JMY600 Series IC Card Module

ICODE SLI-S Custom Commands Operation Guide

（Revision 1.00）

Beijing Jinmuyu Electronics Co., LTD

2022/6/15

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 article introduces in detail the operation method and sequence of using JMY600 series card reader module to operate ICODE SLI-S CUSTOM COMMANDS and basic card functions. You can quickly master the use of ICODE SLI-S electronic label customization instructions by reading this manual. This manual is intended for programmers who use JMY600 series RFID modules. We also have example codes of communication protocols, which can be found on Jinmuyu's website. If you still have any problems while writing the program, please feel free to contact our technical support. Or send an email to: jinmuyu@vip.sina.com and we will give you a satisfactory answer.

2 Features and benefits

- Contactless transmission of data and supply energy (no battery needed)
- Operating distance: up to 1.5 m (depending on antenna geometry)
- Operating frequency: 13.56 MHz (ISM, world-wide licence free available)
- I CODE SLI-S Functionality (ISO/IEC 15693)
  - ♦Fast data transfer: up to 53 kbit/s
  - ♦High data integrity: 16-bit CRC, framing
  - ♦True anti-collision
  - ♦Additional fast anti-collision read
  - ♦Password protected Electronic Article Surveillance (EAS) incl. application selection
  - ♦Application Family Identifier (AFI) supported
  - ♦Data Storage Format Identifier (DSFID)
  - ♦Privacy command with 32-bit Privacy password
  - ♦Destroy command with 32-bit Destroy password
- I CODE EPC Functionality
  - ♦Fast data transfer: up to 53 kbit/s
  - ♦High data integrity: 16-bit CRC, framing
  - ♦Anti-collision with high identification speed (approx. 200 I-CODE EPC smart labelsper second)
  - ♦Label DESTROY command with 24-bit Destroy Code protection for EPCfunctionality only
- Long Range Command
- Write distance equal to read distance
- EEPROM
  - ♦2048 bits (2 kbit), organized in 64 blocks of 4 byte each, 4 blocks are summed up to1 page
  - ♦Data retention of 10 years
  - ♦Write endurance 100.000 cycles
- Security features
  - ♦Unique identifier for each device
  - ♦Lock mechanism for each user memory block (write protection)
  - ♦Lock mechanism for DSFID, AFI, EAS

♦Password (32-bit) protected memory management for Read access
♦Password (32-bit) protected memory management for Write access
♦Password (32-bit) protected Label Destroy
♦Password (32-bit) protected Privacy Mode
♦Password (32-bit) protected EAS Functionality

3 Memory organization

The 2048 bit EEPROM memory is divided into 64 blocks. A block is the smallest access unit. Each block consists of 4 bytes (1 block = 32 bits). 4 blocks are summed up to 1 page for password protection. Bit 0 in each byte represents the least significant bit (LSB) and bit 7 the most significant bit (MSB), respectively.

The Memory is divided into 2 parts:

• Configuration Area

- Within this part of the memory all required information are stored like UID,EPC Data,Write protection,Access control information, Passwords and so on.Direct access to this memory area is not possible.

•User Memory

- Within this area the user data are stored. Direct Read/write access to this part of the memory is possible depending on the related security and writes protection conditions.

Table 3. Memory Organization

Page	Block	Byte 0	Byte 1	Byte 2	Byte 3	Description
-6	-24					Configuration Area for internal use
	-23					
	-22					
	-21					
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
-1	-4					
	-3					
	-2					
	-1					
0	0					User Memory • 10 pages • 4 blocks each • 4 bytes each • (total 160 bytes)
	1					
	2					
	3					
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
:	:	:	:	:	:	
9	36					
	37					
	38					
	39					

4 Card Operation

4.1 Example of basic card operation

Please refer to the "JMY600 series card reader module ISO15693 electronic label operation guide V1.12.pdf" manual.

4.2 Custom Commands operation

4.2.1 Basic Instructions

1） In this example, most of the instructions are in select mode, which helps to reduce the packet size of the transmission.

2）Request flags

Request flags 1 to 4 definitions

Bit Nb	Flag name	State	Description
Bit 1	Sub-carrier_flag	0	A single sub-carrier frequency shall be used by the VICC
		1	Two sub-carriers shall be used by the VICC
Bit 2	Data_rate_flag	0	Low data rate shall be used
		1	High data rate shall be used
Bit 3	Inventory_flag	0	Flags 5 to 8 meaning is according to table 4
		1	Flags 5 to 8 meaning is according to table 5
Bit 4	Protocol Extension_flag	0	No protocol format extension
		1	Protocol format is extended. Reserved for future use

Note: 1. Sub-carrier_flag refers to the VICC-to-VCD communication as specified in ISO/IEC 15693-2.

