# MF1ICS50

## Functional specification

Rev. 5.5 — 14 December 2009
001055

Product data sheet
PUBLIC

## 1. General description

NXP has developed the MIFARE MF1ICS50 to be used in a contactless smart card according to ISO/IEC 14443 Type A.

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.

### 1.1 Key applications

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

### 1.2 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.

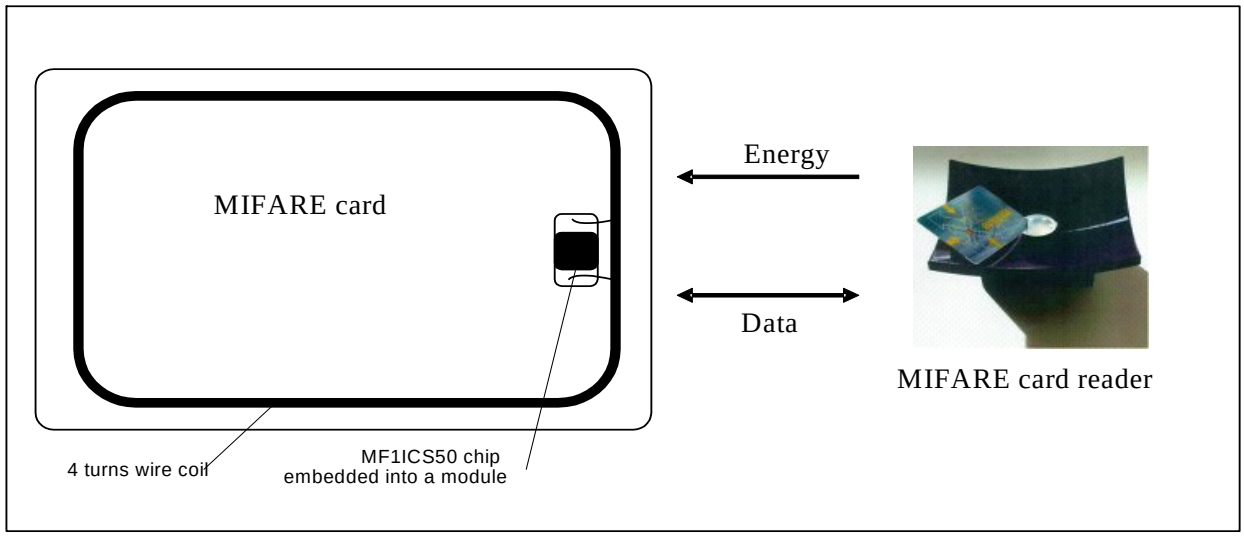


**Fig 1. MIFARE card reader**

founded by Philips

### 1.3 Simple integration and user convenience

The MF1ICS50 is designed for simple integration and user convenience. Which could allow complete ticketing transactions to be handled in less than 100 ms. Thus, the MF1ICS50 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.

### 1.4 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

### 1.5 Delivery options

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

## 2. Features

### 2.1 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 (including backup management)

### 2.2 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



© NXP B.V. 2009. All rights reserved.

