SP_MF-1K, Mifare Classic1K

SP_MF-1K, Mifare Classic 1K- Mainstream contactless smart card

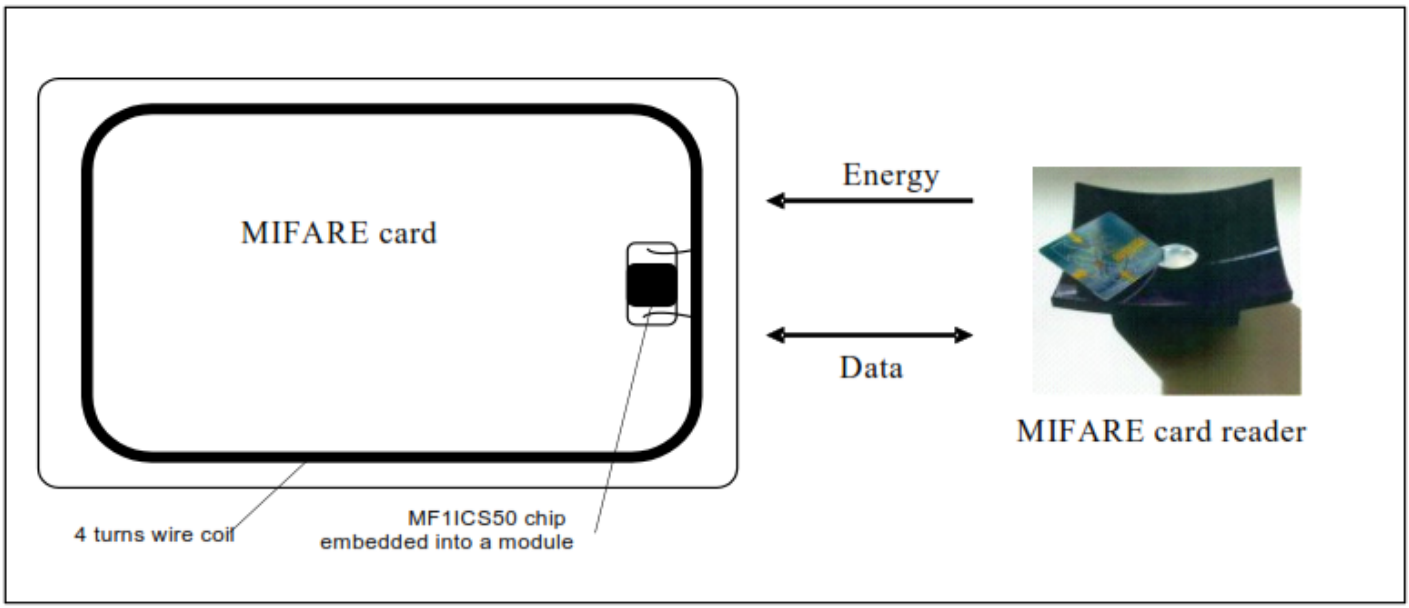
The MIFARE MF1ICS50 IC is used in applications like public transport ticketing where major cities have adopted MIFARE as their e-ticketing solution of choice.

Key applications

- Public transportation
- Access control
- Event ticketing
- Gaming & identity

Anticollision

An intelligent anticollision function allows to operate more than one card in the field simultaneously.
The anticollision algorithm selects each card individually and ensures that the execution of a transaction with a selected card is performed correctly without data corruption resulting from other cards in the field.



SP_MF-1K, Mifare Classic1K

Simple integration and user convenience

The SP_MF 1k is designed for simple integration and user convenience.
Which could allow complete ticketing transactions to be handled in less than 100 ms. Thus, the SP_MF 1k card user is not forced to stop at the reader leading to a high throughput at gates and reduced boarding times onto busses.
The MIFARE card may also remain in the wallet during the transaction, even if there are coins in it.