2. Data_rate_flag refers to the VICC-to-VCD communication as specified in ISO/IEC 15693-2.

Request flags 5 to 8 definition when inventory flag is NOT set

Bit Nb	Flag name	State	Description
Bit 5	Select_flag	0	Request shall be executed by any VICC according to the setting of Address_flag
		1	Request shall be executed only by VICC in selected state
Bit 6	Address_flag	0	Request is not addressed. UID field is not present. It shall be executed by any VICC.
		1	Request is addressed. UID field is present. It shall be executed only by the VICC whose UID matches the UID specified in the request.
Bit 7	Option_flag	0	Meaning is defined by the command description. It shall be set to 0 if not otherwise defined by the command.
		1	Meaning is defined by the command description.
Bit 8	RFU	0	Shall be set to 0.

Note: if the Select_flag is set to 1, the Address_flag shall be set to 0 and the UID field shall not be present in the request.

Request flags 5 to 8 definition when inventory flag is set

Bit Nb	Flag name	State	Description
Bit 5	AFI_flag	0	AFI field is not present
		1	AFI field is present
Bit 6	Nb_slots_flag	0	16 slots
		1	1 slot
Bit 7	Option_flag	0	Meaning is defined by the command description. It shall be set to 0 if not otherwise defined by the command.
		1	Meaning is defined by the command description.
Bit 8	RFU	0	Shall be set to 0.

3）Response flags

Response flags 1 to 8 definitions

Bit Nb	Flag name	State	Description
Bit 1	Error_flag	0	No error
		1	Error detected. Error code is in the "Error" field.
Bit 2	RFU		Shall be set to 0.
Bit 3	RFU		Shall be set to 0.
Bit 4	Extension_flag	0	No protocol format extension.
		1	Protocol format is extended. Reserved for future use.
Bit 5	RFU		Shall be set to 0.
Bit 6	RFU		Shall be set to 0.
Bit 7	RFU		Shall be set to 0.
Bit 8	RFU		Shall be set to 0.

4）Response error code

Response error code definition

Error code	Meaning
'01'	The command is not supported, i.e. the request code is not recognised.
'02'	The command is not recognised, for example: a format error occurred.
'03'	The option is not supported.
'0F'	Unknown error.
'10'	The specified block is not available (doesn't exist).
'11'	The specified block is already -locked and thus cannot be locked again
'12'	The specified block is locked and its content cannot be changed.
'13'	The specified block was not successfully programmed.
'14'	The specified block was not successfully locked.
'A0' – 'DF'	Custom command error codes
all others	RFU

Note: If the VICC does not support error codes listed in table 7, it shall answer with the error code '0F' (unknown error).

5) Password identifier

Key ID and default value

Password identifier	Password	Default(4Bytes)
01h	Read	00000000h
02h	Write	00000000h
04h	Privacy	00000000h
08h	Destroy	00000000h
10h	EAS	00000000h

4.2.2 Read and write protection permission setting and testing

- Inventory:

  Card search operation

  TransPort input: 5C 00

  Send: 00 05 00 5C 00 59

  Receive: 00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

  Card UID: 32 78 58 00 00 02 04 E0

  IC mfg code: 04

- Select:

  The request format (Flags) in the subsequent command specifies the VICC in the selected state to execute the command to reduce the size of the transmission packet.

  TransPort input: 7E 00 04 22 25 32 78 58 00 00 02 04 E0 (request format Flag, CMD, UID)

  Send: 00 10 00 7E 00 04 22 25 EA E8 D1 18 08 01 04 E0 4B

  Receive: 00 05 01 7E 00 7A (response format Flag)

- Get Random Number

  Get random number

  Get Random Number Request format

SOF	Flags	CMD	IC Mfg code	UID	CRC16	EOF
-	8bits	8bits	8bits	64bits	16bits	-
-	See section 4.2.1 Request Format for details.	0xB2		Optional, determined by Flags.	The module is automatically calculated, no need to add in the instruction.	-

  GET RANDOM NUMBER response when Error_flag set

SOF	Flags	Error code	CRC16	EOF
-	8 bits	8 bits	16 bits	-
	See section 4.2.1 Response Format for details.	For details, please refer to Chapter 4.2.1 Error Codes.	The module is automatically verified and does not return in the response.	