# 3. Ordering information

See Delivery Type Addendum of Device

# 4. Block diagram

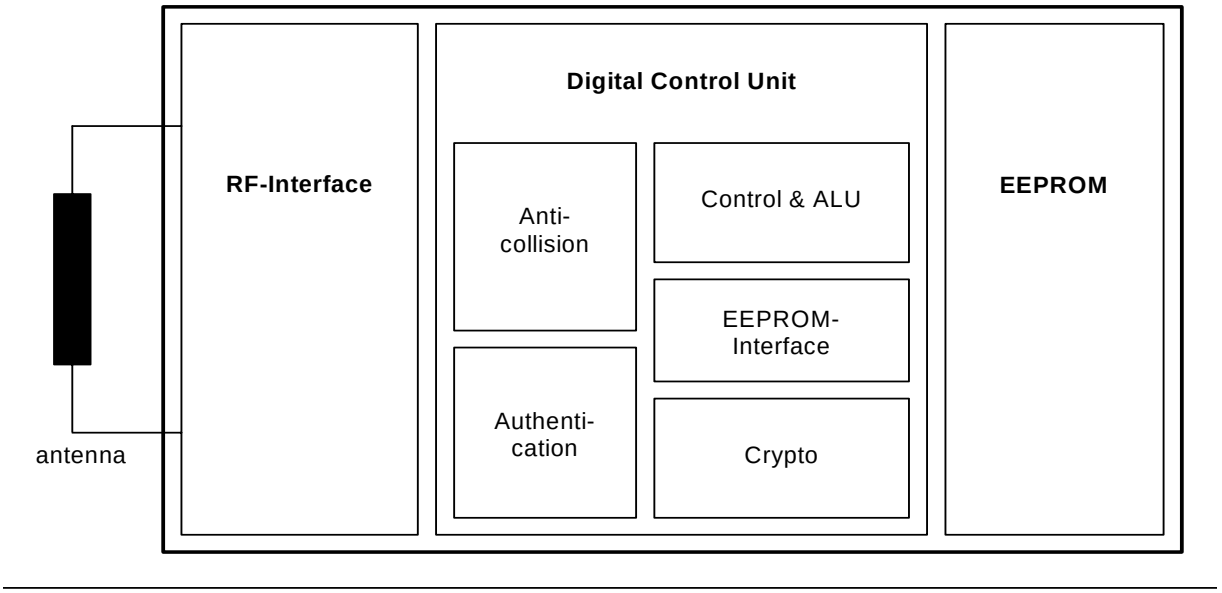


Fig 2. Block diagram

# 5. Pinning information

## 5.1 Pinning

See Delivery Type Addendum of Device



© NXP B.V. 2009. All rights reserved.

# 6. Functional description

## 6.1 Block description

The MF1ICS50 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. (For details on antenna design please refer to the document MIFARE, Card IC Coil Design Guide.)

- 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.

## 6.2 Communication principle

The commands are initiated by the reader and controlled by the Digital Control Unit of the MF1ICS50 according to the access conditions valid for the corresponding sector.

### 6.2.1 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 (ATQA according to ISO/IEC 14443A).

### 6.2.2 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 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.



© NXP B.V. 2009. All rights reserved.

### 6.2.3 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. Please refer to the document MIFARE, Standardized Card Type Identification Procedure for further details.

