UNC20C01R
1Kbyte EEPROM Contactless Card IC

Application

The UNC20C01R is intended for use in contactless payment cards for ticketing, communications, etc. systems. A single IC card may support multiple payment applications thanks to an advanced system of security keys and access conditions for different memory areas.

A special card reader is used for the card operation. The card reader is provided with an antenna to implement inductive coupling with the card.

Features

- **Card configuration**
  - The UNC20C01R IC and an antenna (several coil wire turns along the perimeter of a standard-size card)
  - No battery needed since the card uses the energy of the field generated by the card reader antenna
- **Data exchange**
  - Operating frequency: 13.560±0.007 MHz
  - Data exchange with the card reader complies with ISO 14443 Type A standard
  - Half-duplex mode with acknowledgement, 106 kBaud data rate
  - Operating distance to the reader antenna up to 10 cm (depending on the antenna and reader geometries)
  - The card may be in motion during a transaction
  - Several cards may simultaneously be present in the reader access area (the reader selects a card for data exchange by using a special anti-collision mechanism and a unique serial number by which cards are distinguished from each other)
- **Increased reliability of data transactions**
  - Anticollision function and individual card handling
  - 16 bits CRC per data frame
  - Parity bit for each data byte
  - Bit coding to distinguish between ‘0’, ‘1’ and “no data”
  - Fixed protocol sequence with a start bit and bit count per frame monitoring
  - Command receipt acknowledgement or transfer error message
- **Data storage**
  - 1 Kbyte EEPROM organized in 16 sectors
  - Each sector consists of 4 individually addressable 16-byte blocks
  - Data retention: 10 years or more
  - Write endurance: min 100,000 cycles
- **Data security**
  - Unique unchangeable serial card number
  - A set of 2 secret keys 48 bits long for each sector
  - Capability of restricted access (read or write with or without a secret key) to individual memory blocks
  - Mandatory mutual three pass authentication of the card and reader
  - Encryption of data transmitted via the channel during data exchange
- **Data handling**
  - Read block from the card memory
  - Write block into the card memory
  - Restore 32-bit binary number from a memory block into the card ALU
  - Subtract from 32-bit binary number in the card ALU
  - Add to 32-bit binary number in the card ALU
  - Transfer 32-bit binary number from the ALU into a card memory block
- **Typical transaction time**
  - Card identification (“Start”, “Request Card”, “Anticollision” and “Select Card”) — 3 ms
  - Authentication — 2 ms
  - Block (16 bytes) read — 2.5 ms
  - Block write and control reading — 8.5 ms
- **Absolut maximum ratings**
  - Operating temperature: –25...+75°C
  - Storage temperature: –55...+125°C

UNC20C01R Structure

The UNC20C01R structure is shown in Fig. 1.

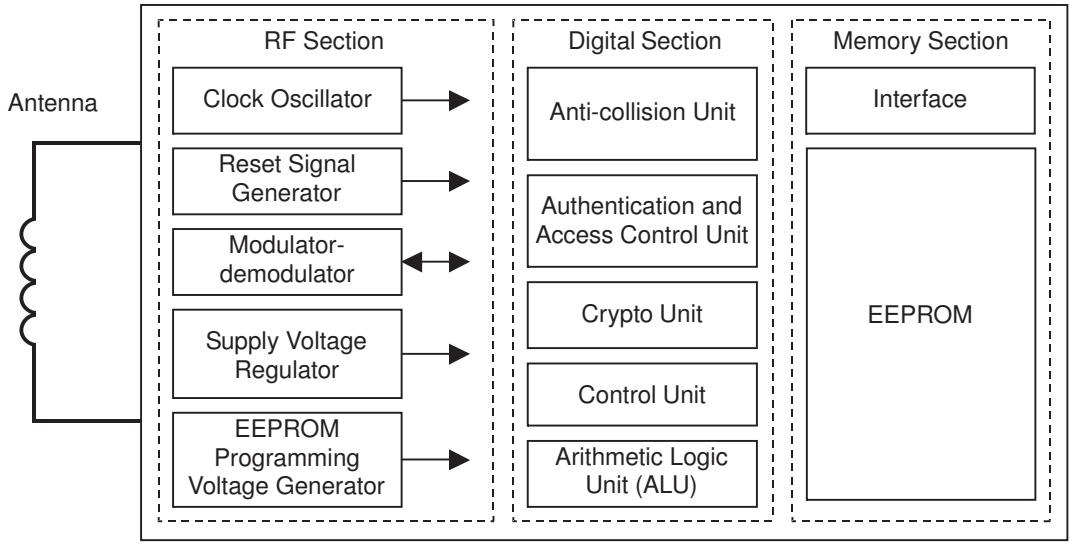


Fig. 1. UNC20C01R structure

The UNC20C01R has only two terminals connected to the antenna coil. Directly connected to the antenna is the radio frequency (RF) section used for energizing and synchronization of all IC units as well as for data exchange with the reader. The digital section controls all data exchange processes between the card and the reader. The memory section contains an electrically erasable programmable read-only memory (EEPROM) to store payment applications data, encryption keys and access codes.

