FUDAN MICROELECTRONICS

复旦微电子

FM11RF32

32KBits Contactless IC Card Chip

Functional Specification

May. 2008

Content

1. Features

- **Contactless communications RF interface**
  - Contactless transmission of data and supply (no battery needed)
  - Operating distance: up to 100mm (depending on antenna geometry)
  - Operating frequency: 13.56MHz
  - Fast communication baud rate: 106Kbit/s
  - Half duplex communication protocol using handshake
  - Compatible: with ISO/IEC 14443-A
  - Encryption algorithm compatible with M1 standard
  - Typical Ticking Transaction: ＜100ms
- **EEPROM**
  - 4096 x 8bit EEPROM
  - High security level data communication
  - Organized in security separated 64 sectors supporting multi-application .
- **High security**
  - Mutual three pass authentication
  - Each sector has its own two secret keys for systems using key hierarchies.
  - Assess conditions for each block defined by user
- **Arithmetic capability: increase and decrease.**
- **High reliability**
  - Endurance: 100,000 cycle
  - Data Retention: 10 Years

2. Product Overview

2.1. Introduction

FM1RF32 is the contactless IC card chip development by Shanghai FM Co., Ltd. The chip has 4K x 8bits EEPROM organization; the maximum communication range between the reader antenna and contactless card is approximately 10cm. Data is exchanged half duplex at a 106-kbit/s rate.

The FM11RF32 is a true multi-application smart card with the functionality of a processor card realized with hardware logic, and also has a very high security performance with the encryption and communication circuit, so FM11RF32 can be especially tailored to meet the requirements of a payment card which can be used for ticketing systems in public transport and comparable applications.

The Contactless smart card contains three components: FM11RF32 chip、antenna and the card base with PVC (or PET) material. No battery is needed. When the chip is positioned in proximity of the coupling device antenna, the high speed RF communication interface allows transmitting data with 106 Kbit/s.

