JMY600 Series IC Card Module

ST25TV02KC ST25TV512 Commands

Operation Guide

（Revision 1.00）

Beijing Jinmuyu Electronics Co., LTD

2022/9/16

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 the JMY600 series card reader module to operate ST25TV02KC/ST25TV512C and the basic card function design. You can quickly master the use of ST25TV02KC/ST25TV512C electronic tags 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

- Based on ISO/IEC 15693
- NFC Forum Type 5 tag certified by the NFC Forum
- Supports all ISO/IEC 15693 modulations, coding, subcarrier modes, and datarates up to 26 Kbit/s
- Single block reads and writes, multiple block reads
- Up to 2560 bits (320 bytes) of EEPROM
- Flexible user memory segmentation and access condition setting
- Multiple password protection mechanisms
- With anti-collision mechanism, support multi-card operation
- The data storage period is 60 years, can be rewritten 100K times, and read unlimited times
- Operating temperature: -25 to +85 ℃
- Working frequency: 13.56MHz

3 Memory organization

User memory is addressed as blocks (= pages) of 4 bytes, starting at address 0 and ending at address END_MEM. Value of END_MEM is 0Fh and 4Fh for ST25TV512C and ST25TV02KC devices respectively. The ST25TVxxxC user memory can be configured in single area (AREA1) or in dual area mode (AREA1 and AREA2) depending on the value of the END_A1 register at the start of a RF session.

When the value of END_A1 is equal to END_MEM, the ST25TVxxxC user memory is configured in single area mode defined as follows:

• AREA1 starts at address 00h. It is composed of (END_MEM+1) blocks. It can be read- or read/write protected by a dedicated 64-bit password. AREA1 is dedicated to user data.

When the value of END_A1 is lower than END_MEM, the ST25TVxxxC user memory is configured in dual area mode defined as follows:

• AREA1 starts at address 00h. It is composed of (END_A1+1) blocks. It can be read- or

readwrite-protected by a dedicated 32-bit password. AREA1 is dedicated to user data.

• AREA2 starts at address (END_A1+1). It is composed of (END_MEM-END_A1) blocks. It can be read- or readwrite-protected by a dedicated 32-bit password. AREA2 is dedicated to user data.

Block 00h belongs to AREA1, but can always be read regardless of the read-protection mode of AREA1. This block is dedicated to the CC file content defined by the NFC Forum Type 5 application. An application

User memory in single area mode

Block Address	Byte Address				Comment
	LSByte	-	-	MSByte	
00h	0000h	0001h	0002h	0003h	AREA1
01h	0004h	0005h	0006h	0007h	
02h	0008h	0009h	000Ah	000Bh	
:	:	:	:	:	
END_MEM	END_MEM*4+0	END_MEM*4+1	END_MEM*4+2	END_MEM*4+3	

User memory in dual area mode

Block Address	Byte Address				Comment
	LSByte	-	-	MSByte	
00h	0000h	0001h	0002h	0003h	AREA1
01h	0004h	0005h	0006h	0007h	
02h	0008h	0009h	000Ah	000Bh	
:	:	:	:	:	
END_A1	END_A1*4+0	END_A1*4+1	END_A1*4+2	END_A1*4+3	
END_A1+1	END_A1*4+4	END_A1*4+5	END_A1*4+6	END_A1*4+7	AREA2
:	:	:	:	:	
END_MEM	END_MEM*4+0	END_MEM*4+1	END_MEM*4+2	END_MEM*4+3	

4 Card Operation

4.1 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

Definition of Request_flags LSBs

Table 88. Definition of Request_flags LSBs

Bit	Flag	Decription
0	Subcarrier_flag(1)	0 : A single subcarrier is used by the VICC 1 : Two subcarriers are used by the VICC
1	Datarate_flag(1)	0 : Low data rate is used by the VICC 1 : High data rate used by the VICC
2	Inventory_flag	0 : Bits 4 to 7 are described by Table 89 1 : Bits 4 to 7 are described by Table 90
3	Protocol_extension_flag	0 : No protocol format extension 1 : Not supported (RFU)

