8kBits Contactless Smart Card Chip FM11RF08

FM11RF08 is the contactless smart card chip developed by shanghai FM Co.,Ltd..It takes 0.6um CMOS EEPROM processing technology. The chip has 1K×8Bits EEPROM organization, and 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 FM11RF08 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.

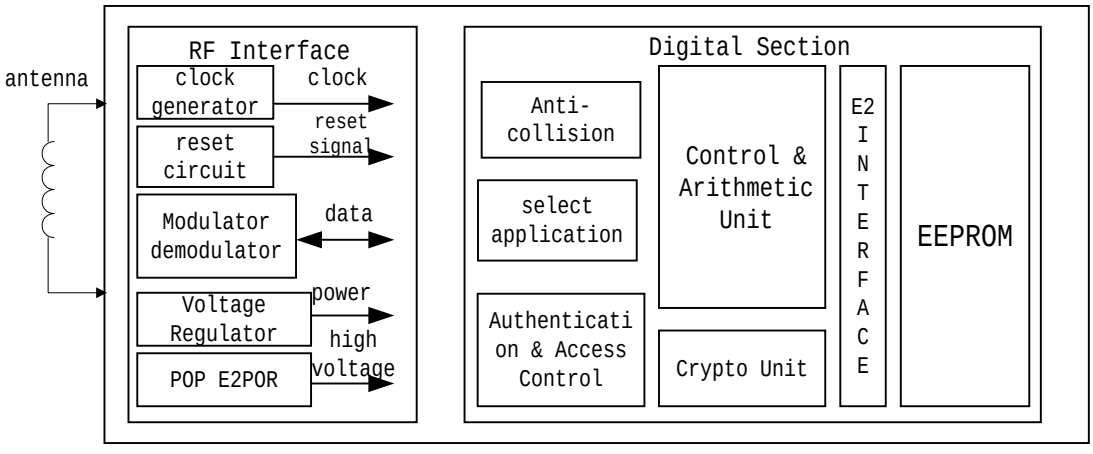
FEATURES

◆Compatible with ISO/IEC 14443
◆1024×8bit EEPROM memory, no battery.
◆13.56MHZ operating frequency
◆106Kbaud data communication rate
◆The permissible distance between antenna and card is up to 100mm free air.
◆Half duplex communication protocol using handshake
◆High security level data communication
◆Organized in security separated 16 sectors supporting multiapplication use.
◆Each sector has its own two secret files for systems using key hierarchies.
◆Access to memory zones ate flexible user defined by a variety of access conditions.
◆Arithmetic capability: increase and decrease.
◆More than ten thousand write test, data retention of 10 years

Typical Transaction Time

◆	Identification of a card	3ms
◆	Read Block (16bytes)	2.5ms(excl. Authentication)
◆	Write Block +Control Read	12ms(excl. Authentication)
		14ms(incl. Authentication)
◆	Typical Ticketing Transaction	<100ms

