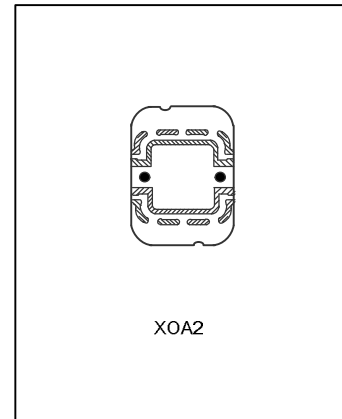## 8K-BIT CONTACTLESS IC CARD

DESCRIPTION

SC23R01 is a smart card module utilizing CMOS EEPROM technology. It is a multi-application functionality smart card with 1024 bytes EEPROM memory. Its embedded crypto and communication modules can protect the system from any kind of tampering and make it attractive in ticketing applications.

FEATURES

* 1024 X 8 bit EEPROM;

* Operating frequency: 13.56MHz; baud rate: 106Kbit/s;

* Contactless transmission of data and not need external power supply;

* Operating distance: up to 10cm;

* High security data transmission;

* 16 independence sectors which support manifold applications;

* For some key hierarchy system, each sector has two secret keys;

* Customer definable access conditions for each memory block;

* Arithmetic logic function;

* High credible EEPROM controller, write endurance100000 cycles, data retention of 10 years;

* Comply to the ISO/IEC14443 type A.

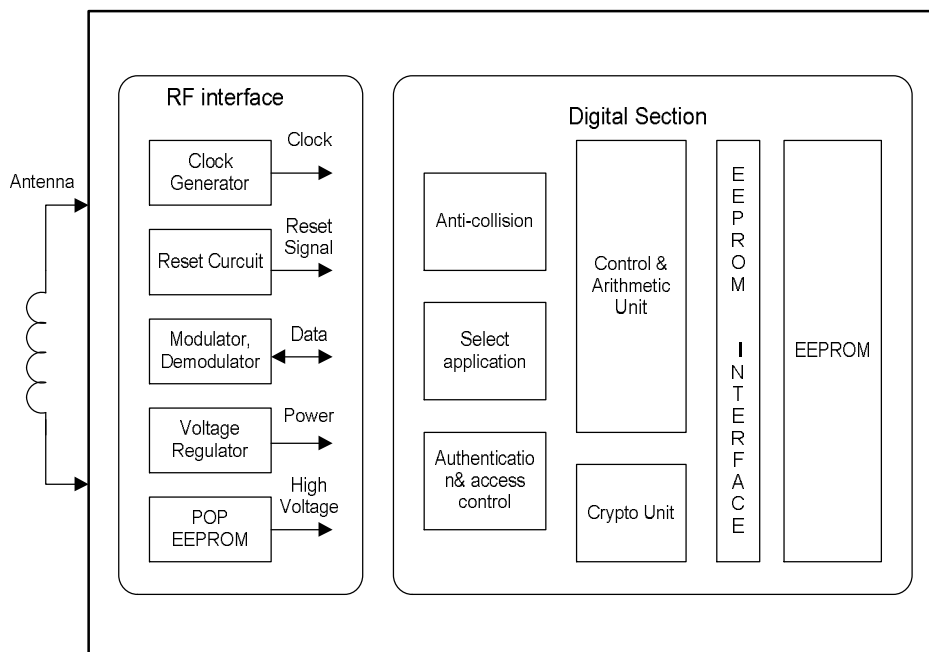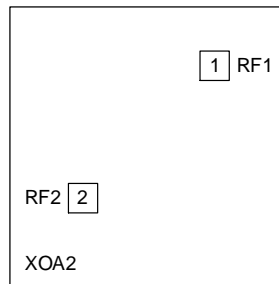XOA2

ORDERING INFORMATION

Device	Package
SC23R01	XOA2
SC23R01T-01-002	Gold bump

APPLICATIONS

* used for ticketing system with IC card.

BLOCK DIAGRAM

PIN CONFIGURATION

```
                        ┌───┐
                        │ 1 │ RF1
                        └───┘

            ┌───┐
      RF2   │ 2 │
            └───┘
      XOA2
```

FUNCTION DESCRIPTION

1. RF interface and read/write device

1.1 Request （REQ STD/ALL）

The communication protocol of SC23R01 is complied with the ISO14443A. When the card is positioned in the proximity of the read/write device (RWD), the RWD sends the REQ STD/ALL command to confirm whether the card is SC23R01.