Security

Mutual three pass authentication (ISO/IEC DIS 9798-2)
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy
- Unique serial number for each device

Delivery options

- Die on wafer
- Bumped die on wafer
- MOA4 or MOA2 contactless card module
- Flip chip package

MIFARE, RF Interface (ISO/IEC 14443 A)

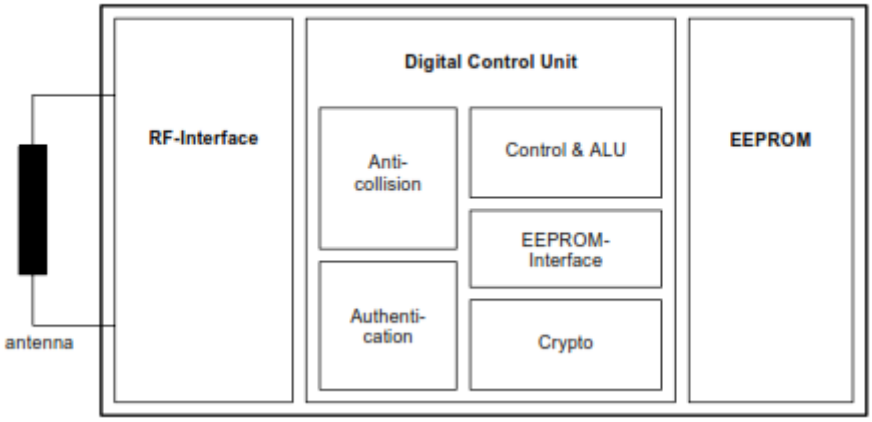
Contactless transmission of data and supply energy (no battery needed)
Operating distance: Up to 100mm (depending on antenna geometry)
Operating frequency: 13.56 MHz
Data transfer: 106 kbit/s
Data integrity: 16 Bit CRC, parity, bit coding, bit counting
Anticollision
Typical ticketing transaction: < 100 ms

EEPROM

1 Kbyte, organized in 16 sectors with 4 blocks of 16 bytes each (one block consists of 16 byte)
User definable access conditions for each memory block
Data retention of 10 years.
Write endurance 100.000 cycles

SP_MF-1K, Mifare Classic1K

Block diagram



Block description

The SP_MF chip consists of the 1 Kbyte EEPROM, the RF-Interface and the Digital Control Unit.
Energy and data are transferred via an antenna, which consists of a coil with a few turns directly connected to the MF1ICS50.
No further external components are necessary. • RF-Interface:
– Modulator/Demodulator
– Rectifier
– Clock Regenerator
– Power On Reset
– Voltage Regulator
• Anticollision: Several cards in the field may be selected and operated in sequence
• Authentication: Preceding any memory operation the authentication procedure ensures that access to a block is only possible via the two keys specified for each block
• Control & Arithmetic Logic Unit: Values are stored in a special redundant format and can be incremented and decremented
• EEPROM-Interface
• Crypto unit: The CRYPTO1 stream cipher of the MF1ICS50 is used for authentication and encryption of data exchange.
• EEPROM: 1 Kbyte is organized in 16 sectors with 4 blocks each. A block contains
16 bytes.
The last block of each sector is called “trailer”, which contains two secret keys and programmable access conditions for each block in this sector.

SP_MF-1K, Mifare Classic1K

Communication principle

The commands are initiated by the reader and controlled by the Digital Control Unit of the SP_MF 1k according to the access conditions valid for the corresponding sector.

Request standard/ all

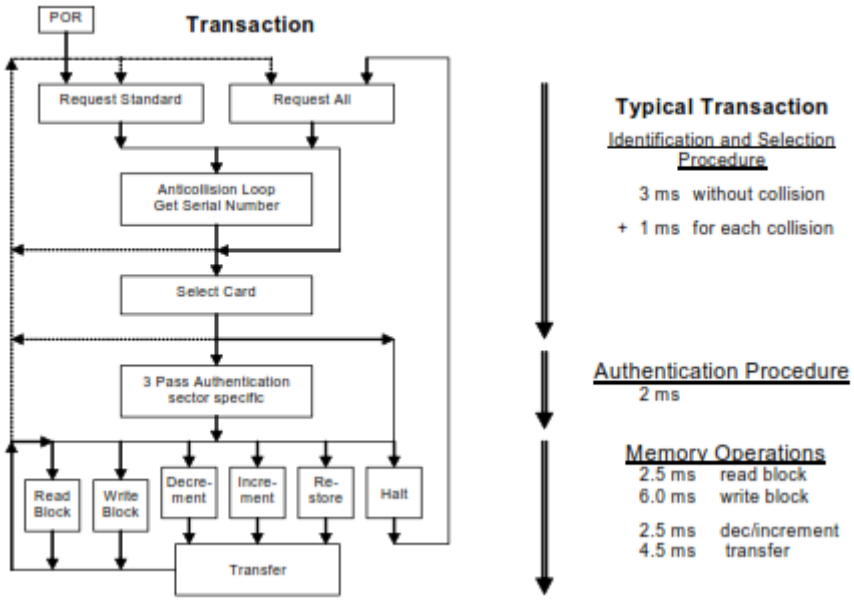
After Power On Reset (POR) of a card it can answer to a request command - sent by the reader to all cards in the antenna field - by sending the answer to request code

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 reader, 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.

