SL-RFM-P001 Series card reader
Product manual

Version / Revision	Modify pages	Modification record	Modified by	Reviewed by	Approval	Date
0.0		Initial version				

目录

Abbreviation：

ED	Electronic Deposit
EP	Electronic Purse
MAC	Message Authentication Code
POS	Point of Service
PSAM	Purchase Secure Access Module
TAC	Transaction Authorization Crypogram
FCI	File Control Information
AID	Application Identifier

1. Product introduction

SL-RFM-P001 reader is a serial reader. Users must send commands to it through the host (including MCU, arm, DSP and PC) to control its reading and writing. This application guide will focus on the serial communication protocol and commands between the SL-RFM-P001 and the host.
SL-RFM-P001 module is a kind of suitable for reading and writing in accordance with ISO/IEC14443 TypeA/TypeB standard non-contact CPU card module, at the same time reserved in accordance with ISO7816 standard ESAM module card, in addition to support reading and writing M1 card. This module has the characteristics of simple and easy to use, high reliability, small volume, users do not need to understand the complex ISO/IEC14443 protocol and complex ISO7816 protocol and complex operation card function, SL-RFM-P001 has related operation into a few simple instructions, Users only need to send a few simple operations through the serial port to complete the operation of the card.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution:
Changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement Caution: This Transmitter must be installed to provide a separation distance of at least 20 cm from all persons.

FCC Statement:
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

IC statement:
This device complies with Industry Canada licence-exempt RSS standard(s).
Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.
:
Cet émetteur doit être installé pour fournir une distance de séparation d'au moins 20 cm de toute personne.

