation command
3	0xX3	DESfire card operation command
4	0xX4	MIFARE card operation command
5	0xX5	MIFAREPLUS card operation command
6	0xX6	FeliCa card operation command
7	0xX7	NFC lable operation command
8	0xX8	ISO15693 card operation command
9	0xX9	Card commands reservation
10	0xXA	RAM 1 and RAM 2 data comparison command
11	0xXB	Data output command
12	0xXC	Data encryption and decryption

3.1 SAM Card operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x1 SAM card operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command
Parameter A	DATA[2]		0x00 ~ 0x1F Start address of RAM data write command
Parameter B	DATA[3]		0x00 ~ 0x1F RAM data write command data length
APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		Data conforming to ISO7816 format

Detailed command:

Function	Command	SAM No.:	Baud rate	Data
SAM Reset	0x4D	1byte	1byte	no
Sending APDU	0x4F		no	Data conforming to ISO7816 format

SAM No.: 0x01: SAM1
0x02: SAM2

Baud rate: 0x00: 9600 0x01:19200
0x02:38400 0x03:55800

0x04:57600 0x05:115200

0x06:230400 Other values remain

Detailed return:

Function	Data
SAM Reset	ATR
Sending APDU	Data conforming to ISO7816 format

3.2 CPU card operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x2 CPU card operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command
Parameter A	DATA[2]		0x00 ~ 0x1F Start address of RAM data write command
Parameter B	DATA[3]		0x00 ~ 0x1F RAM data write command data length
APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		Data conforming to ISO7816 format

3.3 DESfire card operation command structure

Function: Send the commands in the script to the contactless card in accordance with the commands that comply with the DESfire card operating specifications. Some commands are processed by the card reader.

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x3 DESFire card operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command
Parameter A	DATA[2]		0x00 ~ 0x1F Start address of RAM data write command
Parameter B	DATA[3]		0x00 ~ 0x1F RAM data write command data length

APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		Data conforming to the DESFire command format

In the DESFire card application, most commands can be sent and received in clear text, and some commands need to be encrypted or decrypted by DES, and the data can be sent and received multiple times to complete the function.
This system supports the function of automatic authentication key.

Automatic authentication key command structure:

DESFire command	Key serial number	Key
0x0A	1byte	8 bytes

The DESFire command is conforming to the authentication key in the DESFire specification.
Key serial number: 1byte, the key sequence number is the key sequence in the DESFire specification.
Key: 8bytes, the key is the protection key of the card file.

The above three items are described in detail in the DESFire Datasheet. This command lists the parameters required for the authentication key together, and the card reader automatically completes the authentication process.

3.4 MIFARE card operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x4 MIFARE card operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command
Parameter A	DATA[2]		0x00 ~ 0x1F RAM The starting address of the data writes command.
Parameter B	DATA[3]		0x00 ~ 0x1F RAM The data length of the data write command
APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		command

Detailed command:

Function	Command	Key type	Data block	Key	Data
Read block	0x21	1byte	1byte	6bytes	no
Write block	0x22	1byte	1byte	6bytes	16bytes

Key type: 0x00: KEY A

0x01: KEY B

Data block: S50 card from 0 to 0x3F

S70 card from 0to 0xFF

Key: 6bytes (Unreadable, read script commands are all 0xFF by default)

Detailed return:

Command	Data
Read block	16bytes
Write block	no

3.5 MIFAREPLUS card operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x5 MIFAREPLUS card operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command
Parameter A	DATA[2]		0x00 ~ 0x1F RAM The starting address of the data writes command.
Parameter B	DATA[3]		0x00 ~ 0x1F RAM The data length of the data write command
APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		command

Detailed command:

Function	Command	Key type	Block address	key	Data
Authorization data block	0x36	1byte	2bytes	16bytes	no
Read block	0x37	no	2bytes	no	no
Write block	0x38	no	2bytes	no	16bytes

Key type: 0x00: KEY A

0x01: KEY B

Block address: 2 bytes (MSB)

Key: 16bytes (Unreadable, read script commands are all 0xFF by default)

Data: 16bytes

Detailed return:

Command	Status	Data

Authorization data block	1byte	no
Read block	1byte	16bytes
Write block	1byte	no

Status code： 0x90: success
Other: failure

3.6 FeliCa card operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x6 FeliCa card operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command
Parameter A	DATA[2]		0x00 ~ 0x1F RAM The starting address of the data writes command.
Parameter B	DATA[3]		0x00 ~ 0x1F RAM The data length of the data write command
APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		command

Detailed command:

Function	Command	Data
Send and receive commands	0x2F	According to FeliCa card specification

Detailed return:

Data
According to FeliCa card specification

3.7 NFC Label operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x7 NFC label operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM, no operation 0x1 Command result is written to RAM_1 0x2 Command result is written to RAM_2 0x4 RAM_1 data write command 0x8 RAM_2 data write command

Parameter A	DATA[2]		0x00 ~ 0x1F RAM The starting address of the data writes command.
Parameter B	DATA[3]		0x00 ~ 0x1F RAM The data length of the data write command
APDU Length	DATA[4]		Sending data length
APDU Data	DATA[5~31]		command

Detailed command:

Function	Command	Starting block address	Data
Read block	0x41	1byte	no
Write block	0x42	1byte	4bytes

Starting block address: 1byte

Data: 4bytes

Detailed return:

Function	return value	Remarks
Read block	16bytes	Read 4 blocks of data (16 bytes) by default
Read block	no	