2.2. Block Diagram

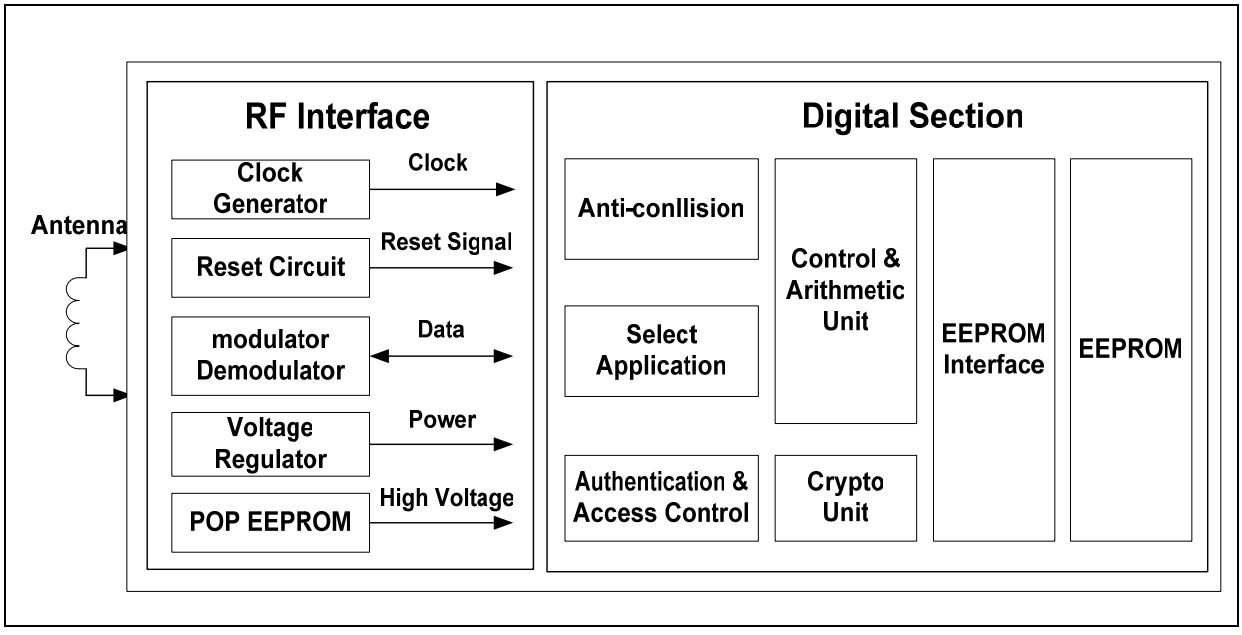

Figure 2-1 FM11RF32 Block Diagram

2.3. Function Description

2.3.1. Transaction sequence

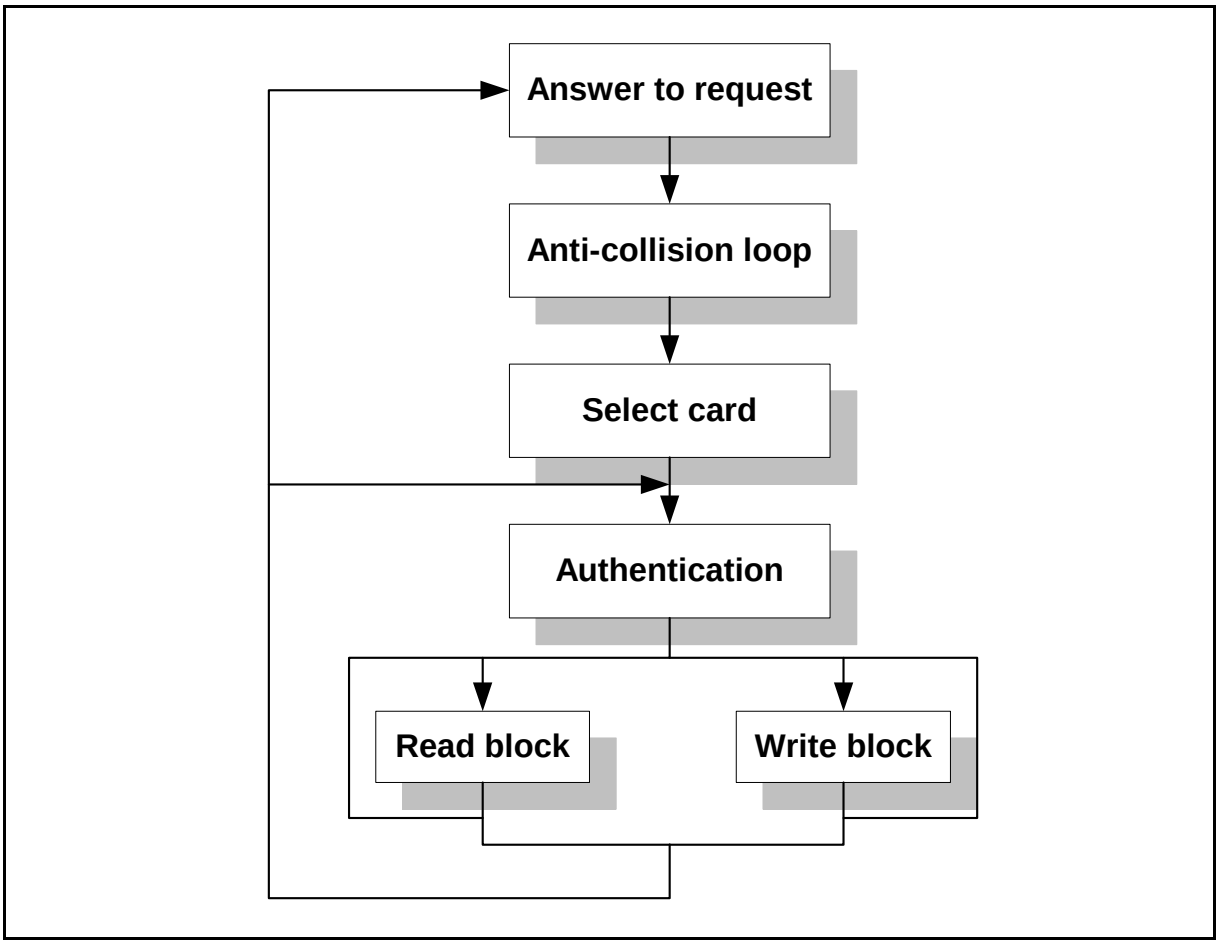

Figure 2-2 FM11RF32 Transaction sequence diagram

2.3.2. Transaction sequence description

Answer to Request: The communication protocol and the communication baud rate between RWD and card are defined in advance. When a card is in the operating range of a RWD, the RWD will communication with the appropriate protocol, to validate the type of a card.