1.1. Product principle block diagram

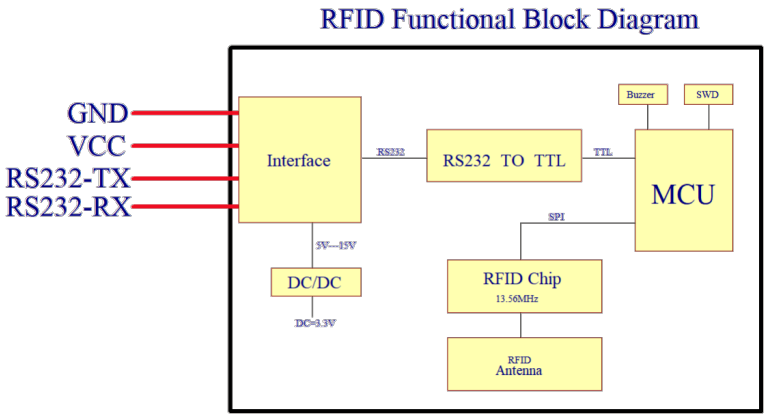

Fig. 1 Schematic diagram

1.2. Picture of real products

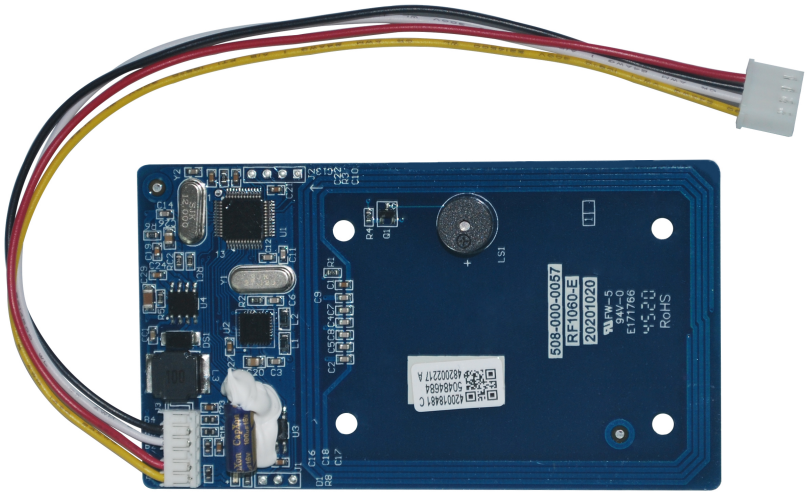

Fig. 2 Product picture

1.3. Outline dimension drawing

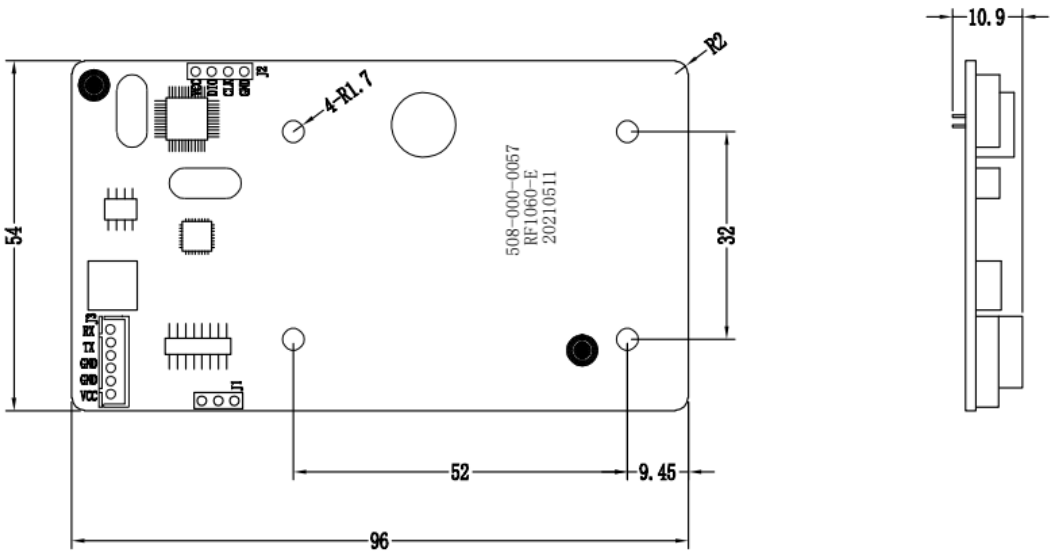

Fig. 3 Dimension drawing

1.4. Technical parameters

Card reading distance	0----50mm
Interface	RS232 interface, communication baud rate 57600bps-N-8-1 (baud rate 57600, 8 data bits, no parity bit, 1 stop bit).
Supported card types	Contactless: contactless card conforming to ISO/IEC14443 TypeA/TypeB, including CPU card, M1 card, contact: ESA module conforming to ISO7816 standard is reserved.
Maximum operating current	110mA（5V）
physical characteristics	Size: 96mm*54mm (locating hole r=1.7mm)
Environmental parameters	Operating ambient temperature：-20℃～55℃ Storage temperature：-30℃～75℃ Relative humidity：5%～95%
Pin description	 From left to right: 1、VCC（+5V） 2、GND 3、GND 4、TXD 5、RXD 6、Standby

Table 1 Technical parameters

2. Protocol introduction

2.1. Physical layer

The read-write module adopts the external power supply mode, with the voltage of 5V---15V. The communication interface is asynchronous full duplex communication, and the default baud rate is 57600. The data consists of one start bit, eight data bits and one stop bit, and there is no check bit.

2.2. Communication packet definition

The communication data package includes command data package and response data package. See Table 2 for the specific content, length and meaning.

Serial number	Content	Length (bytes)	Explain
1	Data frame header(STX)	1	Constant:0x02
2	（Data_len） Data cell length	2	The length of the data part of the data unit to be transmitted, with the high byte in front and the low byte in the back, expressed in hexadecimal. For example: 0x0010 indicates that the data part has 16 bytes.
3	The unit of data to be transmitted （Data）	Indeterminate	Data unit length is determined by data_ Len definition: the first two bytes of this data unit are command code (the terminal sends commands to the read-write module) or status (the read-write module returns data to the terminal), followed by other parameters.
4	Inspection value （LRC）	1	Data Indicates the xor value of each byte of Data.
5	End of data frame（ETX）	1	Constant:0x03

Table 2 Meaning of data communication package items

Note: the total length of the data packet is: Data_ Len+5 bytes. The maximum length of the packet cannot exceed 255 bytes. APDU instruction (including command header, which cannot exceed 250 bytes).