  GET RANDOM NUMBER response format when Error_flag NOT set

SOF	Flags	Random number	CRC16	EOF
-	8 bits	16 bits	16 bits	-
	See section 4.2.1 Response Format for details.		The module is automatically verified and does not return in the response.	

  Note: See the ICODE SLI-S datasheet Custom commands chapter for details, and other commands will not be listed one by one.

  TransPort input：7E 00 04 12 B2 04（request format Flag， CMD， IC mfg code）
  Send：00 09 00 7E 00 04 12 B2 04 D7
  Receive：00 07 01 7E 00 66 C4 DA

  Random Number：66 C4

- Set Read Password：

  Authentication card read key
  Read keyID：0x01
  Default Key：0x00000000
  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}
  Example： 0x00000000 XOR 0x66C466C4 = 0x66C466C4
  TransPort input：7E 00 04 12 B3 04 01 66 C4 66 C4
  Send：00 0E 00 7E 00 04 12 B3 04 01 66 C4 66 C4 D0
  Receive：00 05 01 7E 00 7A

- Set Write Password：

  Authentication card write key

  Write keyID：0x02

  Default Key：0x00000000

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  Example： 0x00000000 XOR 0x66C466C4 = 0x66C466C4

  TransPort input：7E 00 04 12 B3 04 02 66 C4 66 C4

  Send：00 0E 00 7E 00 04 12 B3 04 02 66 C4 66 C4 D3

  Receive：00 05 01 7E 00 7A

- Protect Page

  Set protection permissions

  Note: This command requires authentication of read and write keys

  Example

  0x09：Set protection permissions for page 0x09.

  0x10：To protect permissions, write 0x09 page requires authentication write key.

  TransPort input：7E 00 04 12 B6 04 09 10

  Send：00 0B 00 7E 00 04 12 B6 04 09 10 C8

  Receive：00 05 01 7E 00 7A

- Lock Page Protection Comdition

  Locked page protection status, the protection status cannot be changed after locking. After this state is set, it cannot be restored and can be omitted during testing.

  TransPort input：7E 00 04 12 B7 04 09

  Send：00 0A 00 7E 00 04 12 B7 04 09 D8

  Receive：00 05 01 7E 00 7A

- The card is powered off and the card is searched

- Inventory：

  Search Card operation

  TransPort input：5C 00

  Send：00 05 00 5C 00 59

  Receive：00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

- Read Blocks (page9, 36~39blocks)

  TransPort input：54 24 04

  Send：00 06 00 54 24 04 72

  Receive：00 14 01 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 41

- Write Blocks(page9, 36~39 blocks)

  TransPort input：55 24 04 44 44 44 44 33 33 33 33 22 22 22 22 11 11 11 11

  Send：00 16 00 55 24 04 44 44 44 44 33 33 33 33 22 22 22 22 11 11 11 11 63

Receive：00 04 01 AA AF

Writing the 0x09 page requires authentication of the write key. If the write key is not authenticated, the data write operation fails.

- Select：

  TransPort input：7E 00 04 22 25 32 78 58 00 00 02 04 E0

  Send：00 10 00 7E 00 04 22 25 32 78 58 00 00 02 04 E0 99

  Receive：00 05 01 7E 00 7A

- Get Random Number

  Get random number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 AC D6 02

  Random Number：AC D6

- Set Write Password：

  Authentication card write key

  Write KeyID：0x02

  Default Key：0x00000000

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 12 B3 04 02 AC D6 AC D6

  Send：00 0E 00 7E 00 04 12 B3 04 02 AC D6 AC D6 D3

  Receive：00 05 01 7E 00 7A

- Write Blocks(page9, 36~39 blocks)

  TransPort input：55 24 04 44 44 44 44 33 33 33 33 22 22 22 22 11 11 11 11

  Send：00 16 00 55 24 04 44 44 44 44 33 33 33 33 22 22 22 22 11 11 11 11 63

  Receive：00 04 01 55 50

  After the write key is authenticated, the write operation to page 0x09 is successful.

- Read Blocks (page9, 36~39 blocks)

  TransPort input：54 24 04

  Send：00 06 00 54 24 04 72

  Receive：00 14 01 54 44 44 44 44 33 33 33 33 22 22 22 22 11 11 11 11 41

  Verify that the read data is consistent with the written data.

