Smart card script protocol file

1 Outline

In the access control system, a variety of smart cards are authenticated in the form of executable script files.

2 Script data storage structure

There are 15 script commands storage units in the system. Every command is 32bytes. The whole 15 commands are storage in a FLASH (512bytes). Please use "Clear script" command to clear FLASH in advance when updating commands each time. The empty FLASH data are all 0xFF.

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

Other available resources

The system provides two 32 bytes of RAM, as the intermediate data cache.

RAM 1	RAM 2
32 bytes	32 bytes

The system provides a 16-byte output buffer for output script execution results.

Out Buffer
16 bytes

3 Script Commands

No.:		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	0xX5-0xX9	Card command reserved
6	0xXA	RAM 1 and RAM 2 data comparison command
75	0xXB	Data output command

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

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 according to the commands conforming to the DESfire card operation specifications. Some commands are processed by the card readers.

Execution No. & Command	DATA[0]	7~4Bit	Command sequence
		3~0Bit	0x3 DESFire card operation command
Operation	DATA[1]	7~4Bit	Reserved
		Bit3	1=enable; 0=disable; RAM_2 data write command
		Bit2	1=enable; 0=disable; RAM_1 data write command
		Bit1	1=enable; 0=disable; Command results written RAM_2
		Bit0	1=enable; 0=disable; Command results written RAM_1
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]		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 DESFirecommand is conforming to the authentication key in the DESFire specification.

The key sequence number is the key sequence in the DESFire specification.

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

Command explanation:

MIFARE command	Command serial number	Key type	Data block	Key
Read block command	0x21	1byte	1byte	6bytes
Write block command	0x22	1byte	1byte	6bytes

Key type: 0x00: KEYA
0x01: KEYB
Data block: S50 card from 0 to 0x3F
S70 card from 0to 0xFF
Key: 6bytes

3.5 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]		
APTU Data	DATA[5~31]		

3.6 Data 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
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]		
APTU Data	DATA[5~31]		

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).

1, 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

2, 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

3, 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.

4, Judge the application result (can be omitted)
Send： 3A 01 00 01 01 00
Refer to the above second command

5, 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

6, Judge the application result (can be omitted)
Send： 5A 01 00 01 01 00
Refer to the above second command

7, 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 and read the first 4 bytes of the first block.

1, 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

2, Output result

Send： 1B 01 00 04

1B 1: Command number; B: output data

01 Output RAM_1 data

00 Specify the output location of RAM1

04 Output length