2.3. Protocol description

The module and terminal equipment are connected through data lines, and the communication between the module and the terminal shall comply with the provisions of the communication protocol regardless of the sending and receiving.

The terminal first sends a command data packet to the read-write module through the communication interface, and then waits for the response data packet from the read-write module.

After correctly receiving the command data packet sent by the terminal, the read-write module parses the command. If it is not necessary to operate the card, it processes the command and responds to the terminal response data; If

you need to operate the card, you can communicate with the card, get the response data of the card, and send the response data to the terminal.

If the terminal fails to receive the correct response packet from the read / write module within the specified maximum time, the terminal will end this data communication and prompt an error message.

If the read-write module does not receive the card response data within the specified maximum time, the read-write module shall return the card operation timeout response to the terminal.

The default maximum allowable timeout of each command sent by the terminal to the read-write module is set to 0.5 s, and the maximum timeout of each command for card operation by the read-write module shall be less than 0.5 s.

2.4. Data unit format

2.4.1. Command cell format

The format of command unit is shown in Table 3 below.

Note: the protocol header, length, checksum and protocol tail shall be added to all command sending and receiving. For the convenience of description, the protocol header, data length, checksum and protocol tail will not be mentioned in the subsequent chapters.

Project	Length	Explain
Frame header	1 byte	0x02
Data length	2 byte	0xXX 0xXX
CommandH	1 byte	Command category
CommandL	1 byte	Command code
Parameter	Indefinite length	Command parameters
Checksum	1 byte	0xXX
End of frame	1 byte	0x03

表 3 命令单元格式

Table 3 Command unit format

2.4.2. Format of response unit

See Table 4 below when responding to cells.

Project	Length	Explain
Frame header	1 byte	0x02
Data length	2 byte	0xXX 0xXX
StatusH	1 byte	Status code high byte
StatusL	1 byte	Status code low byte
Data	Indefinite length	Response data
Checksum	1 byte	0xXX
End of frame	1 byte	0x03

Table 4 Format of response unit

3. Module management operation instructions

3.1. Buzzer control

Controls the buzzer (external) single tone delay time and number of calls (low level buzzes).

Command data unit

Identification	Content	Explain
CommandH	31H	Function command category
CommandL	13H	Buzzer control command code
DelayTime	0000H~FFFFH （2 byte）	Buzzer sounding time (unit: ms)
Times	01H~FFH （1 byte）	Number of beeps

Table 5 Definition of buzzer control command data unit

Note: DelayTime is the single buzzer duration, and Times is the number of buzzers. The time and number of determined according to actual needs, but should not be too much. The terminal sends this command to the reader only once. The reader controls the buzzer based on this command.

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct

Table 6 Definition of buzzer control response data unit

3.2. Turn on RF

Open the RF field of the module to supply power to the RF cards within the RF field.

Command data unit

Identification	Content	Explain
CommandH	31H	Function command category
CommandL	90H	Turn on RF

Table 7 Definition of open RF command data unit

Reply data unit

identification	Content	Explain
Status	00H，00H	Command execution is correct

Table 8 Definition of open RF command response data unit

3.3. Turn off RF

Command data unit

Identification	Content	Explain
CommandH	31H	Function command category
CommandL	91H	Turn off RF

Table 9 Definition of closing RF command data unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct

Table 10 Definition of closing RF command response data unit

4. Card operation instructions

4.1. Contact card power on

Power on the card and receive the data of the response

Command data unit

Identification	Content	Explain
CommandH	32H	Card operation command code
CommandL	22H	Card power on command code
DelayTime	2 byte	Waiting time for card insertion (ESAM card does not process this parameter) 0: no need to wait and return directly without card Non 0: judge whether the card is inserted in place within the delaytime. (unit: ms)
CardNo	1 byte	Card No. (User card: 00H ~ 0FH; PSAM card: 10H~1FH)