Select card

With the select card command the reader 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.



SP_MF-1K, Mifare Classic1K

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 reader and card to ensure very reliable data transmission:

- 16 bits CRC per 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)

Three pass authentication sequence

1. The reader specifies the sector to be accessed and chooses key A or B.
2. 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 reader (pass one).
3. The reader calculates the response using the secret key and additional input. The response, together with a random challenge from the reader, is then transmitted to the card (pass two).
4. The card verifies the response of the reader by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).
5. The reader 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 reader is encrypted.

SP_MF-1K, Mifare Classic1K

RF interface

The RF-interface is according to the standard for contactless smart cards ISO/IEC 14443 A.
The carrier field from the reader is always present (with short pauses when transmitting),
because it is used for the power supply of the card.
For both directions of data communication there is only one start bit at the beginning of each frame.
Each byte is transmitted with a parity bit (odd parity) at the end.
The LSB of the byte with the lowest address of the selected block is transmitted first.
The maximum frame length is 163 bits (16 data bytes + 2 CRC bytes = 16 * 9 + 2 * 9 + 1 start bit).

Memory organization

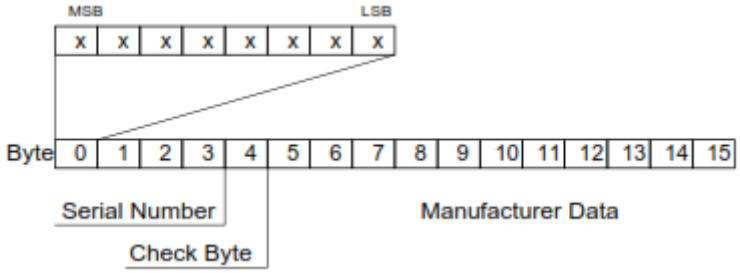
The 1024 x 8 bit EEPROM memory is organized in 16 sectors with 4 blocks of 16 bytes each.
In the erased state the EEPROM cells are read as a logical “0”, in the written state as a logical “1”.

		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

SP_MF-1K, Mifare Classic1K

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.



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.

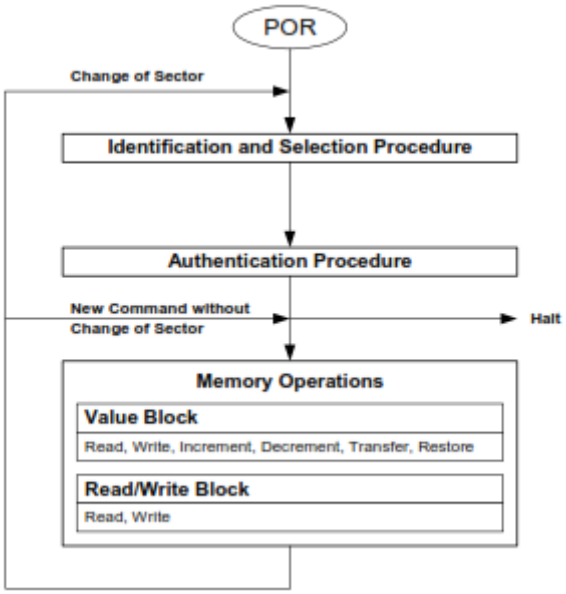
Value Blocks

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 man~~ agement.
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.

SP_MF-1K, Mifare Classic1K

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.



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.
Remark: With each memory access the internal logic verifies the format of the access conditions.
If it detects a format violation the whole sector is irreversible blocked.
Remark: In the following description the access bits are mentioned in the non-inverted mode only.

SP_MF-1K, Mifare Classic1K

Dimensions	5.40 x 8.57 x 0.084 cm
Operating frequency	13.56 MHz
Memory Size/ Application Areas	1 kB, organized in 16 sectors
Data retention	10 years
Write endurance	100000 cycles
Data transfer	106 kbit/s
Anti-collision	Yes