Description

BL75R06SM Contactless smart card chip consists of the RF-Interface, the Digital Control Unit and the 8 Kbit EEPROM. Operating distance is up to 10cm(depending on antenna geometry). The communication layer complies to parts 2 and 3 of the ISO/IEC 14443A standard. The chip supports PHILIPS's MIFARE card reader. It can be used for ticketing systems in public transport and comparable applications.

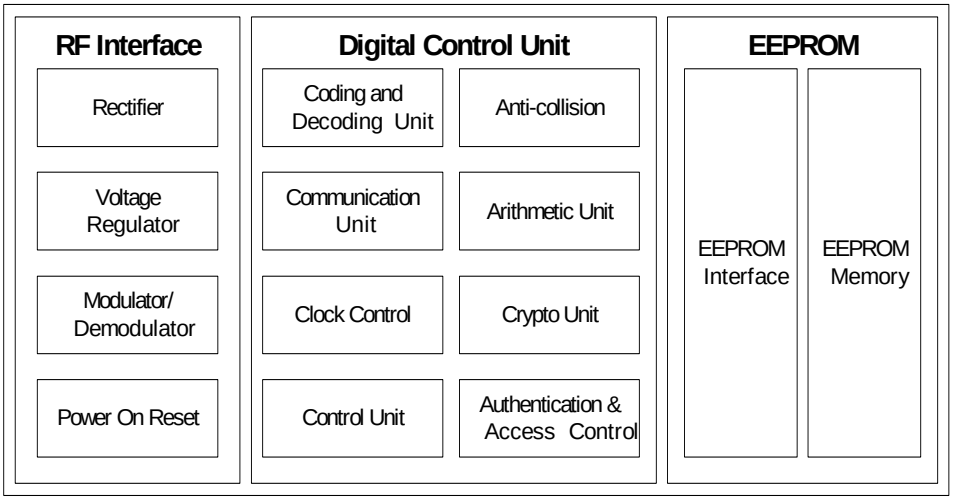
Features

- RF interface : ISO/IEC 14443 Type A
- Operating frequency : 13.56 MHz
- Fast data transfer : 106 kbit/s
- Memory size : 8 Kbit
- No battery needed : contactless transmission of data and supply energy
- Anti-collision : allows to operate more than one card in the field simultaneously
- Operating distance : Up to 100mm (depending on antenna geometry)
- Transaction possible with moving card
- Half-duplex communication protocol using handshake
- Following mechanisms are implemented in the contactless communication link between RWD and card to ensure very reliable data transmission :
  --- Anti-collision mechanism
  --- 16 bits CRC pre 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)
- Offer multi-application functionality
  --- 8 K-bit EEPROM（16 Sectors×4 Blocks×16 Bytes×8 Bit）
  --- Organised in securely separated 16 sectors supporting multi-application use
  --- each sector consists of 4 blocks
  --- A block is the smallest part to be addressed and consists of 16 bytes
  --- Individual set of two keys per sector(per application)
  --- User definable access conditions for each memory block
  --- Arithmetic : increment and decrement
- Data retention of 10 years
- Write endurance 100,000 cycles
- Typical operation parameter :
  --- Anti-collision time : 3.0ms + 1.0ms
  --- Authentication : 2.0ms
  --- Read block : 2.5ms
  --- Write block : 6.0ms
  --- Transfer : 4.5ms
- Typical ticketing transaction : < 100ms
  Identification of card + 6 Blocks read (768 bit, 2 Sector Authentication) + 2 Blocks write(256bit) with Backup