UNC20C01R Control Command Set

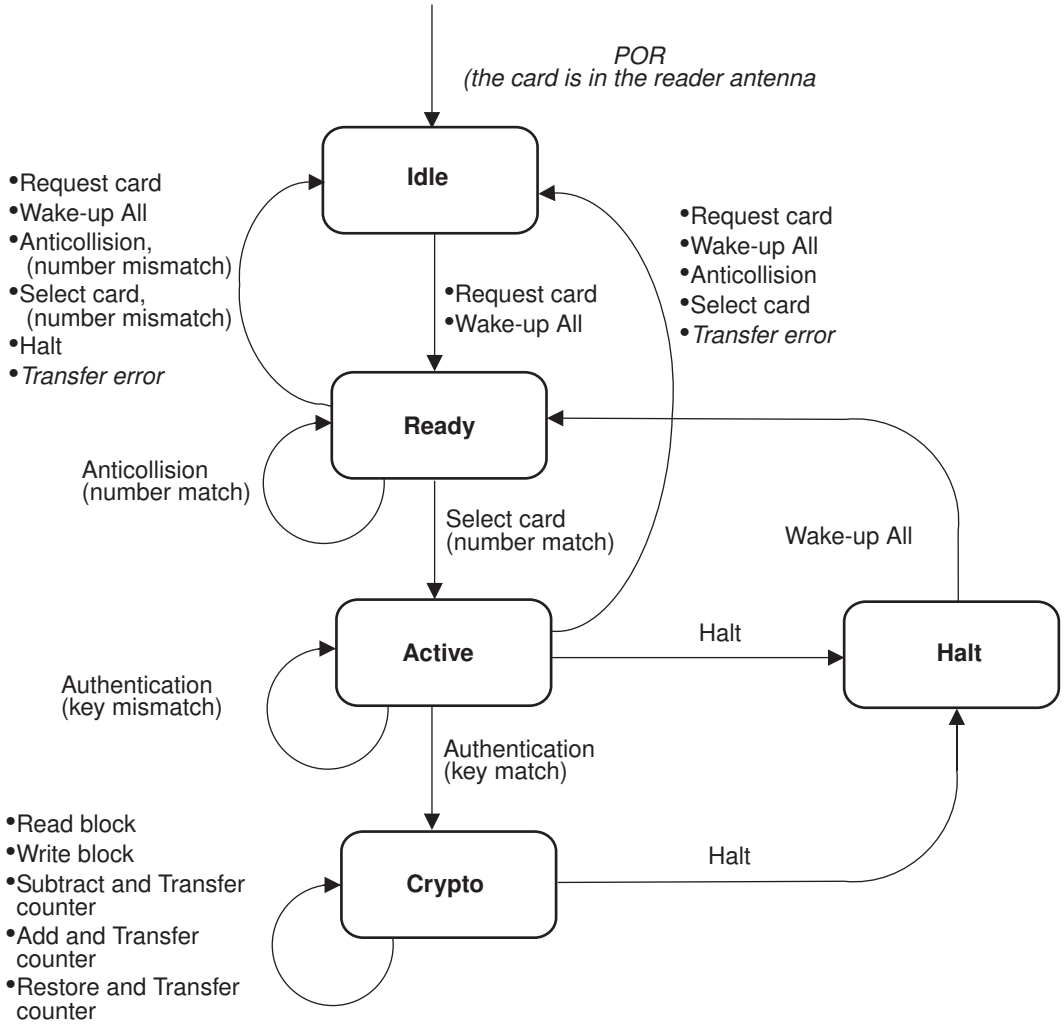
Table 1. UNC20C01R Command Set

Num.	Name	Mnemonics	Code (hex)
1	Request card	REQ	26h
2	Wake-up All	WUP	52h
3	Anticollision	ACOL	93h
4	Select card	SEL	93h
5	Authentication with key A	AUT_A	60h
6	Authentication with key B	AUT_B	61h
7	Read block	READ	30h
8	Write block	WRITE	A0h
9	Restore counter	REST	C2h
10	Add to counter	ADD	C1h
11	Subtract from counter	SUB	C0h
12	Transfer counter	TRANS	B0h
13	Halt	HLT	50h

To operate the UNC20C01R IC card, the reader uses a command set listed in Table 1.