Anti-collision Loop: If there are several cards in the operating range of RWD. They can be distinguished by their unique serial numbers and one can be selected for further transactions. The unselected cards return to the standby mode and wait for a new Answer to Request and Anti-collision loop.

Select Card: After a card selection, the card returns the Answer to Select code (SAK).

3 Pass Authentication: After selection of a card, RWD specifies the sector number and use the corresponding key for the 3 Pass Authentication procedures. Any communication after authentication is performed via stream cipher encryption. (If the next sector is selected, cipher verifying is necessary to the new sector.).

Read/Write: After authentication, the following operations may be performed:

READ: Read one block

WRITE: Write one block

DECREMENT: Decrements the contents of one block and stores the result in the data-register

INCREMENT: Increments the contents of one block and stores the result in the data-register

TRANSFER: Writes the contents of the data-register to one block

RESTORE: Stores the contents of one block in the data-register

Halt: Pause operation

3. Commands

3.1. Command code (HEX)

Commands	Code（HEX）
Request std	26
Request all	52
Anti-collision	93
Select Card	93
Authentication.la	60
Authentication.lb	61
Read	30
Write	A0
Increment	C1
Decrement	C0
Restore	C2
Transfer	B0
Halt	50

Table 3-1 FM11RF32 Command Code (HEX)

3.2. Commands demonstration

Answer to Request: Look for card in operating area. ‘Request Std’ means looking for card which is not set to halt, ‘Request All’ means looking for all cards which are in operating area.

Anti-collision: It means selecting only one card if there is one card or several cards in operating area.

Select Card: It means setting up the communication with the selected card after the anti-collision command.

Authentication: Before visiting memory, the user must verify if the operation is legal by coherence of cipher in RWD and cipher in card.

Read: Read 16 bytes of one block.

Write: Write data to one block.

Increment: Increment a certain value to numerical block, store the result in register.

Decrement: Decrement a certain value to numerical block, store the result in register.

Restore: Read contents of numerical block to register.

Transfer: Write contents of register to numerical block.

Halt: Card is set to halt.

4. Memory Organization and Access Conditions

The FM11RF32 has integrated a 32Kbits EEPROM which is split into 64 sectors with 4 blocks. One block consists of 16 bytes each, the structure of memory is shown below:

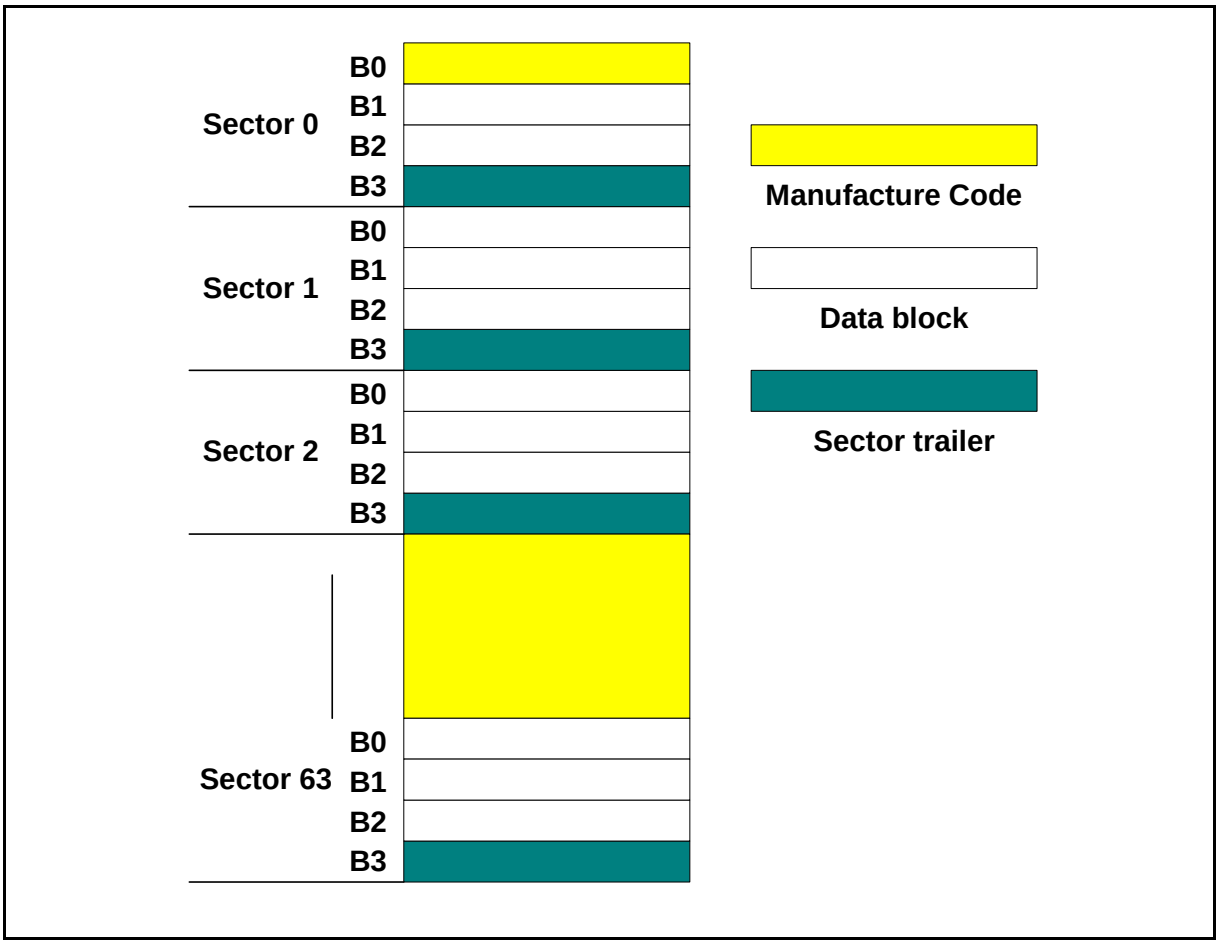

Figure 4-1 FM11RF32 Memory Organization

The fourth block of any sector contains access KEYA (6 bytes), KEYB (6 bytes) and the access conditions (4 bytes).The other three blocks of the sector serve as common data blocks. The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block and is also solidified. In many documents it is named “block0”. There are two kinds of data block application, one is data reserved and direct read/write, the other is denoted special data format, it can be initialization evaluation, increment, decrement and read. The structure of block 3 is shown below.

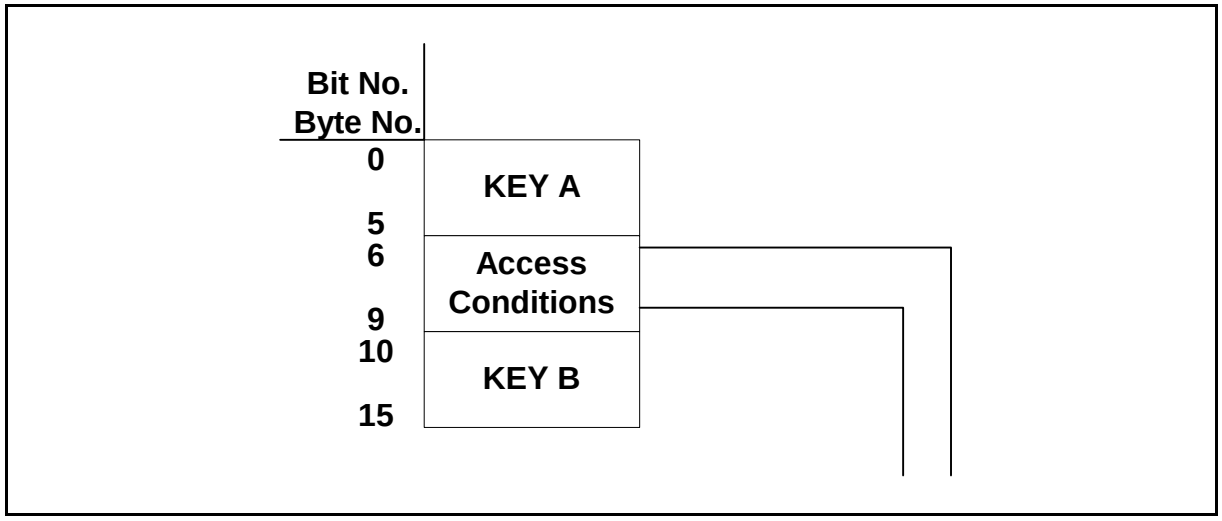

Figure 4-2 FM11RF32 Structure of Block 3

bit 7	bit 6	bit 5	bit4	bit3	bit 2	bit 1	bit 0
C2X3_b	C2X2_b	C2X1_b	C2X0_b	C1X3_b	C1X2_b	C1X1_b	C1X0_b
C1X3	C1X2	C1X1	C1X0	C3X3_b	C3X2_b	C3X1_b	C3X0_b
C3X3	C3X2	C3X1	C3X0	C2X3	C2X2	C2X1	C2X0
BX7	BX6	BX5	BX4	BX3	BX2	BX1	BX0