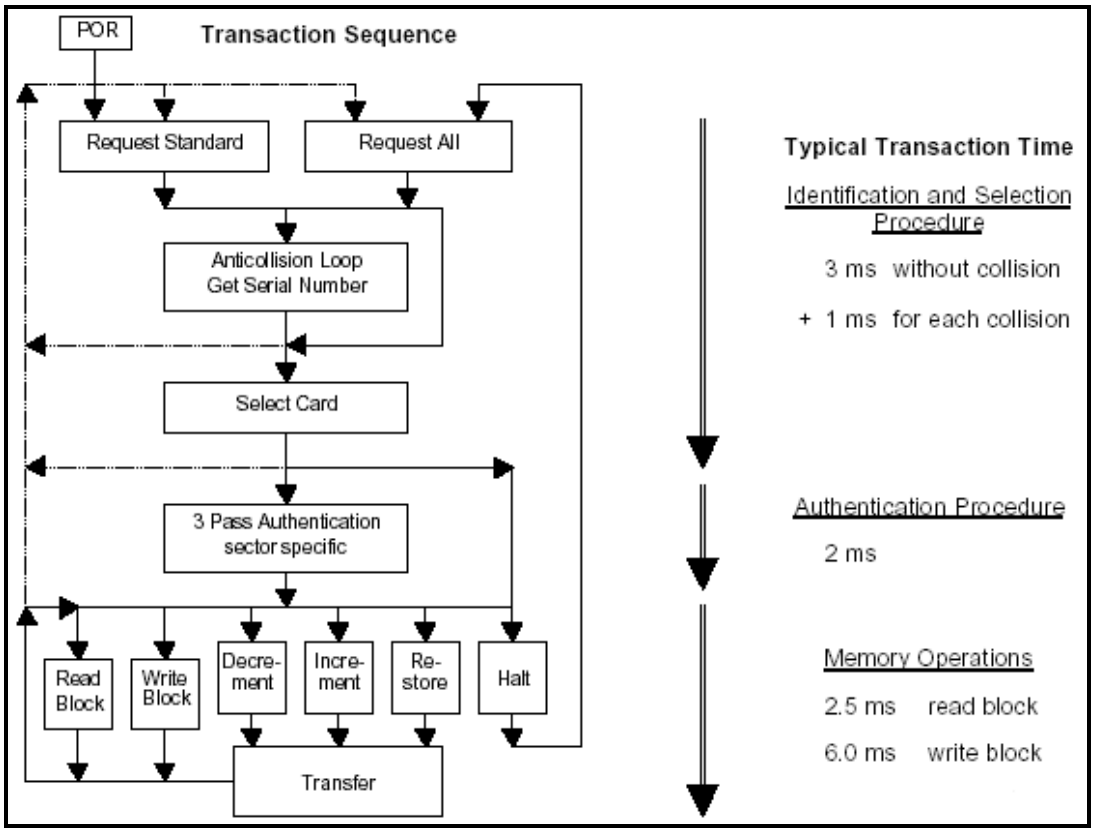
Functional Description

Block Diagram

BL75R06SM Contactless smart card IC consists of the RF-Interface, the Digital Control Unit and the 8 Kbit EEPROM, as show in the below figure:



Transaction Sequence Diagram



Commands

The BL75R06SM RFID ICs support the following commands:

1 Request Standard / All

After Power On Reset (POR) of a card it can answer to a request command - sent by the RWD to all cards in the antenna field - by sending the answer to request code (ATQA according to ISO/IEC 14443A).

2 Anticollision Loop

In the anticollision loop the serial number of a card is read. If there are several cards in the operating range of the RWD, they can be distinguished by their unique serial numbers and one can be selected (select card) for further transactions. The unselected cards return to the standby mode and wait for a new request command.

3 Select Card

With the select card command the RWD selects one individual card for authentication and memory related operations. The card returns the Answer To Select(ATS) code (= 08h), which determines the type of the selected card.

4 3 Pass Authentication

After selection of a card the RWD specifies the memory location of the following memory access and uses the corresponding key for the 3 pass authentication procedure. After a successful authentication all memory operations are encrypted.

5 Memory Operations

After authentication any of the following operations may be performed:

Read block

Write block

Decrement: Decrements the contents of a block and stores the result in a temporary internal data-register

Increment: Increments the contents of a block and stores the result in the data-register

Restore: Moves the contents of a block into the data-register

Transfer: Writes the contents of the temporary internal data-register to a value block

Data Integrity

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

- 16 bits CRC per block
- Parity bits for each byte

Security

To provide a very high security level a three pass authentication according to ISO 9798-2 is used.