Any command (the majority of them are followed by additional information) are transmitted by the reader for all cards present in its antenna field. According to its state, every card ignores the command or

responds to it, i.e. performs a required operation and, as a rule, sends feedback information to the reader. Available card states and their change logic are illustrated by a status graph shown in Fig. 2.



Legend: Card states are represented by nodes of the graph. The arcs indicate allowable transitions between states. Transitions from one state to another may be command-driven or event-driven. Events are shown by italics on arcs of the graph; commands are shown by normal font.

Fig. 2. A graph of UNC20C01R card states

- The card is driven to the Idle state immediately after the reader's antenna field energy becomes sufficient for powering the whole IC. After that the clock oscillator starts up and the reset generating circuit performs initial power-on reset of all card units. In the Idle state the card responds to only two commands.
- On receiving a “Request Card” or “Wake-up All” command, all cards that are in the Idle state go the Ready state. Cards in the Halt state may switch to the Ready state only by the “Wake-up All” command. The cards are held in the Ready state during the anticollision procedure when the reader defines the number of a card it will operate further. The procedure consists of consecutive issuing the “Anticollision” command until collision is not detected in any bit of the card serial number received by the reader. Cards whose numbers did not match with a portion of the number defined by the reader during a previous “Anticollision” command are automatically returned to the Idle

state and no longer participate in the anticollision procedure. Therefore, after a definite number of steps the reader leaves in the Ready state only one card that will be used for data exchange.

- The card whose number has been defined is driven by the reader from the Ready state to the Active state with a “Select Card” command. In this state a mutual three-pass authentication of the card and the reader is performed. During the authentication one of the two sector keys to run the application is used. If the authentication fails the card remains in the Active state.
- In case of successful authentication, the card passes to the cryptographic protection (“Crypto”) state. In this state the whole data exchange process is encrypted with a selected key and the application receives associated access to the information of the memory sector indicated during the above authentication.
- The exit from the Crypto and Active states is implemented by a “Halt” command after which the reader may start to process other cards held in the Idle state.

Memory Organization

1K byte of the non-volatile reprogrammable memory of the UNC20C01R IC is organized into 16 sectors 64 byte each. A sector, in its turn, is divided into four 16-byte blocks.

The last block of every sector stores housekeeping data defining conditions and modes for access to the sector information. This block is referred to as the sector trailer.

The card memory structure is shown in Fig. 3.

sector 0	block 0	Manufacturer’s info
	block 1	data
	block 2	data
	block 3	sector trailer
sector1	block 0	data
	block 1	data
	block 2	data
	block 3	sector trailer
sector 2	block 0	data
	block 1	data
	block 2	data
	block 3	
sector 15	block 1	data
	block 2	data
	block 3	sector trailer

Fig, 3. Card memory organization

The sector trailer stores keys used for the authentication procedure and secure data transfers between the reader and a card sector. The trailer houses access code bits to access individual sector blocks. Besides, the trailer contains a byte to store additional information defined by the application.

The sector trailer organization is shown in Fig. 4.

Any sector is accessed using a mandatory key A and an optional key B. When key B is not needed the memory allocated for it may be used to store any other information.

The access codes determine the reader’s ability to read and write blocks as well as handle counters stored in blocks (“Restore”, “Subtract”, “Add” and “Transfer” commands). Each sector block has a three-bit access code. Each code bit is represented twice in the sector trailer: by a non-inverted value and an

bytes	bits							
	7	6	5	4	3	2	1	0
0	Key A (48 bits)							
1								
2								
3								
4								
5								
6	ic32	ic22	ic12	ic02	ic31	ic21	ic11	ic01
7	c31	c21	c11	c01	ic33	ic23	ic13	ic03
8	c33	c23	c13	c03	c32	c22	c12	c02
9	Additional data area (byte)							
10	Optional key B (48 bits) or additional data area							
11								
12								
13								
14								
15								

Legend:
cYZ —access code bit Z (Z=1…3) for access to block Y(Y=0…3) of the current sector
icYZ —inverted access code bit Z (Z=1…3) for access to block Y (Y=0…3) of the current sector
Notes:
1. Each of the four blocks has its own access code consisting of 3 bits
2. Taking into account the finite number of memory re-programming cycles and to increase the storage reliability, different access code bits for the same block are distributed among different trailer bytes. Moreover, the same bit is represented twice in the trailer: as a non-inverted bit and an inverted bit.