1. *Subcarrier_flag and Datarate_flag refer to the VICC-to-VCD communication.*

Definition of Request_flags MSBs when Inventory_flag value is 0

Table 89. Definition of Request_flags MSBs when Inventory_flag value is 0

Bit	Flag	Decription
4	Select_flag(1)	0 : The command is processed according to the value of Address_flag 1 : UID field not present. The command is processed only by the VICC in SELECTED state(2)
5	Address_flag(1)	0 : UID field not present. command is processed by any VICC 1 : UID field present. command is processed only by the VICC whose UID matches the field value
6	Option_flag	0 : Option not activated 1 : Option activated
7	RFU_flag	0 : Unless otherwise specified 1 : Not supported (RFU)

1. *Select_flag=1 and Address_flag=1 is an invalid case, a request with such setting is ignored by the ST25TVxxxC device.*
2. *The SELECTED state is defined in section 6.2.8*

Definition of Request_flags MSBs when Inventory_flag value is 1

Table 90. Definition of Request_flags MSBs when Inventory_flag value is 1

Bit	Flag	Decription
4	AFI_flag	0 : AFI field is not present 1 : AFI field is present
5	Nb_slots_flag	0 : 16 slots mode 1 : 1 slot mode
6	Option_flag	0 : Option not activated 1 : Option activated
7	RFU_flag	0 : Unless otherwise specified 1 : Not supported (RFU)

3）Response format

Definition of Response_flags

Bit	Flag	Description
0	Error_flag	0 : No error 1 : Error detected. Error code present in the Data field
1	RFU	0 : Unless otherwise specified 1 : Not supported (RFU)
2		
3		
4		
5		
6		
7		

4）Response and error codes

Definition of response error codes

Error code	Description
01h	Invalid IC Mfg code value
02h	Invalid request format
03h	Invalid Request_flags value
0fh	Error with no information given
10h	Requested data not available
11h	Requested data is already locked and thus cannot be locked again
12h	Requested data is locked and its content cannot be changed
13h	Programmation of requested data failed
14h	Lock of requested data failed
15h	Requested data is protected in read

5) List of password registers

List of password registers

Password	Password_id	Password_data size
PWD_CFG	00h	4 bytes
PWD_A1	01h	4 bytes if END_A1 < END_MEM
		8 bytes if END_A1 = END_MEM
PWD_A2	02h	4 bytes if END_A1 < END_MEM
		Invalid request if END_A1 = END_MEM
PWD_UNTR	03h	4 bytes

4.2 Read and write test - password protection is not turned on

- Inventory

  Card search operation

  TransPort input: 5C 00

  Send: 00 05 00 5C 00 59

  Receive: 00 0D 01 5C 00 85 0C 2D 37 02 08 02 E0 2B

  Card UID: 85 0C 2D 37 02 08 02 E0

- 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 85 0C 2D 37 02 08 02 E0（request format Flag, CMD, UID）

  Send: 00 10 00 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0 16

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

- Read Single Block (0x01)

  TransPort input: 7E 00 04 12 20 01

  Send: 00 09 00 7E 00 04 12 20 01 40

  Receive: 00 09 01 7E 00 11 22 33 45 33

- Write Single Block (0x01)

  TransPort input: 7E 00 04 12 21 01 00 00 00 00

  Send: 00 0D 00 7E 00 04 12 21 01 00 00 00 00 45

  Receive: 00 05 01 7E 00 7A

- Read Single Block (0x01)

  TransPort input: 7E 00 04 12 20 01

  Send: 00 09 00 7E 00 04 12 20 01 40

  Receive: 00 09 01 7E 00 00 00 00 00 76

4.3 Enable read and write protection (single area)

Note: In single area mode, the read/write authentication key is 64bit.