Three Pass Authentication Sequence

a. The RWD specifies the sector to be accessed and chooses key A or B.
b. The card reads the secret key and the access conditions from the sector trailer. Then the card sends a random number as the challenge to the RWD (pass one).
c. The RWD calculates the response using the secret key and additional input. The

response, together with a random challenge from the RWD, is then transmitted to the card (pass two).

d. The card verifies the response of the RWD by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).

e. The RWD verifies the response of the card by comparing it to its own challenge.

After transmission of the first random challenge the communication between card and RWD is encrypted.

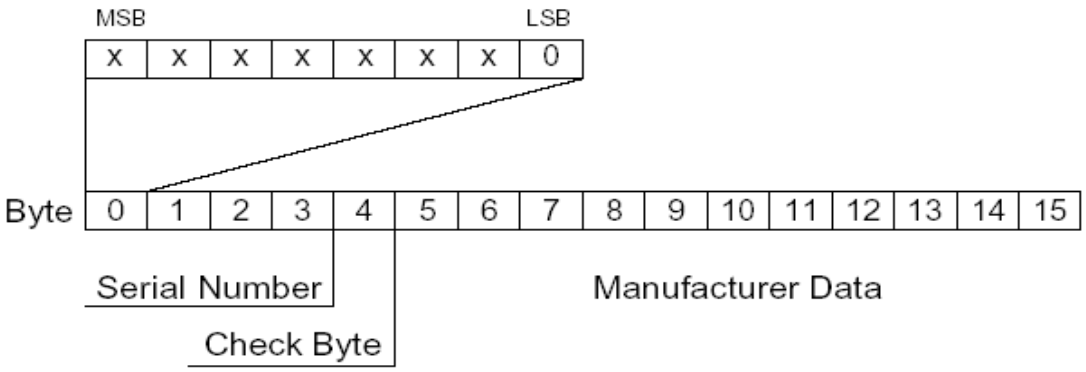
Memory Organisation

The 1024 x 8 bit EEPROM memory is organized in 16 sectors with 4 blocks of 16 bytes each. In the erased state the EEPROM cells are read as a logical “0”, in the written state as a logical “1”.

		Byte Number within a Block															
Sector	**Block**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	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

1 Manufacturer Block

This is the first data block (block 0) of the first sector (sector 0).It contains the IC manufacturer data. Due to security and system requirements this block is write protected after having been programmed by the IC manufacturer at production.



2 Data Blocks

All sectors contain 3 blocks of 16 bytes for storing data (Sector 0 contains only two data blocks and the read-only manufacturer block).

The data blocks can be configured by the access bits as

- read/write blocks for e.g. contactless access control or
- value blocks for e.g. electronic purse applications, where additional commands like increment and decrement for direct control of the stored value are provided.

An authentication command has to be carried out before any memory operation in order to allow further commands.

Value Blocks

The value blocks allow to perform electronic purse functions (valid commands*: read, write, increment, decrement, restore, transfer*). The value blocks have a fixed data format which permits error detection and correction and a backup management. A value block can only be generated through a *write* operation in the value block format:

- Value: Signifies a signed 4-byte value. The lowest significant byte of a value is stored in the lowest address byte. Negative values are stored in standard 2´s complement format. For reasons of data integrity and security, a value is stored three times, twice non-inverted and once inverted.
- Adr: Signifies a 1-byte address, which can be used to save the storage address of a block, when implementing a powerful backup management. The address byte is stored four times, twice inverted and non-inverted. During *increment, decrement, restore* and *transfer* operations the address remains unchanged. It can only be altered via a *write* command.

Byte Number Description

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Value				Value				Value				Adr	$\overline{\text{Adr}}$	Adr	$\overline{\text{Adr}}$

3 Sector Trailer (Block 3)

Each sector has a sector trailer containing the secret keys A and B(optional), which return logical “0”s when read and the access conditions for the four blocks of that sector, which are stored in bytes 6...9. The access bits also specify the type (read/write or value) of the data