### 6.2.4 Three pass authentication

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

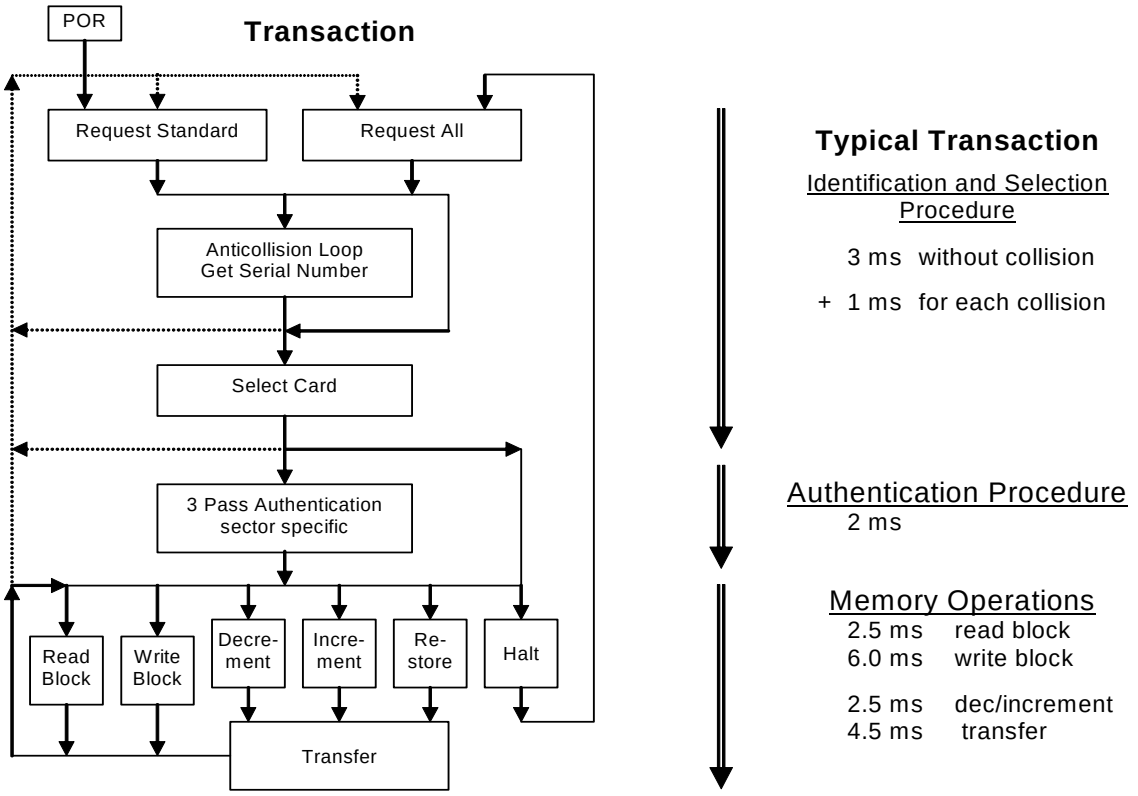


**Fig 3. Three pass authentication**



© NXP B.V. 2009. All rights reserved.

### 6.2.5 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

## 6.3 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)

## 6.4 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.



© NXP B.V. 2009. All rights reserved.