- Get multiple block protection status

  Get protection status of multiple blocks

  TransPort input：7E 00 06 12 B8 04 00 28(Read the protection status of all blocks, which

takes slightly longer)

Send：00 0B 00 7E 00 06 12 B8 04 00 28 F5

Receive：00 2D 01 7E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 04 04 04 52

Only the write key protection set by the 36~39 blocks on page 0x09, please refer to the ICODE SLI-S Datasheet for detailed analysis.

4.2.3 Key modification locking test

- Inventory：

  Card search operation

  TransPort input：5C 00

  Send：00 05 00 5C 00 59

  Receive：00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

- Select：

  TransPort input：7E 00 04 22 25 32 78 58 00 00 02 04 E0

  Send：00 10 00 7E 00 04 22 25 32 78 58 00 00 02 04 E0 99

  Receive：00 05 01 7E 00 7A

- Get Random Number

  Get random number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 FC F8 7C

  Random Number：FC F8

- Set Read Password：

  Authentication card read key

  Read key ID：0x01

  Default Key：0x00000000

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 12 B3 04 01 FC F8 FC F8

  Send：00 0E 00 7E 00 04 12 B3 04 01 FC F8 FC F8 D0

  Receive：00 05 01 7E 00 7A

- Write Read Password：

  Set the card reading key

  Read key ID：0x01

  Key Data：4 bytes plaintext, example set to 0x11111111

  TransPort input：7E 00 04 12 B4 04 01 11 11 11 11

  Send：00 0E 00 7E 00 04 12 B4 04 01 11 11 11 11 D7

  Receive：00 05 01 7E 00 7A

Note: After modifying the card key, you need to re-obtain the random number and authenticate.

- Get Random Number

  Get random number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 5F 00 27

  Random Number：5F 00

- Set Read Password：

  Authentication card read key

  Read key ID：0x01

  Modify key：0x11111111

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  Example： 0x11111111 XOR 0x5F005F00 = 0x4E114E11

  TransPort input：7E 00 04 12 B3 04 01 4E 11 4E 11

  Send：00 0E 00 7E 00 04 12 B3 04 01 4E 11 4E 11 D0

  Receive：00 05 01 7E 00 7A (Success, indicating that the key modification is completed)

- Lock Read Key Test

- Get Random Number

  Get random number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 98 8A 6A

  Random Number：98 8A

- Set Read Password：

  Authentication card read key

  Read keyID：0x01

  Modify key：0x11111111

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 12 B3 04 01 89 9B 89 9B

  Send：00 0E 00 7E 00 04 12 B3 04 01 89 9B 89 9B D0

  Receive：00 05 01 7E 00 7A

- Lock Password

  Lock Card Read Key

  Read keyID：0x01

TransPort input：7E 00 04 12 B5 04 01
Send：00 0A 00 7E 00 04 12 B5 04 01 D2
Receive：00 05 01 7E 00 7A

- Write Read Password：
  Set the card reading key
  Write keyID：0x01
  Key data: 4 bytes plaintext, example set to 0x00000000
  TransPort input：7E 00 04 12 B4 04 01 00 00 00 00
  Send：00 0E 00 7E 00 04 12 B4 04 01 00 00 00 00 D7
  Receive：00 06 01 7E 01 0F 77（The key is locked, modifying the key fails, the response is correct）

The modified key test is completed, and the other key processes are the same, so they are not listed one by one.

4.2.4 Privacy Mode Test

- Inventory：
  Card search operation
  TransPort input：5C 00
  Send：00 05 00 5C 00 59
  Receive：00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

- Select：
  TransPort input：7E 00 04 22 25 32 78 58 00 00 02 04 E0
  Send：00 10 00 7E 00 04 22 25 32 78 58 00 00 02 04 E0 99
  Receive：00 05 01 7E 00 7A

- Get Random Number
  Get random number
  TransPort input：7E 00 04 12 B2 04
  Send：00 09 00 7E 00 04 12 B2 04 D7
  Receive：00 07 01 7E 00 78 7E 7E

  Random Number：78 7E
- Set Privacy Password
  KeyID：0x04
  Default Key：0x00000000
  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 12 B3 04 04 78 7E 78 7E
  Send：00 0E 00 7E 00 04 12 B3 04 04 78 7E 78 7E D5
  Receive：00 05 01 7E 00 7A