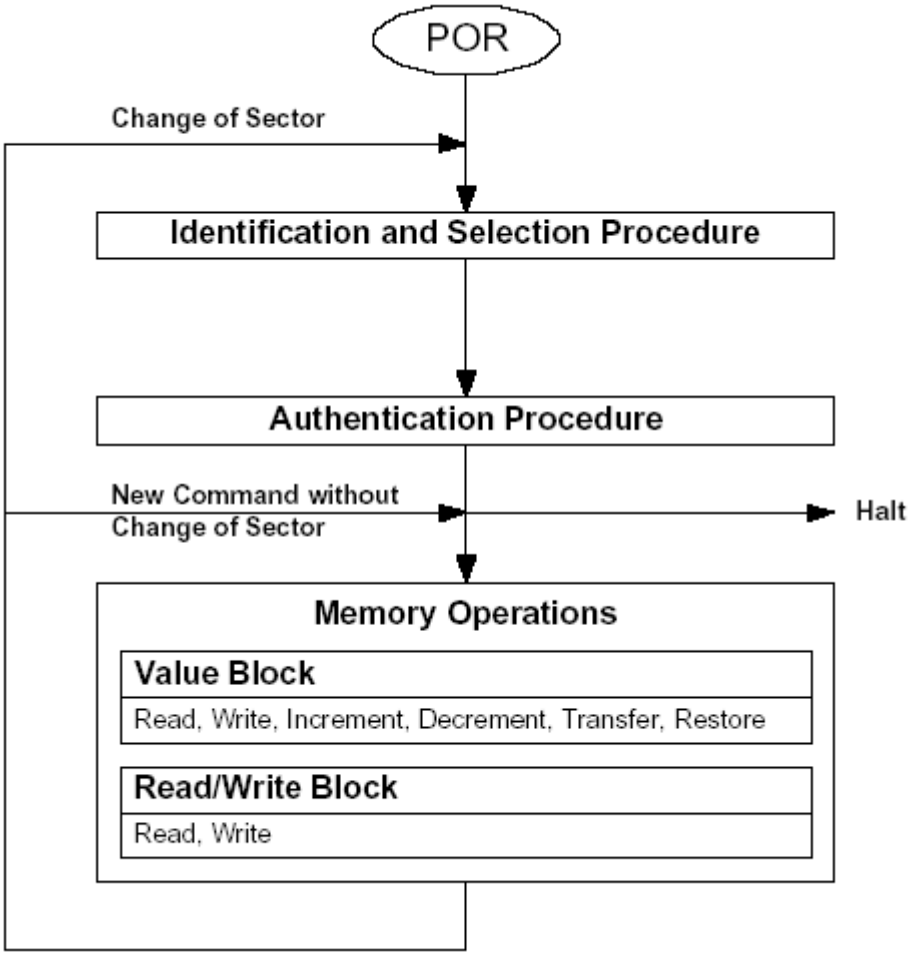
blocks.

If key B is not needed, the last 6 bytes of block 3 can be used as data bytes. Byte 9 of the sector trailer is available for user data. For this byte apply the same access rights as for byte 6, 7 and 8.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Key A						Access Bits				Key B (optional)					

Memory Access

Before any memory operation can be carried out, the card has to be selected and authenticated as described previously. The possible memory operations for an addressed block depend on the key used and the access conditions stored in the associated sector trailer.



Memory Operations		
Operation	**Description**	**Valid for Block Type**
Read	reads one memory block	read/write, value and sector trailer
Write	writes one memory block	read/write, value and sector trailer
Increment	increments the contents of a block and stores the result in the internal data register	value
Decrement	decrements the contents of a block and stores the result in the internal data register	value
Transfer	writes the contents of the internal data register to a block	value
Restore	reads the contents of a block into the internal data register	value

1 Access Conditions

The access conditions for every data block and sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector.

The access bits control the rights of memory access using the secret keys A and B. The access conditions may be altered, provided one knows the relevant key and the current access condition allows this operation.