## 6.5 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).

## 6.6 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”.

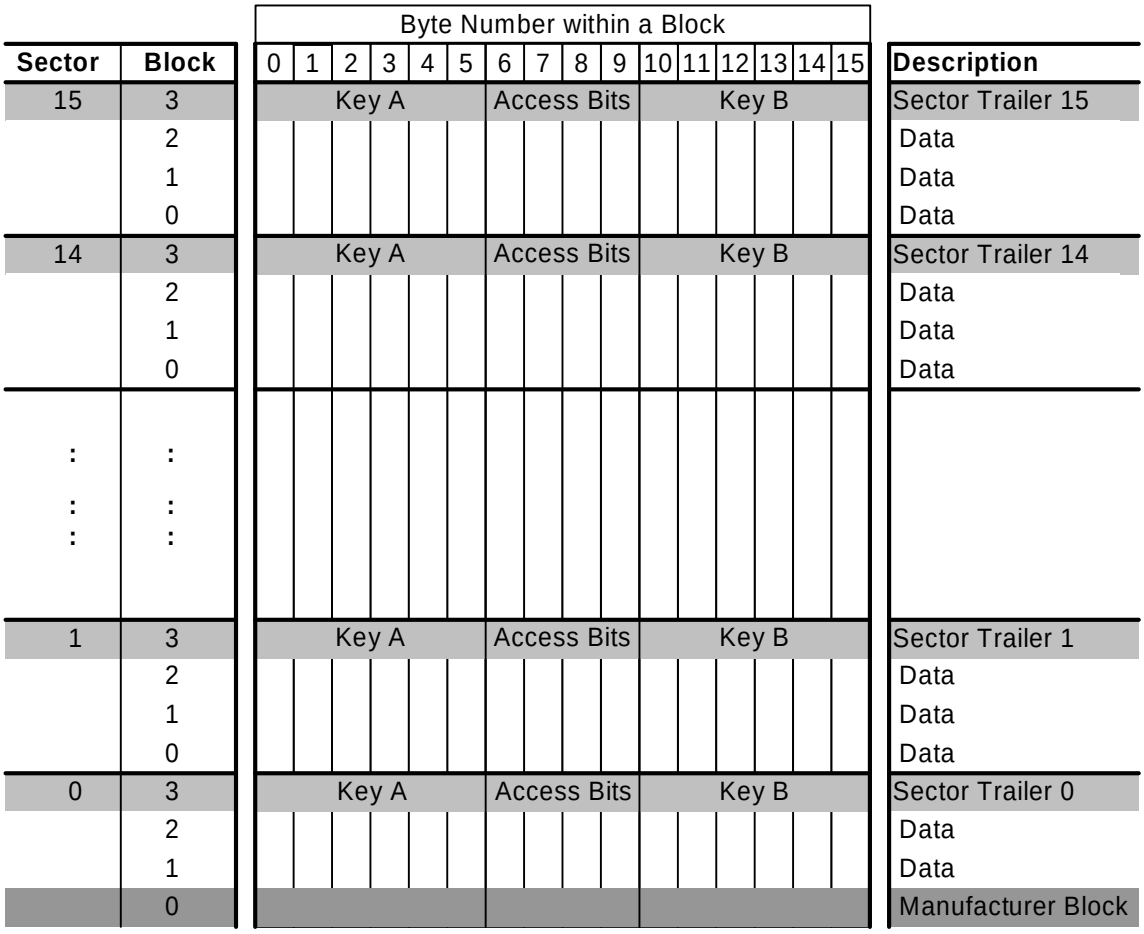


**Fig 4. Memory organization**



© NXP B.V. 2009. All rights reserved.

### 6.6.1 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.

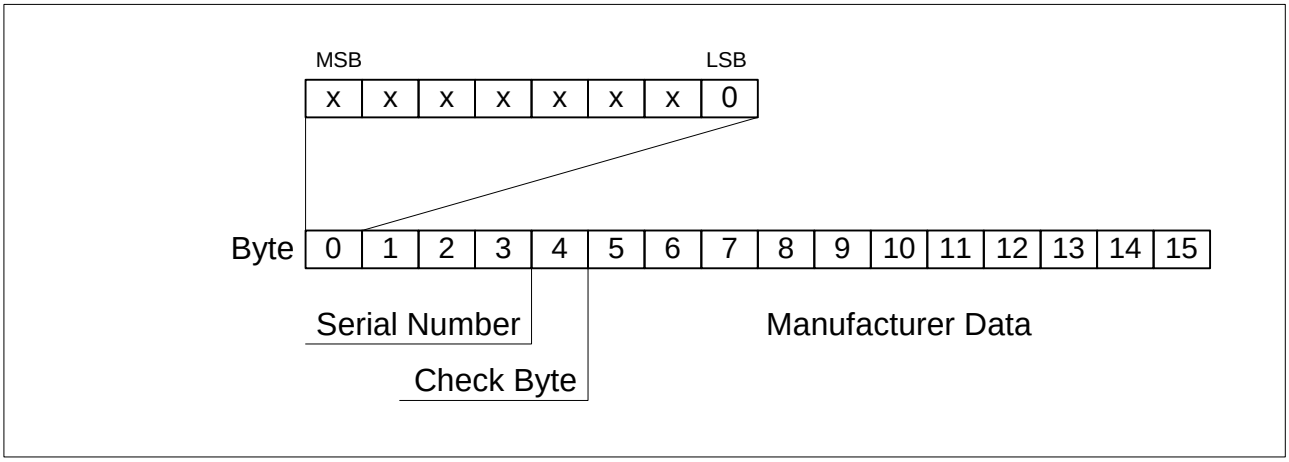


**Fig 5. Manufacturer block**

### 6.6.2 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.

#### 6.6.2.1 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.



© NXP B.V. 2009. All rights reserved.

- 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.