- Inventory

  Card search operation

  TransPort input: 5C 00

  Send: 00 05 00 5C 00 59

Receive: 00 0D 01 5C 00 85 0C 2D 37 02 08 02 E0 2B

- Select

  TransPort input: 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0
  Send: 00 10 00 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0 16
  Receive: 00 05 01 7E 00 7A

- Get Random Number

  Get random number
  TransPort input: 7E 00 04 12 B4 02
  Send: 00 09 00 7E 00 04 12 B4 02 D7
  Receive: 00 07 01 7E 00 62 6E 74

  Random Number: 62 6E

- Authentication PWD_CFG (ID = 00h)

  Authentication configuration area key, the default key is 00000000h.
  Key data processing: Password[31:0] XOR { Rand [15:0]，Rand [15:0]}
  Example: 0x00000000 XOR 0x626E626E = 0x626E626E
  TransPort input: 7E 00 04 12 B3 02 00 62 6E 62 6E
  Send: 00 0E 00 7E 00 04 12 B3 02 00 62 6E 62 6E D7
  Receive: 00 05 01 7E 00 7A

- Enable read and write permissions

  Write system configuration registers: RW_PROTECTION_A1（FID:0x00, PID:0x00）.
  The write value is: 02h.
  Read allowed if AREA1 security session is open
  Write allowed if AREA1 security session is open
  TransPort input: 7E 00 04 12 A1 02 00 00 02
  Send: 00 0C 00 7E 00 04 12 A1 02 00 00 02 C5
  Receive: 00 05 01 7E 00 7A

- Switch the antenna and activate the permission setting

  Turn off the antenna
  TransPort input: 11 00
  Send: 00 05 00 11 00 14
  Receive: 00 04 01 11 14

  Open the antenna
  TransPort input: 11 01
  Send: 00 05 00 11 01 15
  Receive: 00 04 01 11 14

- Inventory

  Card search operation

  TransPort input: 5C 00

  Send: 00 05 00 5C 00 59

  Receive: 00 0D 01 5C 00 85 0C 2D 37 02 08 02 E0 2B

- Select

  TransPort input: 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0

  Send: 00 10 00 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0 16

  Receive: 00 05 01 7E 00 7A

- Read Single Block (0x01)

  TransPort input: 7E 00 04 12 20 01

  Send: 00 09 00 7E 00 04 12 20 01 40

  Receive: 00 06 01 7E 01 15 6D (Failed to read until key is authenticated)

- Write Single Block (0x01)

  TransPort input: 7E 00 04 12 21 01 11 22 33 44

  Send: 00 0D 00 7E 00 04 12 21 01 11 22 33 44 01

  Receive: 00 06 01 7E 01 12 6A (Failed to read until key is authenticated)

- Get Random Number

  Get random number

  TransPort input: 7E 00 04 12 B4 02

  Send: 00 09 00 7E 00 04 12 B4 02 D7

  Receive: 00 07 01 7E 00 C0 BC 04

  Random Number: C0 BC

- Authentication PWD_A1 (ID = 01h)

  Authentication A1 area key, the default key is 0000000000000000h.

  Key data processing: Password [63:0] XOR {Rand [15:0], Rand [15:0], Rand [15:0], Rand [15:0]}

  Example:0000000000000000h xor C0BCC0BCC0BCC0BCh = C0BCC0BCC0BCC0BCh

  TransPort input: 7E 00 04 12 B3 02 01 C0 BC C0 BC C0 BC C0 BC

  Send: 00 12 00 7E 00 04 12 B3 02 01 C0 BC C0 BC C0 BC C0 BC CA

  Receive: 00 05 01 7E 00 7A

- Read Single Block (0x01)

  TransPort input: 7E 00 04 12 20 01

  Send: 00 09 00 7E 00 04 12 20 01 40

  Receive: 00 09 01 7E 00 00 00 00 00 76

- Write Single Block (0x01)
  TransPort input: 7E 00 04 12 21 01 11 22 33 44
  Send: 00 0D 00 7E 00 04 12 21 01 11 22 33 44 01
  Receive: 00 05 01 7E 00 7A

- Read Single Block (0x01)
  TransPort input: 7E 00 04 12 20 01
  Send: 00 09 00 7E 00 04 12 20 01 40
  Receive: 00 09 01 7E 00 11 22 33 44 32

4.4 Modify PWD_A1

- Inventory
  Card search operation
  TransPort input: 5C 00
  Send: 00 05 00 5C 00 59
  Receive: 00 0D 01 5C 00 85 0C 2D 37 02 08 02 E0 2B

- Select
  TransPort input: 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0
  Send: 00 10 00 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0 16
  Receive: 00 05 01 7E 00 7A

