HF RFID QR2217 CHIP

Datasheet

V1.01

2008.8.6

Shanghai Quanray Electronics Co., Ltd.

Add: 2F, Building 10-01, No.1387, Zhang Dong Road, Pudong District, Shanghai, China
Tel: 86-21-68795432 Fax: 86-21-68795835
Web: www.quanray.com Zip：201203

Contents

1 Specification..2

1.1 ISO/IEC 14443 A RF 接口..2

1.2 EEPROM Memory..2

1.3 Security..2

1.4 Basic Chip Function Description...3

1.5 Electrical Specification...4

2 Function Description 4

2.1 Blocks division 4

2.2 Chip Block Diagram 5

2.3 Principle and State of Communication 6

2.4 Data integrity mechanism...7

2.5 Security..7

2.6 RF interface 8

2.7 Memory structure...8

2.8 Commands...9

2.9 Typical transaction flow..10

1 Specification

1.1 ISO/IEC 14443 A RF 接口

- Contact-less data transmission and energy supply (no battery is needed)
- Operating distance: Up to 100mm (Depending on inlay antenna and reader)
- Minimal working magnetic field strength: 0.3A/m (standard ID-1 antenna size)
- Maximal working magnetic field strength: 7.5A/m(standard ID-1 antenna size)
- Operating frequency: 13.56MHz
- Data rate: 106k bit/s
- High date integrity: 16 bits CRC, parity, bit coding and bit counting.
- True anti-collision
- 4 bytes serial number (according to ISO/IEC 14443-3 Cascade level 1)
- Typical ticketing transaction: < 100ms
- Fast counter transaction: < 10ms

1.2 EEPROM Memory

- 1K bytes, organized in 16 sectors with 4 blocks each, and 16 bytes in each block.
- The access of each page can be customized
- Data retention of at least 10 years
- Write/Erase endurance 100,000 cycles

1.3 Security

- 3-pass authentication: ISO/IEC DIS9798-2
- All data is encrypted in communication to prevent being intercepted.
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy.

- Unique 4-byte serial number in each card
- Cryptograms protection in transmission

1.4 Basic Chip Function Description

The air interface of QR2217 chip complies with ISO/IEC 14443 Type A（parts 2 and 3）standards. Adopting CRYPTO1 stream encryption in security protocol is to protect the security of data exchange.

QR2217 adopts advanced manufacturing technology. There is a high-speed CMOS EEPROM inside the chip. There aren’t any other elements except for IC and a high efficient antenna on the card. No battery is needed. The communication data rate is up to 106kbit/s when the card is inside the reader communication zone.

QR2217 can implement anti-collision function: when there is more than one card inside the reader communication zone, the anti-collision function can select one card and transact with it without being affected by the other cards’ in or out.

Application needs were taken into account during design. When passing the readers, user needn’t stop because of high communication data rate (<100ms). So the applications of the card include various certification, electronic wallets, automatic toll system, AFC System, etc.

Special emphasis has been placed on security against fraud. Mutual challenge and response authentication, data ciphering and message authentication checks protect the system from any kind of tampering and thus make it attractive for ticketing application. QR2217 adopts 3-pass authentication (ISO, IEC, DIS 9798-2), and CRYPTO1 stream encryption in all data to prevent being intercepted. The 4-byte UID is programmed during fabrication and cannot be modified later, which is actually a very effective anti-clone approach. This UID number can be used to encrypt the data in the chip or to derive diversified keys per ticket.

The chip and system offers real multi-application functionality. Two different keys for each sector support systems using key hierarchies.

In order to be more easily applied to different ways, the chip has several different on-chip resonant capacitance values to select. The capacitance can vary from 15pf to 50pf by replacing one metal mask according to customers' demands.

1.5 Electrical Specification

Parameter	Symbol	Note	Min	Nom	Max	Unit
Antenna Input Peak Current	Ian_peak				60	mA
Total Power Dissipation per die	Pin				100	mW
Storage Temperature	Ts		-55		125	°C
ESD Immunity	Ant1-Ant2[1]		+/-2			kV

Table 1 Absolute Maximum Ratings [1]

[1] Note: Stress beyond the limits of those listed under 'Absolute Maximum Ratings' may cause permanent damage to the device.