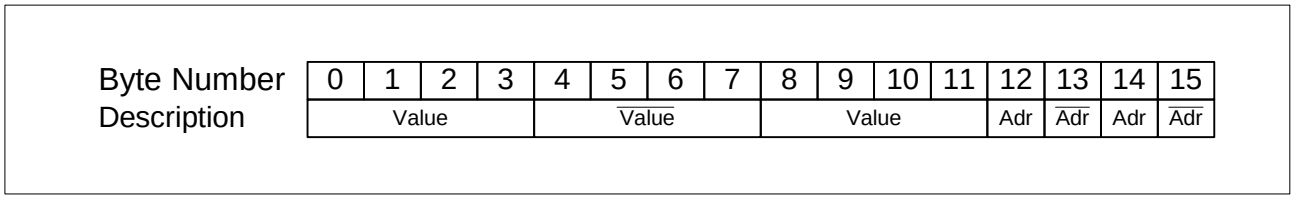


**Fig 6. Value blocks**

### 6.6.3 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 the same access rights as for byte 6, 7 and 8 apply.

All keys are set to $FFFFFFFFFFFF_h$ at chip delivery.

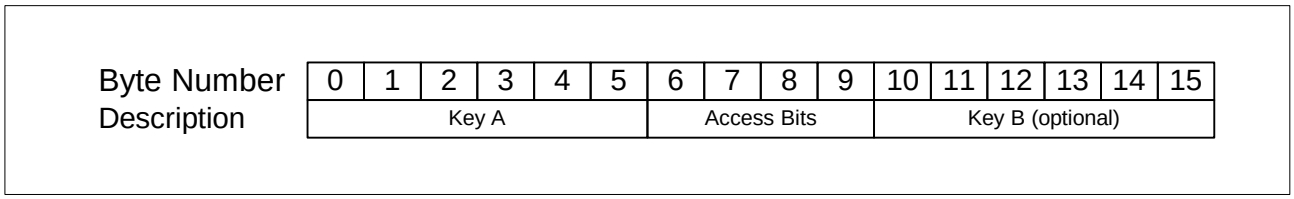


**Fig 7. Sector trailer**



© NXP B.V. 2009. All rights reserved.