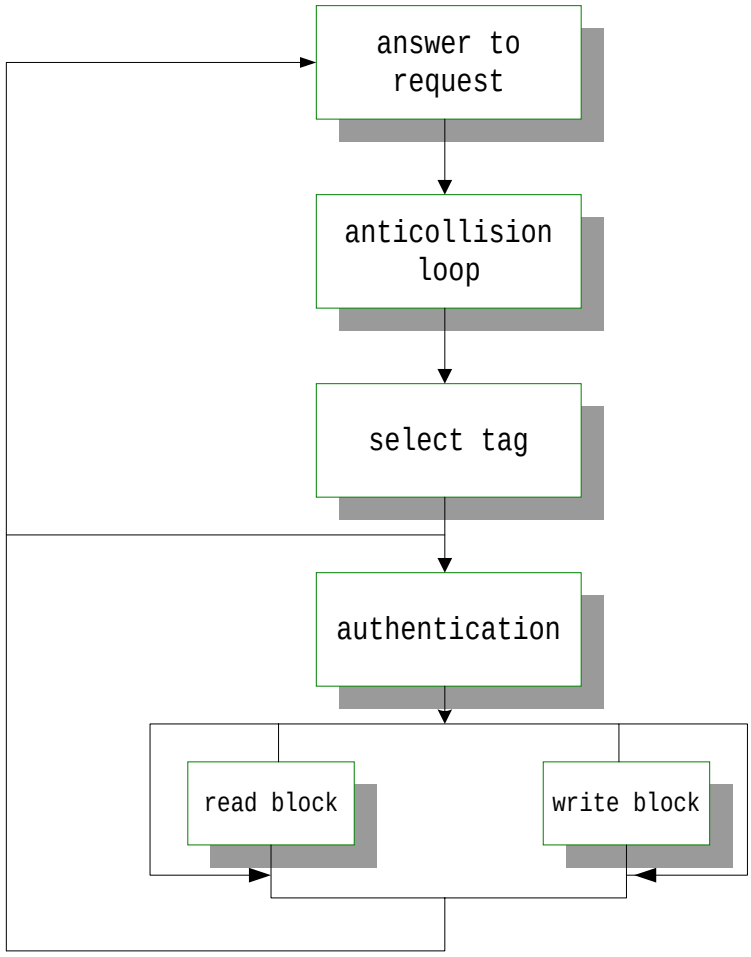
BLOCK DIAGRAM



The electronic unit of the card comprises just an antenna (coil) and an ASIC （FM11RF08）and no further external components.

FUNCTION DESCRIPTION

1. **Transaction sequence:**



Answer to Request:

The type of a card defines the communication protocol and the communication baudrate between RWD and card. When a card is in the operating range of a RWD, the RWD continues communication with the appropriate protocol, specified by the type of a card.

Anticollision Loop:

If there are several cards in the operating range of RWD they can be distinguished by their different 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 Anticollision Loop.

***Select Card**:*

After selection of a card, the card returns the Answer To Select code (SAK).

3 Pass Authentication:

After Selection of a card, RWD specifies the memory location of the following memory access and use the corresponding key for the 3 Pass Authentication procedure. Any communication after authentication is performed via stream cipher encryption.

Read/Write:

After authentication of 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

2.Commands aggregation:

Commands	Code
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

3. Data Integrity

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

- Anticollision
- 16 bit CRC per block
- 16 bit Parity per block
- Bit count checking
- Bit coding to distinguish between “1”, “0”, and no information
- Channel monitoring (Protocol sequence and bit stream analysis)