- Enable Privacy

  Enter privacy mode

  TransPort input：7E 00 04 12 BA 04

  Send：00 09 00 7E 00 04 12 BA 04 DF

  Receive：00 05 01 7E 00 7A

- The card is powered off and the card is searched again

  Card search operation

  TransPort input：5C 00

  Send：00 05 00 5C 00 59

  Receive：00 04 01 A3 A6（Failed, entered privacy mode）

- Set the module card reader type to ISO15693 mode

  TransPort input：70 02

  Send：00 05 00 70 02 77

  Receive：00 04 01 70 75

- Turn on the antenna

  TransPort input：11 01

  Send：00 05 00 11 01 15

  Receive：00 04 01 11 14

- Get Random Number

  Get a random number; note that the request Flags is set to 02

  TransPort input：7E 00 04 02 B2 04

  Send：00 09 00 7E 00 04 02 B2 04 C7

  Receive：00 07 01 7E 00 60 F1 E9

  Random Number：60 F1

- Set Privacy Password：

  Authentication card privacy key, note that Request Flags is set to 02。

  Read keyID：0x04。

  Default Key：0x00000000

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 02 B3 04 04 60 F1 60 F1

  Send：00 0E 00 7E 00 04 02 B3 04 04 60 F1 60 F1 C5

  Receive：00 05 01 7E 00 7A

- Inventory

  Card search operation

  TransPort input：5C 00

  Send：00 05 00 5C 00 59

Receive：00 0D 01 5C 00 EA E8 D1 18 08 01 04 E0 76（Success, exit privacy mode）

4.2.5 EAS setup and test

- Inventory：

  Card search operation

  TransPort input：5C 00

  Send：00 05 00 5C 00 59

  Receive：00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

- Select：

  TransPort input：7E 00 04 22 25 32 78 58 00 00 02 04 E0

  Send：00 10 00 7E 00 04 22 25 32 78 58 00 00 02 04 E0 99

  Receive：00 05 01 7E 00 7A

- Get Random Number

  Get random number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 FC E3 67

  Random Number：FC E3

- Set EAS Password：

  Authenticate EAS key

  KeyID：0x10

  Default Key：0x00000000

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 12 B3 04 10 FC E3 FC E3

  Send：00 0E 00 7E 00 04 12 B3 04 10 FC E3 FC E3 C1

  Receive：00 05 01 7E 00 7A

- Set EAS：

  Set EAS mode

  TransPort input：7E 00 04 12 A2 04

  Send：00 09 00 7E 00 04 12 A2 04 C7

  Receive：00 05 01 7E 00 7A

- Write EAS ID

  Set EAS ID to 0x22 11

  TransPort input：7E 00 04 12 A7 04 22 11

  Send：00 0B 00 7E 00 04 12 A7 04 22 11 F3

  Receive：00 05 01 7E 00 7A

- After the card is powered off, power on again

- Set the module card reader type to ISO15693 mode
  TransPort input：70 02
  Send：00 05 00 70 02 77
  Receive：00 04 01 70 75

- Turn on the antenna
  TransPort input：11 01
  Send：00 05 00 11 01 15
  Receive：00 04 01 11 14

- EAS Alarm：
  EAS alert, does not match EAS ID
  TransPort input：7E 00 04 02 A5 04
  Send：00 09 00 7E 00 04 02 A5 04 D0
  Receive：00 25 01 7E 00 2F B3 62 70 D5 A7 90 7F E8 B1 80 38 D2 81 49 76 82 DA 9A 86 6F AF 8B B0 F1 9C D1 12 A5 72 37 EF DA

- EAS Alarm：
  EAS alert, match 1 byte EAS ID, 0x22
  TransPort input：7E 00 06 42 A5 04 08 22
  Send：00 0B 00 7E 00 06 42 A5 04 08 22 BA
  Receive：00 25 01 7E 00 2F B3 62 70 D5 A7 90 7F E8 B1 80 38 D2 81 49 76 82 DA 9A 86 6F AF 8B B0 F1 9C D1 12 A5 72 37 EF DA

- EAS Alarm：
  EAS alert, matching 2-byte EAS ID, 0x2211
  TransPort input：7E 00 06 42 A5 04 10 22 11
  Send：00 0C 00 7E 00 06 42 A5 04 10 22 11 B4
  Receive：00 25 01 7E 00 2F B3 62 70 D5 A7 90 7F E8 B1 80 38 D2 81 49 76 82 DA 9A 86 6F AF 8B B0 F1 9C D1 12 A5 72 37 EF DA