## 6.7 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.

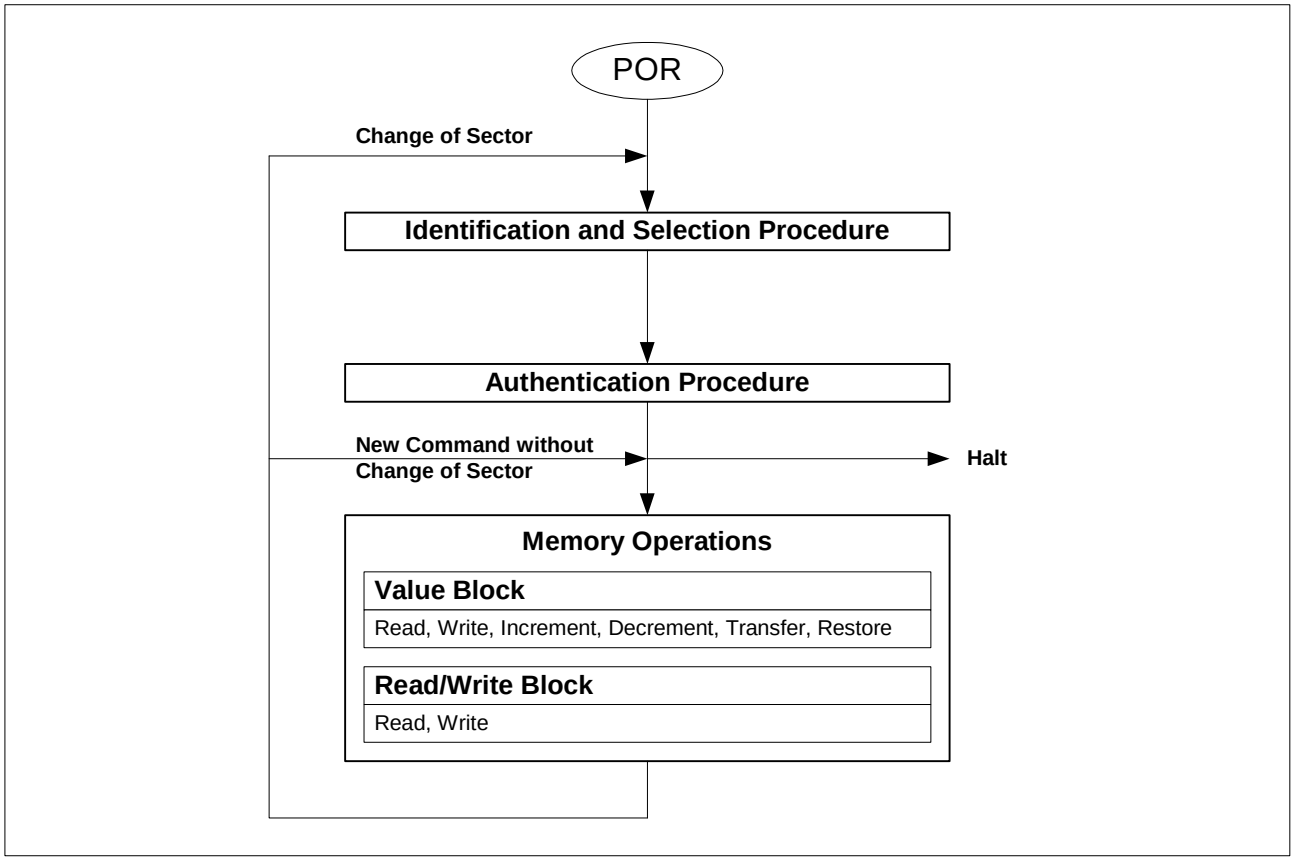


**Fig 8. Memory access**



© NXP B.V. 2009. All rights reserved.

**Table 1. 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 |



© NXP B.V. 2009. All rights reserved.

### 6.7.1 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.

**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.

The internal logic of the MF1ICS50 ensures that the commands are executed only after an authentication procedure or never.

**Table 2. Access conditions**

| 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 |

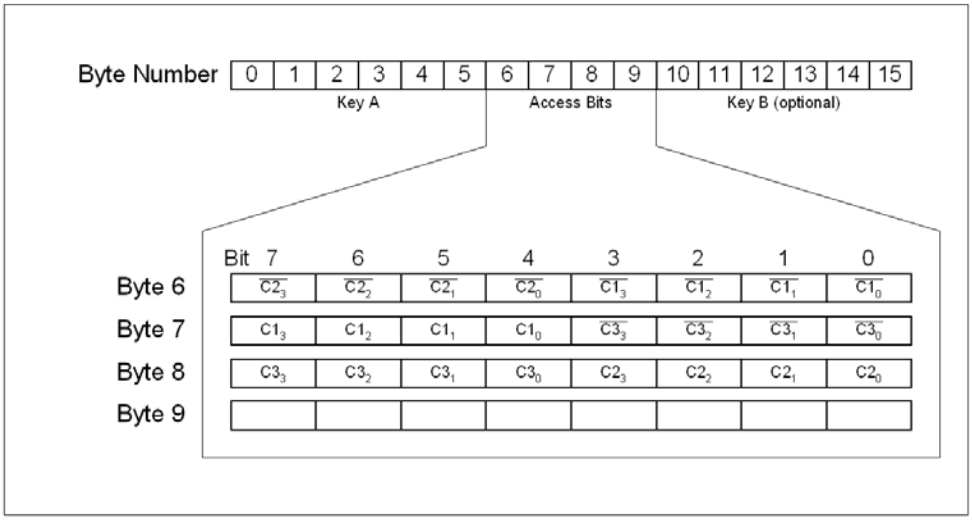


**Fig 9. Access conditions**



© NXP B.V. 2009. All rights reserved.

### 6.7.2 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 trailers and key A are predefined as transport configuration. Since key B may be read in transport 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.