[2] MIL Standard 883-G method 3015 Human Body Model: C=100pf R=1.5k

Parameter	Symbol	Note	Min	Nom	Max	Unit
Operating carrier frequency	Fin		13.55	13.56	13.57	MHz
Input capacitance	Cin	2VRMS[1]	14.9	15.7[2]	16.5	pf
EEPROM Write Endurance	Nwe		100,000			cycles
EEPROM rentetion	Tret		10			years

Table 2 Electrical Characteristics

[1] LCR Meter HP4285 22° C Cp-D, 13.56MHz

[2] Compatible cap value with NXP's S50 IC, easy for packaging with NXP's S50 antenna

2 Function Description

2.1 Blocks division

QR2217 is contact-less IC chip, made up of RF communication interface, digital logic control block (including security control cell), and 1K bytes EEPROM. The energy and data are transmitted by coil antenna connecting with QR2213-CD chip, no external component needed. The structure is illustrated in Figure 1.

Blocks description:

- RF interface
  - Demodulator
  - Rectifier
  - Clock extraction or generation
  - Power on reset
  - Power (voltage) regulator (protector)
- Digital Core
  - Anti-collision: make several cards in the field be selected and operated one by one. The filed strength complies with ISO/IEC 14443 standards.
  - Commands interpretation and implementation: to interpret and implement the commands of QR2217, and operate on EEPROM.
  - Authentication: authentication should be done before every operation on EEPROM, to ensure the access to the data block has passed its operable key authentication.
  - Control and arithmetic logic unit: to store the data value in specific redundant format, and implement increment and decrement.
  - EEPROM interface
  - Encryption：CRYPTO1stream cryptogram is to protect data exchange security.
- EEPROM
  - With 1K bytes, organized in 16 sectors with 4 blocks each, and 16 bytes each block. The last blocks, called ‘trailer’ in each sector, stores two keys and programmable access condition to this page.

2.2 Chip Block Diagram

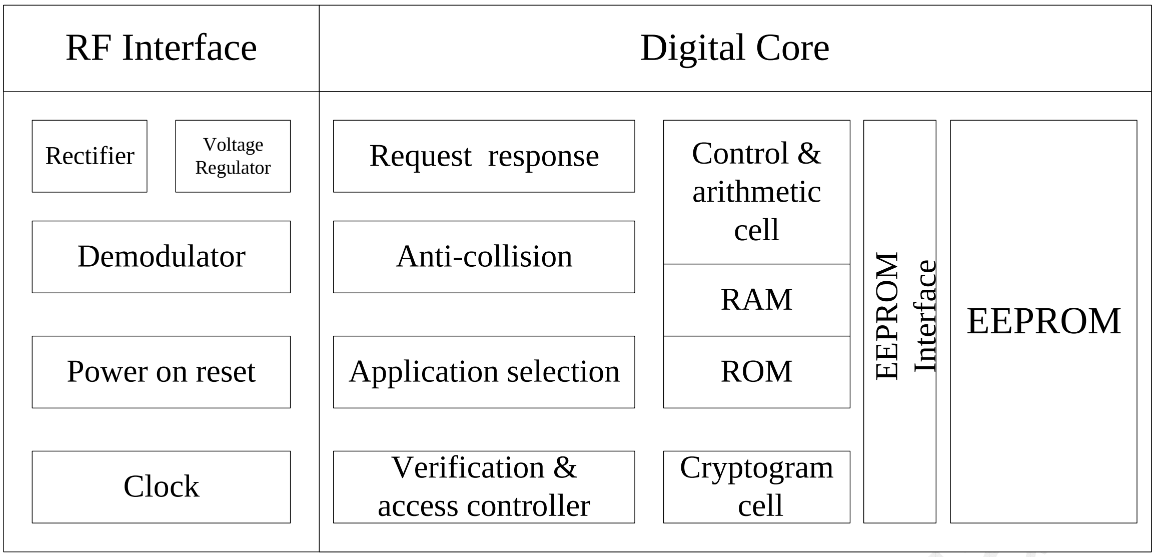


Figure 1 Chip Block Diagram

2.3 Principle and State of Communication

The communication (transaction) can be triggered by the PCD (Proximity Coupling Device) according to communication protocol. The signal protocol works on half-duplex mode, which means a time-division communication between PICC and PCD. In the communication, PICC is in passive mode. The digital core in PICC chip is to accomplish the jump between different states or commands operation according to the chip’s current state and input commands. If response is needed, the digital core can also transmit it.