Fig. 4. Structure of a trailer (the last sector block)

inverted value. Access code bits for the same block are stored in different bytes of the trailer. All these security measures take into account technological features of the reprogrammable memory of the card and have been adopted to increase the reliability of access code storage. The coinciding non-inverted and inverted values of the same bit point to a failure of the reprogrammable card memory in which case the application should change the sector or reject the whole card.

Access code values are listed in Tables 2 and 3.

On changing access codes, new codes become active after they have been written into the memory. Every time the reader accesses to card the card checks the codes stored in the memory and makes a request in compliance with them.

Important! An error in writing access codes into the trailer may result in the loss of access to the block making it impossible to correct the error. In this case either another block or another card will have to be used because the corrupted card cannot be restored. Therefore, in all access code change operations the card should by all means stay in the reader's antenna field area to avoid errors in executing a write operation and potential card damage.

Table 2. Access codes for sector data blocks

cY1	cY2	cY3	Read	Write	Add	Restore, Subtract, Transfer
0	0	0	keys A or B	keys A or B	keys A or B	keys A or B
0	0	1	keys A or B	never	never	keys A or B
0	1	0	keys A or B	never	never	never
0	1	1	key B	key B	never	never
1	0	0	keys A or B	key B	never	never
1	0	1	key B	never	never	never
1	1	0	keys A or B	key B	key B	keys A or B
1	1	1	never	never	never	never

Legend:
Y — number of a data block (0…2) the access code refers to.

Notes:
1. If key B can be read from the trailer of a sector associated with the data block (access codes 000, 001 and 010 in Table 3), then it makes no sense to use it for authentication since in this case all subsequent operations on data blocks of the requested sector will be ignored by the card.
2. Block 0 of sector 0 is accessible only for reading; all other operations on it are forbidden. It holds true irrespective of the value of an access code associated with it.

Table 3. Access codes for sector trailer

c31	c32	c33	Key A (bytes 0…5)		Access codes (bytes 6…9)		Key B (bytes 10…15)	
			Read	Write	Read	Write	Read	Write
0	0	0	never	key A	key A	never	key A	key A
0	0	1	never	key A	key A	key A	key A	key A
0	1	0	never	never	key A	never	key A	never
0	1	1	never	key B	key A or B	key B	never	key B
1	0	0	never	key B	key A or B	never	never	key B
1	0	1	never	never	key A or B	key B	never	never
1	1	0	never	never	key A or B	never	never	never
1	1	1	never	never	key A or B	never	never	never

Notes:
1. Other commands (“Add”, “Subtract”, “Restore” and “Transfer”) are forbidden for the trailer.
2. If key B can be read (access codes 000, 001 and 010), it implies using the memory area of key B for data storage, therefore authentication with this key has no sense since all subsequent operations on the current sector blocks (including the trailer) will be ignored by the card
3. When the trailer is read, bytes that are forbidden for reading (key A always and key B only at access codes 011…111), will be read as zeros.

IC Memory Contents at Chip Delivery

The zero block of the zero sector stores the manufacturer's information, e.g. the unique serial number of the card. This block is accessible only for reading, regardless the state of access codes. The structure of the zero block of the zero sector is shown in Fig. 5.

bytes	bits							
	7	6	5	4	3	2	1	0
0	4 bytes of unique serial card number							
1								
2								
3								
4	check byte of serial number							
5	special information							
6								
14	at manufacturer's option							
15								

Note:
The check byte is obtained through a bitwise "Exclusive OR" operation on all 4 bytes of the serial number

Fig. 5. Structure of the manufacturer's data block (block 0 of sector 0)

Sector trailers at the moment of chip delivery contain a secret transport key A (bytes 0...5) known only to the manufacturer and a card user.

Bytes 6, 7 and 8 have hex values FFh, 07h, 80h written into them, which corresponds to access codes 000 for data blocks (0...2) and to access code 001 for the trailer itself.

The contents of bytes 9...15 of the trailer are not defined at chip delivery (bytes may have random values).

Therefore, the user is allowed all operations on data blocks of a "clean card", provided he knows the transport key A, while for the trailers change of key A is permitted along with reading and writing access codes and key B. This makes it possible for the user to set his own values of the keys, access codes as well as to write needed information into data blocks after receiving the card.

Contact information:

Unicore Microsystems LLC

Phone: +7 495 739 02 53

Fax: +7 495 739 02 54

E-mail: office@unicore.ru

Web-site: www.unicore.ru