1.2 Anti-collision loop

When there are several cards in the operating rang of the RWD, the anticollision algorithm selects one card for further transaction. The unselected card return to the standby mode and wait for a new request command. In this course, it will return the serial number of the card.

1.3 Select card

Select the serial number of the selected card, the card returns the answer to select code (=08H).

1.4 3 Pass authentication

After selecting the card, the RWD specifies the memory location which needs access, and uses the corresponding key for 3 pass authentication. After authenticating successfully, all memory operations are encrypted. (for selecting another sector, the key should be authenticated again) .

1.5 Memory operations

After authentication, the following operation may be performed:

Read: read block.

Write: write block.

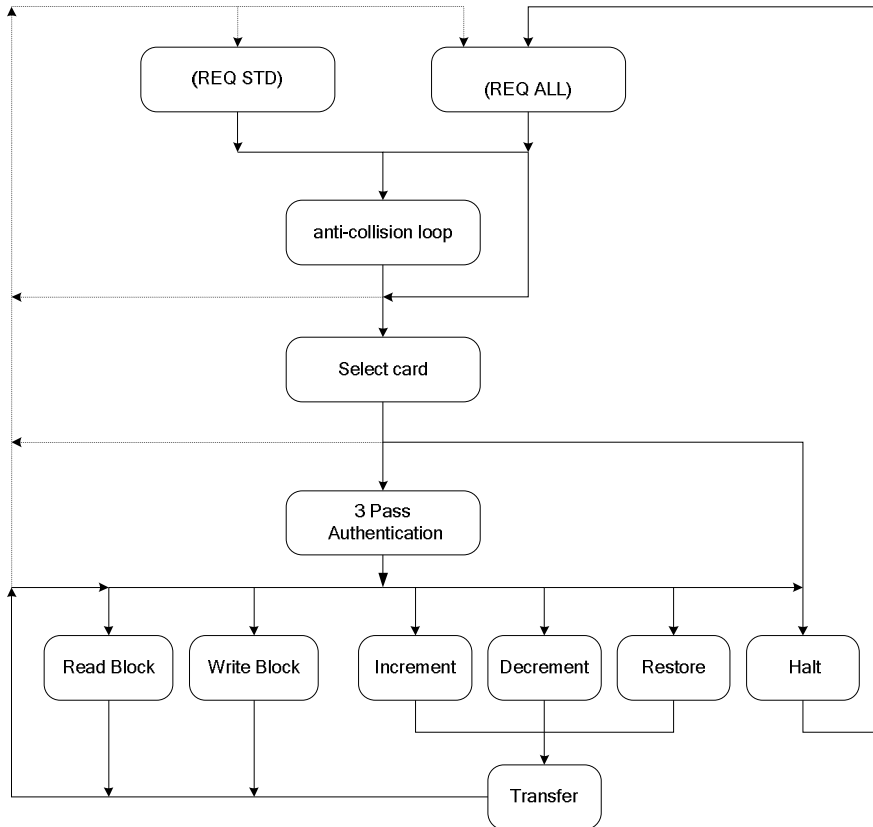Decrement: decrease the content of a block and store the result in a data register.

Increment: increase the content of a block and store the result in a data register.

Transfer: write the content of data register to a value block.

Restore: read the content of the value block to the data register.

Halt: set the card in the halt mode.

The operation flow chart:

2. Instruction

Commands	Code(hex)
Request standby card	26
Request all the cards in the operating range	52
Anti-collision	93
Select card	93
Authentication key A	60
Authentication key B	61
Read	30
Write	A0
Increment	C1
Decrement	C0
Restore	C2
Transfer	B0
Halt	50

3. Data integrity

In the contactless communication, the following measures ensure the data transmission:

- anti-collision
- 16 bits CRC error correction for each frame

- parity bits for each byte
- bit count checking
- bit coding to distinguish between "1" , "0" or no information
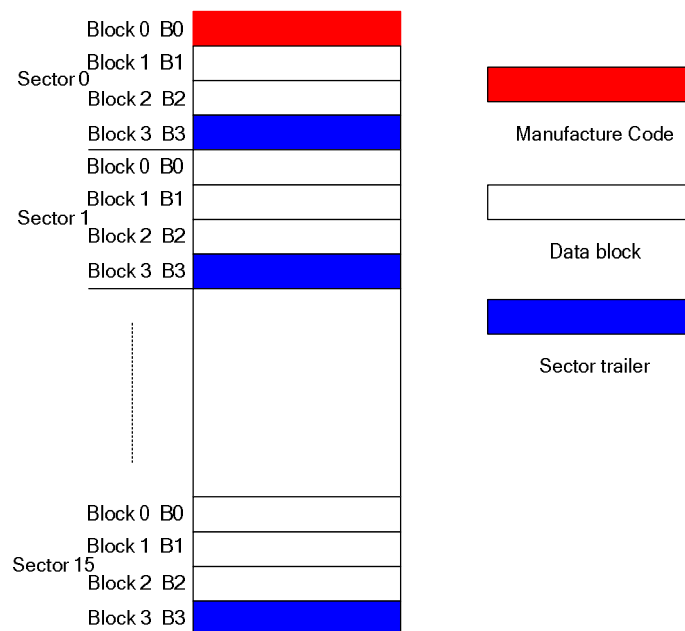- channel monitoring(protocol sequence and bit stream analysis)

4. Security

SC23R01 provides high security: three pass authentication is before read/write operation; each card has different serial number, ; transfer encrypted data and key protection.

The secret key of the card is protected and cannot be read, which only the user knows and can amend it . The EEPROM is divided into 16 sectors, and each sector is with different key, user can set the key according to different sector (with multi-applications in one card). The RWD specifies the sector to be accessed only by verifying the key A or B.

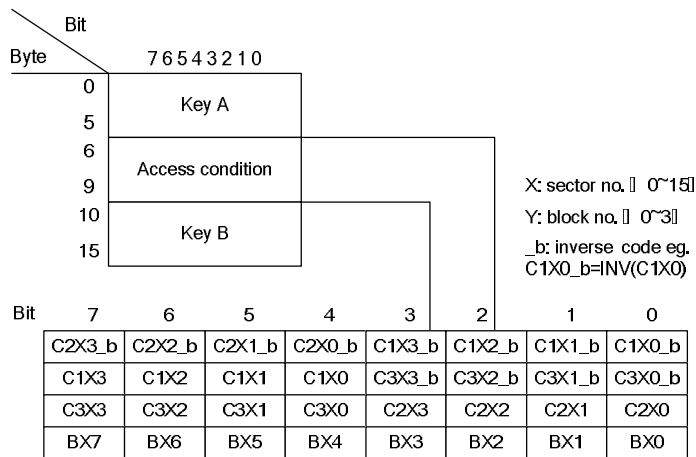## 5. Memory configuration and access condition

The 8 k bits EEPROM is organized in 16 sectors with 4 blocks of 16 bytes each sector.

Memory map:

The block 3 of each sector contains the secret key A (6 bytes), access control condition (4 bytes) and secret key B(6 bytes), which is a specific block , other three blocks are data blocks; but the block 0 of the sector 0 used for store manufacture code and serial number, it is solidified and only readable. The data blocks can be configured two applications: read/write blocks and value blocks; the read/write block is used for store data, direct read and write; the value block is used for initialization, increment, decrement and value reading for direct control of the stored value.

Block 3 configuration:

Bit	7	6	5	4	3	2	1	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

X: sector no. $[0\sim15]$

Y: block no. $[0\sim3]$

_b: inverse code eg. $\overline{C1X0}$_b=INV(C1X0)

Access control of block 3 is as follows:

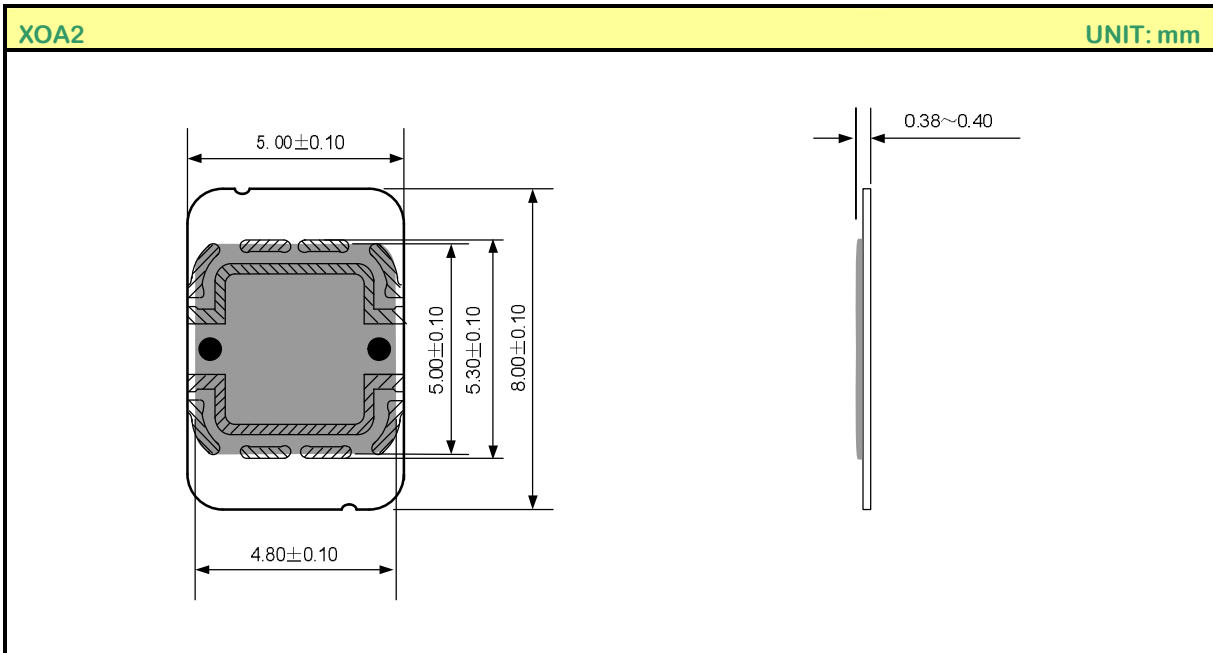| C1X3	C2X3	C3X3	Key A Read	Key A Write	Access Control Read	Access Control Write	Key B Read	Key B Write	Remark
0	0	0	Never	KEY A	KEY A	Never	KEY A	KEY A	Key B may be read
0	1	0	Never	Never	KEY A	Never	KEY A	Never	Key B may be read
1	0	0	Never	KEY B	KEY A|B	Never	Never	KEYB	
1	1	0	Never	Never	KEY A|B	Never	Never	Never	
0	0	1	Never	KEY A	KEY A	KEY A	KEY A	KEY A	Key B may be read, transfer configuration
0	1	1	Never	KEY B	KEY A|B	KEY B	Never	KEY B	
1	0	1	Never	Never	KEY A|B	KEY B	Never	Never	
1	1	1	Never	Never	KEY A|B	Never	Never	Never	

Note: KEYA|B indicates secret key A or key B; never denotes no condition implement.

Data block storage control:

C1XY	C2XY	C3XY	Read	Write	Increment	Decr, Transfer, Restore
0	0	0	KEY A|B[1]	KEY A|B[1]	KEY A|B[1]	KEY A|B[1]
0	1	0	KEY A|B[1]	Never	Never	Never
1	0	0	KEY A|B[1]	KEY B[1]	Never	Never
1	1	0	KEY A|B[1]	KEY B[1]	KEY B[1]	KEY A|B[1]
0	0	1	KEY A|B[1]	Never	Never	KEY A|B[1]
0	1	1	KEY B[1]	KEY B[1]	Never	Never
1	0	1	KEY B[1]	Never	Never	Never
1	1	1	Never	Never	Never	Never

Note: if key B can be read in the sector trailer, then it cannot be as key authentication(all grey line in above table). If the RWD tries to authenticate any blocks with key B using gray line, the card will refuse any operation for memory after authentication.

PACKAGE OUTLINE

XOA2   **UNIT: mm**

5.00±0.10

8.00±0.10
5.30±0.10
5.00±0.10

4.80±0.10

0.38~0.40

MODULE HANDLING DESCRIPTION (ADVICE)

- The substrate material of the card is PVC of 6 layers (Inlay 2 layers).
- Antenna material: monocrystal Cu (enameled wire); antenna coil: 5 loops; linear diameter: $\Phi0.13$mm; inside diameter: 44x75mm; outside diameter: 45 x76mm; the module and antenna adopt bonding technology.
- The winding of the antenna coil makes the inductance to be 5.3~5.5µḨ in order to match the antenna with the module and make sure it will meet the requirement of resonance frequency and induction distance.

CAUTION
ELECTROSTATIC
SENSITIVE DEVICE
DO NOT OPEN OR HANDLE
EXPECT AT A STATIC-FREE
WORKSTATION

HANDLING MOS DEVICES:

Electrostatic charges can exist in many things. All of our MOS devices are internally protected against electrostatic discharge but they can be damaged if the following precautions are not taken:

- Persons at a work bench should be earthed via a wrist strap.
- Equipment cases should be earthed.
- All tools used during assembly, including soldering tools and solder baths, must be earthed.
- MOS devices should be packed for dispatch in antistatic/conductive containers.