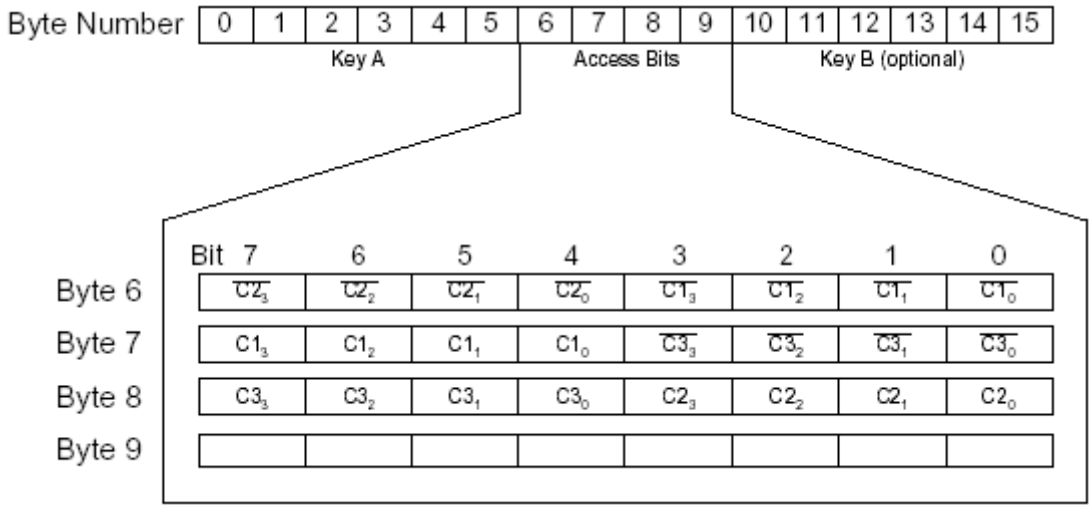
Access Bits	Valid Commands		Block	Description
$C1_3\,C2_3\,C3_3$	read, write	→	3	sector trailer
$C1_2\,C2_2\,C3_2$	read, write, increment, decrement, transfer, restore	→	2	data block
$C1_1\,C2_1\,C3_1$	read, write, increment, decrement, transfer, restore	→	1	data block
$C1_0\,C2_0\,C3_0$	read, write, increment, decrement, transfer, restore	→	0	data block

Note: In the following description the access bits are mentioned in the non-inverted mode only. The internal logic of the BL75R06SM ensures that the commands are executed only after an authentication procedure or never.

2 Access Conditions For The Sector Trailer

Depending on the access bits for the sector trailer (block 3) the read/write access to the keys and the access bits is specified as ‘never’, ‘key A’, ‘key B’ or key A|B’ (key A or key B).

On chip delivery the access conditions for the sector configuration, new cards must be authenticated with key A. Since the access bits themselves can also be blocked, special care should be taken during personalization of cards.



Note: With each memory access the internal logic verifies the format of the access conditons. If it detects a format violation the whole sector is irreversible blocked.

Access bits			Access condition for						Remark
			KEYA		Access bits		KEYB		
C1	C2	C3	read	write	read	write	read	write	
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	key B	
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, transport 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: the grey marked lines are access conditions where key B is readable and may be used for data. trailers and key A are predefined as transport configuration. Since key B may be read in transport.

3 Access Conditions For Data Blocks

Depending on the access bits for data blocks (blocks 0...2) the read/write access is specified as ‘never’, ‘key A’, ‘key B’ or ‘key A|B’ (key A or key B). The setting of the relevant access bits defines the application and the corresponding applicable commands.

- Read/write block: The operations read and write are allowed.
- Value block: Allows the additional value operations *increment, decrement, transfer und restore*.

In one case ('001') only *read* and *decrement* are possible for a non-rechargeable card. In the other case ('110') recharching is possible by using key B.

- Manufacturer block: The read-only condition is not affected by the access bits setting.
- Key management: In transport configuration key A must be used for authentication[1].

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A|B[1]	key A|B[1]	key A|B[1]	key A|B[1]	transport configuration
0	1	0	key A|B[1]	never	never	never	read/write block
1	0	0	key A|B[1]	key B[1]	never	never	read/write block
1	1	0	key A|B[1]	key B[1]	key B[1]	key A|B[1]	value block
0	0	1	key A|B[1]	never	never	key A|B[1]	value block
0	1	1	key B[1]	key B[1]	never	never	read/write block
1	0	1	key B[1]	never	never	never	read/write block
1	1	1	never	never	never	never	read/write block

[1] if Key B may be read in the corresponding Sector Trailer it cannot serve for authentication (all grey marked lines in previous table).

Consequences: If the RWD tries to authenticate any block of a sector with key B using grey marked access conditions, the card will refuse any subsequent memory access after authentication.