3.8 ISO15693 operation command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x8 ISO15693 operation command
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x0 RAM no operation 0x1 The command result is written to RAM_1 0x2 The command result is written to RAM_2 0x4 RAM_1 Data write command 0x8 RAM_2 Data write command
Parameter A	DATA[2]		0x00 ~ 0x1F RAM, Start address of data
Parameter B	DATA[3]		0x00 ~ 0x1F RAM, Length of the data
APTU Length	DATA[4]		Data length
APTU Data	DATA[5~31]		Data

Detailed command:

Function	Command	Starting block address	Number of blocks(N)	Data
Read block	0x54	1byte	1byte	no
Write block	0x55	1byte	1byte	4*N bytes

Detailed return:

Function	return value	Remarks
Read block	4*N bytes	N represents the number of blocks
Write block	no	

3.9 RAM 1 and RAM 2 data comparison command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0xA RAM 1 and RAM 2 data comparison command.
Operation	DATA[1]	7~4Bit	Reserved
		3Bit	0 = The results are equal, execution continue. 1 = The results unequal, execution continue.
		2~0Bit	Scope 0~7 0 = RAM 1 and RAM 2 data comparison 1 = RAM 1 and APDU data comparison 2 = RAM 2 and APDU data comparison Else RFU
Parameter A	DATA[2]		0x00 ~ 0x1F RAM, Start address of data
Parameter B	DATA[3]		0x00 ~ 0x1F RAM, Length of the data
APTU Length	DATA[4]		Data length
APTU Data	DATA[5~31]		Data

3.10Data output command structure

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0xB Data output
Operation	DATA[1]	7~4Bit	Reserved
		3~0Bit	0x1 Output RAM_1 data 0x2 Output RAM_2 data 0x3 Output card UID
Parameter A	DATA[2]		0x00 ~ 0x1F RAM, The starting location of the data
Parameter B	DATA[3]		0x00 ~ 0x1F Output Length
APTU Length	DATA[4]		0x00 or 0x07
APTU Data	DATA[5~31]		DATA (If the length of the APDU is 0, there is no such data)

Detailed DATA:

Number	BITn	Description	Remarks
DATA[5]	Bit6,7	Reserved	Beep and LED control
	Bit5	Green LED Reverse display	
	Bit4	Red LED Reverse display	
	Bit3	Reserved	
	Bit2	Beep control	
	Bit1	Green LED control	
	Bit0	Red LED control	
DATA[6~7]		Buzzer control time (unit: 10ms)	MSB
DATA[8~9]		Green LED control time (unit: 10ms)	MSB
DATA[10~11]		Red LED control time (unit: 10ms)	MSB

3.11 Data encryption and decryption

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0xC Data encryption and decryption
Operation	DATA[1]	7~4Bit	0x0 SM4 Algorithm (customized) 0x1 DES Algorithm 0x2 3DES Algorithm Other reservations
		3~0Bit	0x0 ECB Mode Other reservations
Parameter A	DATA[2]	7~4Bit	0x1 Operate RAM_1 data and store it in RAM_1 0x2 Operate RAM_2 data and store it in RAM_2 Other reservations
		3~0Bit	0x0 Encryption 0x1 Decryption Other reservations
Parameter B	DATA[3]		Operation data length (integer multiple of 8, maximum 32)
Key length	DATA[4]		Key length (8 Bytes, 16 Bytes)
Key	DATA[5~31]		Key value (unreadable, read script commands are all 0xFF by default)

4 Script command programming example

4.1 DESfire Card operation

Operate the DESFire card: select the application (00 00 01), and authentication key (key

serial number 01, key: 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00), then read out the 16 bytes data from the file (01).

Step1: Select the application

Send:	03 01 00 00 04 5A 00 00 01
03	0: Command number; 3: DESFire card command
01	Command result is written to RAM_1
00	no using
00	no using
04	Sending data length
5A 00 00 01	Data sent to the card, Details refer to DESFire card Datasheet

Step2: Judge the application result (can be omitted)

Send:	1A 01 00 01 01 00
1A	1: Command number; A: RAM comparison command
01	RAM 1 and APDU data comparison
00	Compare RAM start address
01	Compare length
01	Length
00	Data

Step3: Authentication key

Send：	23 01 00 00 12 0A 01 112233445566778899AABBCCDDEEFF00
23	2: Command number; 3: DESFire card command
01	Command result is written to RAM_1
00	no using
00	no using
12	Sending data length

0A 01 112233445566778899AABBCCDDEEFF00

For the data sent to the card, refer to the DESFire Datasheet selection authentication key command and the key authentication instructions in the previous chapter.

Step4: Judge the application result (can be omitted)

Send： 3A 01 00 01 01 00

Refer to the above step2

Step5: Read data

Send：	43 01 00 00 08 BD 03 000000 100000
43	4: Command number; 3: DESFire card command
01	Command result is written to RAM_1
00	no using
00	no using
08	Sending data length

BD 03 000000 100000 refer to DESFire Datasheet read file command

Step6: Judge the application result (can be omitted)

Send： 5A 01 00 01 01 00

Refer to the above step2

Step7: Output result

Send： 6B 01 01 04

6B 6: Command number; B: output data

01 Output RAM_1 data

01 Specify the output location of RAM1

04 Output length

4.2 MIFARE Card operation

Operate the MIFARE card, read the first 4 bytes of the first block.

Step1: Read data

Send： 04 01 00 00 09 21 00 01 FFFFFFFFFFFF

04 0: Command number; 4: MIFARE card command

01 Command result is written to RAM_1

00 no using

00 no using

09 Sending data length

21 00 01 FFFFFFFFFFFF Read the first block data

Step2: Output result

Send： 1B 01 00 04 00

1B 1: Command number; B: output data

01 Output RAM_1 data

00 Specify the output location of RAM1

04 Output length