- Get Random Number
  Get random number
  TransPort input: 7E 00 04 12 B4 02
  Send: 00 09 00 7E 00 04 12 B4 02 D7
  Receive: 00 07 01 7E 00 42 3C 06

  Random Number: 42 3C

- Authentication PWD_A1 (ID = 01h)
  TransPort input: 7E 00 04 12 B3 02 01 42 3C 42 3C 42 3C 42 3C
  Send: 00 12 00 7E 00 04 12 B3 02 01 42 3C 42 3C 42 3C 42 3C CA
  Receive: 00 05 01 7E 00 7A

- Get Random Number
  Get random number
  TransPort input: 7E 00 04 12 B4 02
  Send: 00 09 00 7E 00 04 12 B4 02 D7
  Receive: 00 07 01 7E 00 90 40 A8

  Random Number: 90 40

- WRITE PASSWORD - PWD_A1 (ID = 01h)
  Set key: 1122334411223344h
  Random number: 9040904090409040h
  Key encryption: 8162A3048162A304h
  TransPort input: 7E 00 04 12 B1 02 01 81 62 A3 04 81 62 A3 04
  Send: 00 12 00 7E 00 04 12 B1 02 01 81 62 A3 04 81 62 A3 04 C8
  Receive: 00 05 01 7E 00 7A

- Switch the antenna on and off, and actively lose the permission
  Turn off the antenna
  TransPort input: 11 00
  Send: 00 05 00 11 00 14
  Receive: 00 04 01 11 14

  Open the antenna
  TransPort input: 11 01
  Send: 00 05 00 11 01 15
  Receive: 00 04 01 11 14

- Inventory
  Card search operation
  TransPort input: 5C 00
  Send: 00 05 00 5C 00 59
  Receive: 00 0D 01 5C 00 85 0C 2D 37 02 08 02 E0 2B

- Select
  TransPort input: 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0
  Send: 00 10 00 7E 00 04 22 25 85 0C 2D 37 02 08 02 E0 16
  Receive: 00 05 01 7E 00 7A

- Get Random Number
  Get random number
  TransPort input: 7E 00 04 12 B4 02
  Send: 00 09 00 7E 00 04 12 B4 02 D7
  Receive: 00 07 01 7E 00 13 F6 9D

  Random Number: 13 F6

- Authentication PWD_A1 (ID = 01h):
  Authentication A1 area key
  key: 1122334411223344h。
  Random number: 13F613F613F613F6h
  After encryption: 02D420B202D420B2h
  TransPort input: 7E 00 04 12 B3 02 01 02 D4 20 B2 02 D4 20 B2

Send: 00 12 00 7E 00 04 12 B3 02 01 02 D4 20 B2 02 D4 20 B2 CA
Receive: 00 05 01 7E 00 7A

- Read Single Block (0x01)
  TransPort input: 7E 00 04 12 20 01
  Send: 00 09 00 7E 00 04 12 20 01 40
  Receive: 00 09 01 7E 00 11 22 33 44 32

- Write Single Block (0x01)
  TransPort input: 7E 00 04 12 21 01 00 00 00 00
  Send: 00 0D 00 7E 00 04 12 21 01 00 00 00 00 45
  Receive: 00 05 01 7E 00 7A

- Read Single Block (0x01)
  TransPort input: 7E 00 04 12 20 01
  Send: 00 09 00 7E 00 04 12 20 01 40
  Receive: 00 09 01 7E 00 00 00 00 00 76

- Get Random Number
  Get random number
  TransPort input: 7E 00 04 12 B4 02
  Send: 00 09 00 7E 00 04 12 B4 02 D7
  Receive: 00 07 01 7E 00 90 40 A8

  Random Number: 90 40

- WRITE PASSWORD - PWD_A1 (ID = 01h)
  Set key: 0000000000000000h
  Random number: 137E137E137E137Eh
  Key encryption: 137E137E137E137Eh
  TransPort input: 7E 00 04 12 B1 02 01 13 7E 13 7E 13 7E 13 7E
  Send: 00 12 00 7E 00 04 12 B1 02 01 13 7E 13 7E 13 7E 13 7E C8
  Receive: 00 05 01 7E 00 7A