Table 11 Definition of card power on command data unit

Reply data unit

Identification	Content		Explain
Status	00H	00H	Card powered on successfully
	10H	01H	Contact with user card is not supported
		02H	Contact user card not inserted in place
		05H	Contact user card power on failure
	20H	01H	PSAM card not supported
		05H	Power on failure of PSAM card
PTL	0		T=0
	1		T=1

ATR Data	Indefinite length	Protocol and historical characters returned from the card reset response (only available when the card is powered on successfully)

Table 12 Definition of card power on response data unit

Note: PCD200 only supports ESAM cards, not contact user cards. 10H corresponds to ESAM inside the module.

4.2. Contact card power off

Power down the touch card.

Command data unit

Identification	Content	Explain
CommandH	32H	Card operation command code
CommandL	23H	Card power down command code
CardNo	1 byte	Card No. (User card: 00H ~ 0FH; PSAM card: 10H~1FH)

Table 13 Definition of card power down command data unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	10H，01H	Contact with user card is not supported
	20H，01H	PSAM card not supported

Table 14 Definition of off card power response data unit

Note: this command is used for contact cards

4.3. Activate contactless card

The reader / writer is required to search whether the card enters the sensing area within the transfer time, and activate the card entering the sensing area.

Command data unit

Identification	Content	Explain
CommandH	32H	Card operation command code
CommandL	24H	Activate contactless card command code
DelayTime	2 byte	Wait for the card to enter the sensing time. The high order is in the front and the low order is in the back. When it is 0, the direct return fails when there is no card in the sensing area; When it is 0xFFFF, keep looking for the card until the card enters the sensing area; Other values: always judge whether the card enters the sensing area within the delaytime. (unit: ms)

Table 15 Definition of command data unit for activating contactless card

Reply data unit

Identification	Content		Explain
Status	00H	00H	Activation succeeded
	30H	01H	Contactless user card is not supported
	30H	05H	Contactless user card activation failed
	30H	06H	Timeout waiting for the card to enter the sensing area
	30H	09H	There are multiple cards in the sensing area
Type	0AH		Type A card
	1AH		M1 card
	0BH		Type B card
UIDLen	1 byte		Card serial number length
Card UID	UIDLen byte		Card serial number (returned only after successful activation)
ATRLen	1 byte		ATR data length
ATR Data	Indefinite length		Card reset response protocol and historical characters (returned only after activation is successful)

Table 16 Definition of active contactless card response data unit

4.4. Application layer transport command

After the transmission communication link is completed, the terminal and the reader / writer begin to transmit the APDU commands of the application layer.

Command data unit

Identification	Content	Explain
CommandH	32H	Card operation command code
CommandL	26H	Operation card data command code
CardNo	1 byte	Card No. (contactless card: FFH, contact user card: 00H～0FH，ESAM：10H～1FH)
C-APDU	Indefinite length	Command application protocol data unit. (according to ISO/IEC 7816 specification format)

Table 17 Definition of application layer command transmission command data unit

Reply data unit

Identification	Content		Explain
Status	00H	00H	Card returns data normally
	10H	01H	Contact with user card is not supported
		02H	接触用户卡未插到位 Contact user card not inserted in place
		04H	Contact user card is not powered on
		06H	There is no response to the user card data contacted by the operation

		07H	An error occurred when the operation touched the user card data
	20H	01H	PSAM card not supported
		04H	PSAM card is not powered on
		06H	No response to PSAM card data operation
		07H	Error operating PSAM card data
	30H	01H	Contactless user card is not supported
		05H	Contactless user card activation failed
		07H	Error occurred while operating contactless user card data
R-APDU	Indefinite length		Response application protocol data unit (according to ISO/IEC 7816 specification format) or error code

Table 18 Definition of application layer command transmission response data unit

5. M1 card operation

5.1. Load key

This command is mainly used during initialization. The key is stored in the module. Sectors 0-31 are supported.