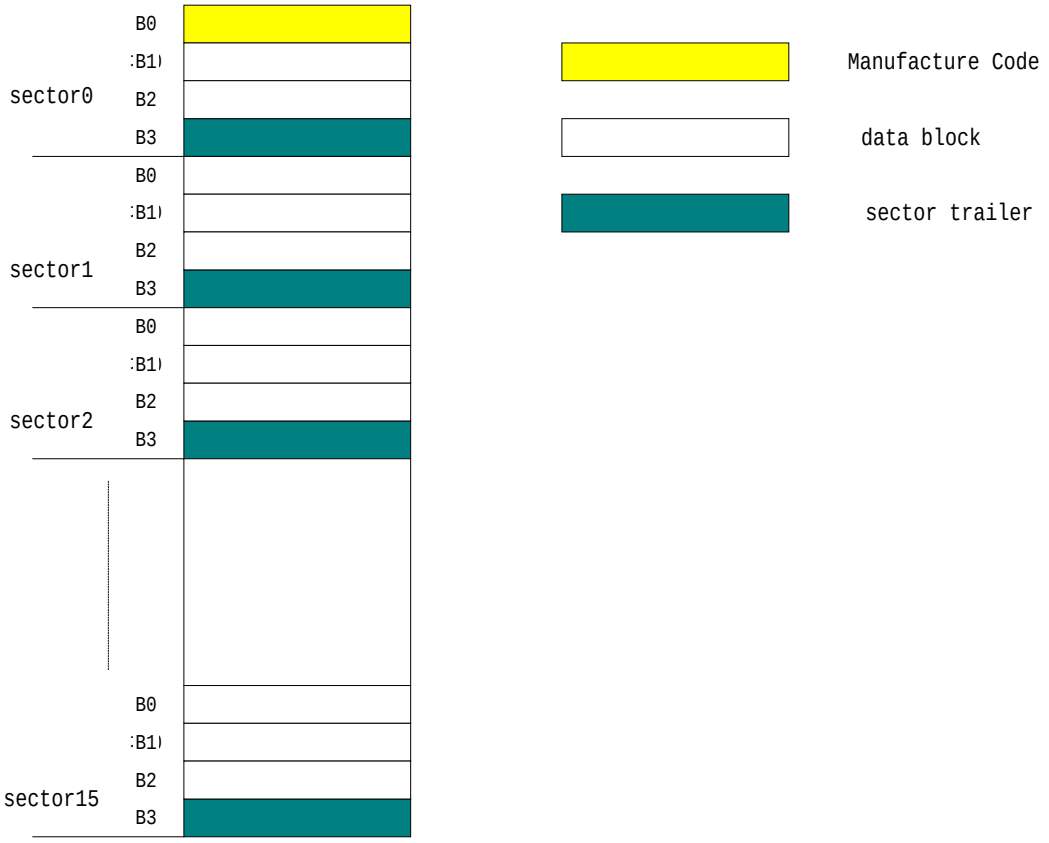
4. Security:

The FM11RF08 Card has high security: 3 PASS Authentication must be through before read/write operation. Serial Numbers, wick can not be altered, guarantee the uniqueness of each card. Crypto-Data transfer, Key Transfer and Access Key Protection.

Keys in the cards are read protected but can be altered by who knows the actual key. There are 16 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 FM11RF08 offers real multi-application functionality.

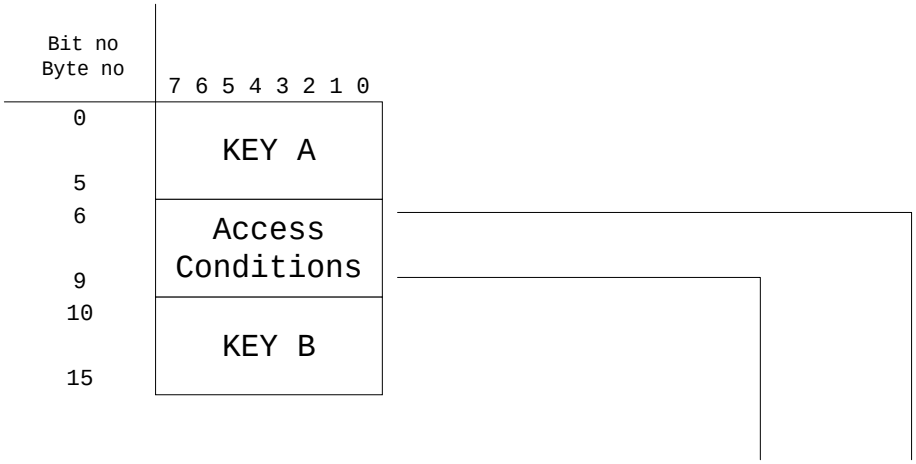
5. Memory Organization and Access Conditions

The FM11RF08 has integrated an 8K bits EEPROM which is split into 16 sectors with 4 blocks. One block consists of 16 bytes



The fourth block of any sector contains access KEYA (6 bytes) and an optional KEYB(6 bytes) and the access conditions for the four blocks of that sector(4 bytes).The other 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. IN many documents it is named “block0”.

The structure of block3 is shown below.



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

b stands for inversion e.g.:C1X0_b=INV(C1X0)

X stands for sector No.(0~15)

Y stands for block No.(0~3)

Access condition for the Sector Trailer(y=3)

			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 (y=0-2)

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