**Table 3. Access conditions for the sector trailer**

| 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 | |

**Remark:** the grey marked lines are access conditions where key B is readable and may be used for data.



© NXP B.V. 2009. All rights reserved.

### 6.7.3 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 and restore. In one case (‘001’) only read and decrement are possible for a non-rechargeable card. In the other case (‘110’) recharging 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]

**Table 4. Access conditions for data blocks**

| Access bits | | | Access condition for | | | | Application |
|---|---|---|---|---|---|---|---|
| C1 | C2 | C3 | read | write | increment | decrement, transfer, restore | |
| 0 | 0 | 0 | key A\|B[1] | key A\|B1 | key A\|B1 | key A\|B1 | 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 reader 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.

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



© NXP B.V. 2009. All rights reserved.

## 7. Limiting values

See Delivery Type Addendum of Device

## 8. Recommended operating conditions

See Delivery Type Addendum of Device

## 9. Characteristics

See Delivery Type Addendum of Device

## 10. Package outline

See Delivery Type Addendum of Device



© NXP B.V. 2009. All rights reserved.

# 11. Revision history

**Table 5. Revision history**

| Document ID | Release date | Data sheet status | Change notice | Supersedes |
|---|---|---|---|---|
| 001055 | 20091214 | Product data sheet | | 001054 |
| Modifications: | • Section 6.6.3 “Sector trailer (block 3)”: added default key values<br>• Section 12.3 “Disclaimers”: added “Export control” | | | |
| 001054 | 20080819 | Product data sheet | | 001053 |
| Modifications: | Section 1 “General description” and Section 2 “Features”: rephrasing of sentences | | | |
| 001053 | 14 December 2009 | Product data sheet | | 001052 |
| Modifications: | • Update<br>• General rewording of MIFARE designation and commercial conditions | | | |
| 001052 | 15 January 2007 | Product data sheet | | 5.1 |
| Modifications: | • The format of this data sheet has been redesigned to comply with the new identity guidelines of NXP Semiconductors.<br>• Legal texts have been adapted to the new company name. | | | |



© NXP B.V. 2009. All rights reserved.

# 12. Legal information

## 12.1 Data sheet status

| Document status[1][2] | Product status[3] | Definition |
|---|---|---|
| Objective [short] data sheet | Development | This document contains data from the objective specification for product development. |
| Preliminary [short] data sheet | Qualification | This document contains data from the preliminary specification. |
| Product [short] data sheet | Production | This document contains the product specification. |

[1] Please consult the most recently issued document before initiating or completing a design.

[2] The term 'short data sheet' is explained in section "Definitions".

[3] The product status of device(s) described in this document may have changed since this document was published and may differ in case of multiple devices. The latest product status information is available on the Internet at URL http://www.nxp.com.

## 12.2 Definitions

**Draft —** The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

**Short data sheet —** A short data sheet is an extract from a full data sheet with the same product type number(s) and title. A short data sheet is intended for quick reference only and should not be relied upon to contain detailed and full information. For detailed and full information see the relevant full data sheet, which is available on request via the local NXP Semiconductors sales office. In case of any inconsistency or conflict with the short data sheet, the full data sheet shall prevail.

## 12.3 Disclaimers

**General —** Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information.

**Right to make changes —** NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

**Suitability for use —** NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage.

NXP Semiconductors accepts no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

**Applications —** Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

**Limiting values —** Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

**Terms and conditions of sale —** NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

**No offer to sell or license —** Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

**Export control —** This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from national authorities.

## 12.4 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

**MIFARE —** is a trademark of NXP B.V.

# 13. Contact information

For additional information, please visit: **http://www.nxp.com**

For sales office addresses, send an email to: **salesaddresses@nxp.com**



© NXP B.V. 2009. All rights reserved.

## 14. Tables



## 15. Figures



continued >>



© NXP B.V. 2009. All rights reserved.

## 16. Contents



Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

**© NXP B.V. 2009.** **All rights reserved.**

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

**Date of release: 14 December 2009**
**Document identifier: 001055**

founded by

PHILIPS