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation
CommandL	00H	Load key instruction
Sector	1 byte	Sector code
KeyType	1 byte	（1 byte，KEYA：60H，KEYB：61H） Key type（1 byte，KEYA：60H，KEYB：61H）
Key	6 byte	Key content, corresponding to KEYA or KEYB

Table 19 Definition of loading key order unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	C0H，01H	Load unsuccessful

Table 20 Definition of loading key order response unit

5.2. Authentication

The M1 card can be directly authenticated before reading and writing.

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation

CommandL	02H	Certification directive
BKeyNo	1 byte	Specify the two keys used for authentication,KEYA or KEYB. 0x60 indicates to use KEYA, 0x61 indicates to use KEYB
bBlock	1 byte	Indicates the block number used
Key	6 byte	Key content, corresponding to KEYA or KEYB
UID	4 byte	It can be left blank. If it is blank, the module will search for the card again

Table 21 Definition of authentication command unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	00H，F5H	Parameter error
	C0H，01H	Authentication error
	C0H，FFH	Other errors

Table 22 Definition of authentication command response unit

5.3. Read block

After authentication, data can be read, and the read data is fixed to 16 bytes.

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation
CommandL	03H	Read block data instruction
bBlock	1 byte	Block number to read

Table 23 Definition of read block data command unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	C0H，01H	Read error
Dat	16 byte	Read only 16 bytes at a time

Table 24 Definition of read block data command response unit

5.4. Write block

After authentication, block data can be written, and the written data is fixed to 16 bytes.

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation
CommandL	04H	Write block data instruction
bBlock	1 byte	Block number to write
Dat	16 byte	Only 16 bytes can be written at a time

Table 25 Write block data command unit definition

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	C0H，01H	write error

Table 26 Definition of write block data command response unit

5.5. Read value

Read out the value. Refer to M1 card description. (special format shall be established for M1 card)

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation
CommandL	06H	Add value operation instruction
bBlock	1 byte	Block number to write

Table 27 Definition of read value operation command unit

Reply data unit

标识 Identification	Content	Explain
Status	00H，00H	Command execution is correct
	C0H，01H	Read failed

Table 28 Definition of read value operation command response unit

5.6. Add value

Add a value to the original value to get a new value, which is stored in the buffer. This operation requires a special card format. Please refer to the description of M1 card. (special format shall be established for M1 card).

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation
CommandL	07H	Add value operation instruction
bBlock	1 byte	Block number to write
bValue	4 byte	For the written value, the low order byte is in front, and the negative number is stored in the form of complement.

Table 29 Definition of value adding operation command unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	C0H，01H	Write failed

Table 30 Definition of adding value operation command response unit

5.7. Impairment

Subtract a value from the original value to get a new value, which is stored in the buffer. This operation requires a special card format. Please refer to the description of M1 card. (special format shall be established for M1 card).

Command data unit

Identification	Content	Explain
CommandH	C2H	M1 card operation
CommandL	08H	Impairment instruction
bBlock	1 byte	Block number to write
bValue	4 byte	For the written value, the low order byte is in front, and the negative number is stored in the form of complement.

Table 31 Definition of devaluation operation command unit

Reply data unit

Identification	Content	Explain
Status	00H，00H	Command execution is correct
	C0H，01H	Write failed

Table 32 Definition of devaluation operation command response unit

6. Card operation steps

For opening and closing the antenna and operating the buzzer, it can be operated at any time. It is not related to the following steps.

The recommended process here is: open antenna - activate card - authentication card - read / write card - close antenna - buzzer prompt.

6.1. M1 card operation steps

1. Activate, using command: 32 24
2. Activate, using command: 32 24
3. Authentication, using command: C2 02
4. Read block, using command: C2 03
5. Write block, using command: C2 04
6. Value operation, using command: C2 06; C2 07； C2 08
7. If you want to operate the data of different blocks, you need to perform step 2 first. After the card is authenticated, you can read, write and value the data.
8. If the card leaves the card reading area during the process, you need to perform step 1 first.