The state of QR2217 is shown in Figure 2.

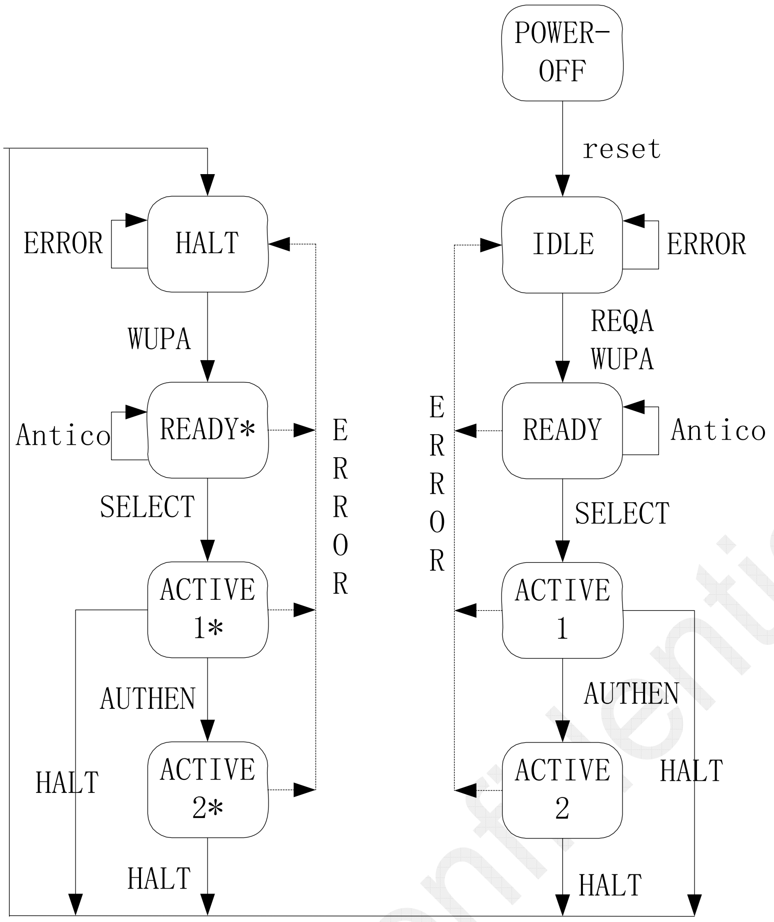


Figure 2 The state of QR2217

Note: * indicates the former state is HALT. If receives error or virtual HALT command, the state will return to HALT state, rather than return to IDLE state.

2.4 Data integrity mechanism

In the air communication between readers and smart cards, the following mechanism is adopted to protect the reliability of data transmission.

16-bit CRC in communication block

A parity bit in each byte

Bit counting check out

Bit Coding, including ‘1’, ‘0’ or nothing

Channel monitoring (by the protocol sequence and bit rate analysis)

2.5 Security

3-pass authentication according to ISO9798-2 is adopted to provide high security level.

The sequence of 3-pass authentication:

a) The reader selects one sector to access, and then selects KEYA or KEYB.

b) The card can read keys and access condition from sector trailer, and then transmit a random number (RB) to the reader. (The first pass of authentication)

c) The reader calculates out the RB by key value and other inputs. Then the reader also generates a random number (RA) and sends "RA + RB" (TokenAB) back to card. (The second pass of authentication).

d) The card validates the response from the reader. If the RB back from reader is correct, which means reader is authenticated; the card transmits a response back to the reader. (The third pass of authentication)

e) The reader validates the response from the tag once again. If the response is correct, the card is authenticated by the reader.

The communication is encrypted between cards and readers after transmitting the first random number (b).