- EAS Alarm：
  EAS alert, matching 2-byte wrong EAS ID, 0x1122
  TransPort input：7E 00 06 42 A5 04 10 11 22
  Send：00 0C 00 7E 00 06 42 A5 04 10 11 22 B4
  Receive：00 04 01 81 84(mistake)

- Cancel EAS
- Inventory：
  Card search operation
  TransPort input：5C 00
  Send：00 05 00 5C 00 59

Receive：00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

- Select：

  TransPort input：7E 00 04 22 25 32 78 58 00 00 02 04 E0

  Send：00 10 00 7E 00 04 22 25 32 78 58 00 00 02 04 E0 99

  Receive：00 05 01 7E 00 7A

- Get Random Number

  Get Random Number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 3F C0 87

  Random Number：3F C0

- Set EAS Password：

  Authenticate the EAS key

  KeyID：0x10

  Default Key：0x00000000

  Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

  TransPort input：7E 00 04 12 B3 04 10 3F C0 3F C0

  Send：00 0E 00 7E 00 04 12 B3 04 10 FC E3 FC E3 C1

  Receive：00 05 01 7E 00 7A

- Reset EAS

  Exit EAS mode

  TransPort input：7E 00 04 12 A3 04

  Send：00 09 00 7E 00 04 12 A3 04 C6

  Receive：00 05 01 7E 00 7A

- EAS Alarm：

  EAS alert, does not match EAS ID

  TransPort input：7E 00 04 02 A5 04

  Send：00 09 00 7E 00 04 02 A5 04 D0

  Receive：00 04 01 81 84(Failed, indicating that EAS mode has been exited)

4.2.6 INVENTORY READ

- Set the module card reader type to ISO15693 mode

  TransPort input：70 02

  Send：00 05 00 70 02 77

  Receive：00 04 01 70 75

- Turn on the antenna

  TransPort input：11 01

  Send：00 05 00 11 01 15

  Receive：00 04 01 11 14

- Inventory Read

  Read pages 0, 1, and 2, a total of 12 blocks. The more data read, the larger the timeout parameter should be.

  TransPort input：7E 00 06 36 B0 04 00 00 00 02

  Send：00 0D 00 7E 00 06 36 B0 04 00 00 00 02 F5

  Receive：00 38 01 7E 00 00 22 22 22 22 33 33 33 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 47(Page Protection status)

- Fast Inventory Read

  Read blocks 00~05, a total of 6 blocks

  TransPort input：7E 00 06 36 B1 04 00 00 00 02

  Send：00 0D 00 7E 00 06 36 B1 04 00 00 00 02 F4

  Receive：00 38 01 7E 00 00 22 22 22 22 33 33 33 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 47

4.2.7 Destroy Mode Operation

- Inventory：

  Card search operation

  TransPort input：5C 00

  Send：00 05 00 5C 00 59

  Receive：00 0D 01 5C 00 32 78 58 00 00 02 04 E0 A4

- Select：

  TransPort input：7E 00 04 22 25 32 78 58 00 00 02 04 E0

  Send：00 10 00 7E 00 04 22 25 32 78 58 00 00 02 04 E0 99

  Receive：00 05 01 7E 00 7A

- Get Random Number

  Get Random Number

  TransPort input：7E 00 04 12 B2 04

  Send：00 09 00 7E 00 04 12 B2 04 D7

  Receive：00 07 01 7E 00 D7 E2 4D

  Random Number：D7 E2

- Set Destroy Password：

  Authentication Destroy key

KeyID：0x08
Default Key：0x00000000
Key Data Processing：Password[31:0] XOR { Rand [15:0]，Rand [15:0]}

TransPort input：7E 00 04 12 B3 04 08 D7 E2 D7 E2
Send：00 0E 00 7E 00 04 12 B3 04 08 D7 E2 D7 E2 D9
Receive：00 05 01 7E 00 7A

- Destroy：

  Destroy tags. NOTE: This operation is irreversible.
  TransPort input：7E 00 04 12 B9 04
  Send：00 09 00 7E 00 04 12 B9 04 DC
  Receive：00 05 01 7E 00 7A

- Card search operation

  TransPort input：5C 00
  Send：00 05 00 5C 00 59
  Receive：00 04 01 A3 A6（failed, deactivated）