6.2. Non contact CPU card operation steps

1. Activate, using command: 32 24

2. Application data operation, using command: 32 26
3. If the card leaves the card reading area during the process, you need to perform step 1 first.

6.3. ESAM (PSAM) module operation steps

1. Activate, using command: 32 22
2. Application data operation, using command: 32 26
3. If the card leaves the card reading area during the process, you need to perform step 1 first.

7. After service

7.1. Warranty conditions

When the product leaves the factory, the user completely abides by the storage, installation and use rules specified in this instruction.

After the product leaves the factory, due to transportation reasons, the user found that the product or supporting parts were damaged during the unpacking inspection.

7.2. Guarantee time

The product quality is guaranteed for 12 months from the date of delivery.

7.3. Warranty method

During the warranty period, the manufacturer is responsible for free replacement or repair.

Beyond the warranty period, the user shall negotiate with the manufacturer to replace or repair in a paid way.

This manual is subject to change without notice.

If the contents of this manual do not conform to the real object, please refer to the real object.

FCC COMPLIANCE STATEMENT:
This device complies with part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can

radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.
Increase the separation between the equipment and receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

Warning: Changes or modifications to this unit not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

OEM Integration Guideline

Integration instructions for host product manufacturers according to KDB 996369 D03 OEM Manual v01

2.2 LIST OF APPLICABLE FCC RULES:
Compliance with § 15.225 regulation

2.3 SPECIFIC OPERATIONAL USE CONDITIONS:
This module is typically used in industrial, household and general office / ITE and audio & video, EV charging system end-products. The product must not be co-located or operating in conjunction with any other antenna or transmitters.

2.4 LIMIT MODULE PROCEDURES:
The module compliance with FCC requirements based on Limit module approval procedures as is no RF shielding for the radio module in place. The module Grantee is required and responsible to review and approve the use of the module in every new Host integration which will require testing and the filing of a Class 2 Permissive Change with the FCC.

2.5 TRACE ANTENNA DESIGNS:
The module is designed with the fixed PCB print antenna, any changes or modifications by the OEM integrator will require additional testing and evaluation.

2.6 RF EXPOSURE CONSIDERATIONS:
The module has been evaluated and shown compliant with the FCC RF Exposure limits under portable exposure conditions. OEM integrator shall equipped the antenna to compliance with antenna requirement part 15.203& 15.204 and must not be co-located or operating in conjunction with any other antenna or transmitters.

2.7 ANTENNAS:
The antenna of the module is designed as printed on the PCBA board and the maximum gain is 0dBi. Modifications to the antenna design are not permitted. If such changes are made he module is to be deemed as NOT certified.

2.8 LABEL AND COMPLIANCE INFORMATION:
The final end product integrating this module must be labelled in a visible area with the either
"Contains FCC ID: 2A7AM-RFM001" or "Contains Transmitter Module FCC ID: 2A7AM-RFM001". If the size of the end product is bigger than 8x10cm, then additional FCC part 15.19 statement is required to be available in the users' manual: "This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation."

2.9 INFORMATION ON TEST MODES AND ADDITIONAL TESTING REQUIREMENTS:

Data transfer module demo board can control the EUT work in RF test mode at specified conditions.

This radio module must not be installed to co-locate and operate simultaneously with other radios in the host system except in accordance with FCC multi-transmitter product procedures. Additional testing and equipment authorization may be required operate simultaneously with other radio. The module Grantee is required and responsible to review and approve the use of the module in every new Host integration which will require testing and the filing of a Class 2 Permissive Change with the FCC.

2.10 ADDITIONAL TESTING, PART 15 SUBPART B DISCLAIMER:

The host product manufacturer is responsible for compliance with any other FCC rules that apply to the host device not covered by the modular transmitter grant.

The final host product still requires Part 15 Subpart B compliance testing with the modular transmitter installed (regardsless of the modules Part 15 Subpart C certification).

General Statements

The module is intended only for OEM integrators.

The OEM integrator is responsible for ensuring that the end-user has no manual instruction to remove or install module.