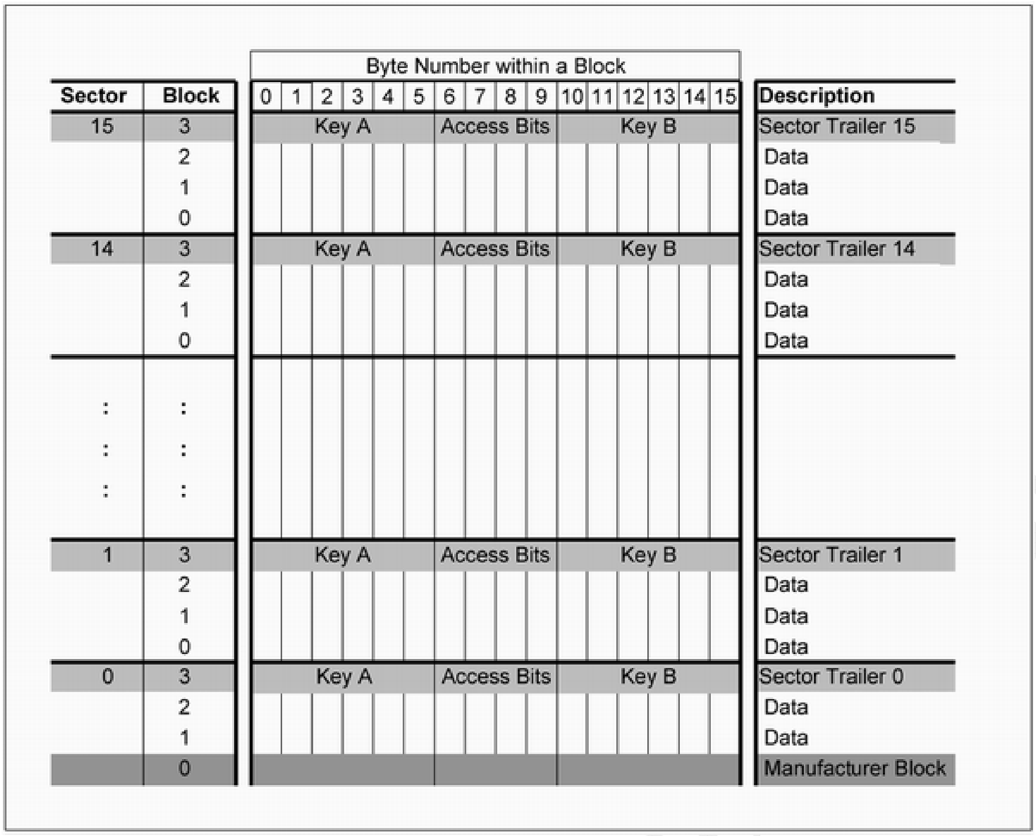
2.6 RF interface

The RF interface complies with ISO/IEC 14443 standards of contact-less smartcard. The carrier wave generated by readers always exists (sometimes stops when transmitting data), as to supply power to the cards.

Each information frame has one start bit in bilateral communication. Each byte is transmitted with a parity bit/odd bit on the rear. The lowest bit in lowest byte in selected data block is transmitted first. The maximum length of information frame is 163 bits. (16 bytes data + 2 bytes CRC + 1 start bit = 16*9+2*9+1)

2.7 Memory structure

The memory structure of QR2213CD is showed as Figure 3. It has 8192 bits, organized in 16 sectors with 4 blocks each, and 16 bytes in each block. Each EEPROM cell has two states: "0" for being cleaned, "1" for being written in.



Sector	Block	Byte 0–5	Byte 6–9	Byte 10–15	Description
15	3	Key A	Access Bits	Key B	Sector Trailer 15
	2				Data
	1				Data
	0				Data
14	3	Key A	Access Bits	Key B	Sector Trailer 14
	2				Data
	1				Data
	0				Data
:	:				
:	:				
:	:				
1	3	Key A	Access Bits	Key B	Sector Trailer 1
	2				Data
	1				Data
	0				Data
0	3	Key A	Access Bits	Key B	Sector Trailer 0
	2				Data
	1				Data
	0				Manufacturer Block

Figure 3 the memory structure of QR2217

2.8 Commands

QR2217 can support the following commands:

Commands	Commands code（Hex）	Description	Remarks
Request std（REQA）	26	Standard requests	
Request all(WUPA)	52	All requests	
AntiCollision	93	Anti-collision	Maybe several interactions *
Select Tag	93	Select Tag	
Authentication_keya	60	KEYA Authentication	Two interactions
Authentication_keyb	61	KEYB Authentication	Two interactions
Read	30		
Write	A0	Write	Two interactions
Increment	C1	Increment	Two interactions
Decrement	C0	Decrement	Two interactions
Restore	C2	Restore	Two interactions
Transfer	B0	Transfer	
Halt	50	Halt	

Table 3 QR2217 commands in normal mode

*: depends on the amount of the cards inside the reader communication zone.

These commands can be supported in different states. There are 10 states in Mifare 1, including Power off、IDLE、READY、ACTIVE1、ACTIVE2、HALT、READY*、ACTIVE1*、ACTIVE2* and TESTMODE. The commands of Read、Write、Increment、Decrement、Restore and Transfer are supported in ACTIVE2 and ACTIVE2*.

In the following paragraphs, the explanations and descriptions of each command are listed in details. For short, Proximity Coupling Device is called PCD, and Proximity Card is called PICC.

2.9 Typical transaction flow

A typical transaction sequence includes request & anti-collision loop, selecting card, 3 pass-authentication, read block, write block, increment, and decrement, etc.

The typical transaction flow and transaction time are shown in the following figure.

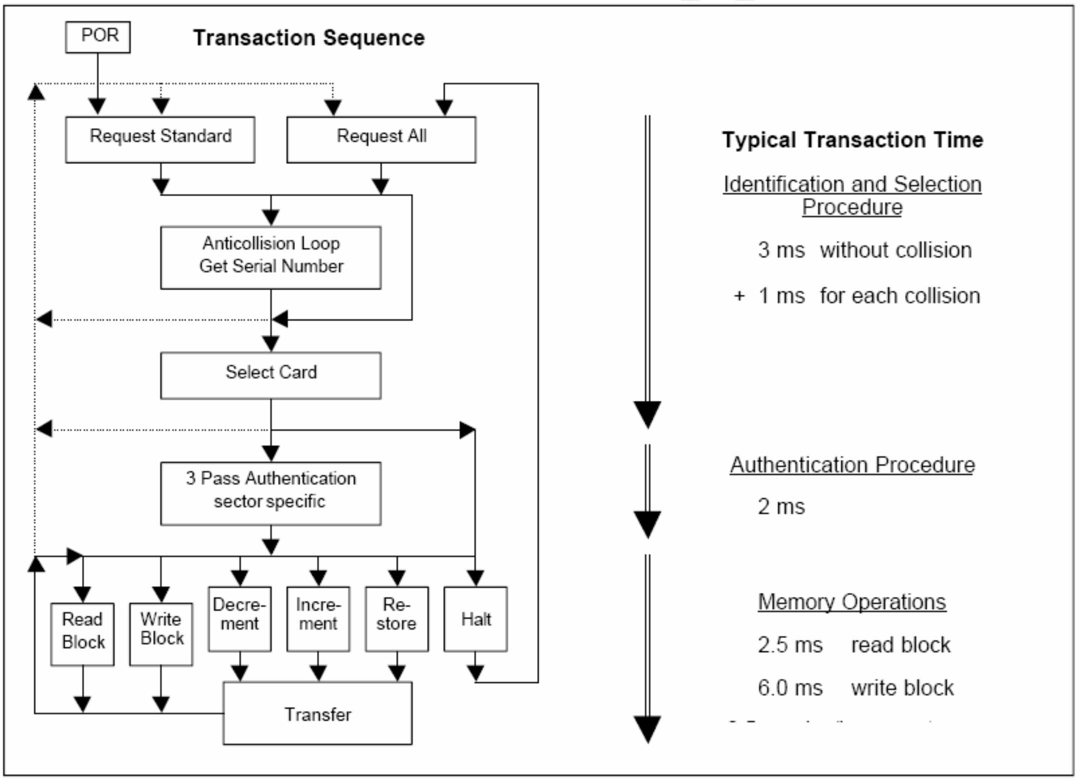


Figure 4 Typical transaction flow