Note: b stands for inversion e.g.:C2X3_b=INV(C2X3)

X stands for sector No.(0~15)

Y stands for block No.(0~3)

C stands for control bit

B stands for reserve bit

Access condition for the Block 3 (X=0-15)

			KEYA	KEYA	Access Con	Access Con	KEYB	KEYB
C1X3	C2X3	C3X3	read	Write	Read	Write	read	Write
0	0	0	never	KEYA|B	KEYA|B	Never	KEYA|B	KEYA|B
0	1	0	never	Never	KEYA|B	Never	KEYA|B	Never
1	0	0	never	KEYB	KEYA|B	Never	never	KEYB
1	1	0	never	Never	KEYA|B	Never	never	Never
0	0	1	Never	KEYA|B	KEYA|B	KEYA|B	KEYA|B	KEYA|B
0	1	1	Never	KEYB	KEYA|B	KEYB	never	KEYB
1	0	1	Never	Never	KEYA|B	KEYB	never	Never
1	1	1	Never	Never	KEYA|B	Never	never	Never

Note: KEY A|B means KEY A or KEY B;

never means can't perform the function.

Access condition for Data Blocks (X=0-15 sectors, y=0-2 block of each sector)

C1XY	C2XY	C3XY	Read	Write	Increment	decr, transfer, restore
0	0	0	KEYA|B	KEYA|B	KEYA|B	KEYA|B
0	1	0	KEYA|B	Never	Never	Never
1	0	0	KEYA|B	KEYB	Never	Never
1	1	0	KEYA|B	KEYB	KEYB	KEYA|B
0	0	1	KEYA|B	Never	Never	KEYA|B
0	1	1	KEYB	KEYB	Never	Never
1	0	1	KEYB	Never	Never	Never
1	1	1	Never	Never	Never	Never

Table 4-1 FM11RF32 Access condition for Data Blocks

5. Data Integrity

Following mechanisms are implemented in the contactless communication link between RWD and card to ensure very reliable data transmission:

- Anti-collision
- 16 bit CRC per block
- parity bits for each byte
- Bit count checking
- Bit coding to distinguish between “1”, “0”, and no information
- Channel monitoring (Protocol sequence and bit stream analysis)

6. Security

The FM11RF32 Card has high security: 3 Pass Authentication must be through before read/write operation. Each card has different Serial Numbers, Crypto-Data transfer, Key Transfer and Access Key Protection which guarantee the uniqueness of each card.

Keys in the cards are read protected but can be altered by who knows the actual key. There are 64 sectors in the card, each sector has own keys (Key A, Key B). Two different keys for each sector support systems using key hierarchies, so FM11RF08SH offers real multi-application functionality.

Revision History

Version	Publication date	Pages	Paragraph or Illustration	Revise Description
1.0	May. 2004	4		Initial Release.
2.0	Oct. 2007	15		Updated Format.
2.1	May. 2008	15	Sales and service	Updated the address of HK office.

Sales and Service

Shanghai Fudan Microelectronics Co., Ltd.
Address: Bldg No. 4, 127 Guotai Rd,
Shanghai City China.
Postcode: 200433
Tel: (86-21) 6565 5050
Fax: (86-21) 6565 9115

Shanghai Fudan Microelectronics (HK) Co., Ltd.
Address: Unit 506, 5/F., East Ocean Centre, 98 Granville Road,
Tsimshatsui East, Kowloon, Hong Kong
Tel: (852) 2116 3288 2116 3338
Fax: (852) 2116 0882

Beijing Office
Address: Room.1208, Bldg C,
Zhongguancun Science and Technology Development Edifice,
34 zhongguancun Street (South),
Hai Dian District, Beijing City, China.
Tel: (86-10) 6212 0682 6213 9558
Fax: (86-10) 6212 0681

Shenzhen Office
Address: Room.1301, Century Bldg, Shengtingyuan Hotel,
Huaqiang Rd (North),
Shenzhen City, China.
Tel: (86-755) 8335 1011 8335 0911
Fax: (86-755) 8335 9011

Web Site: http://www.fmsh.com/