DATA SHEET

mifare®

Standard Card IC
MF1 IC S50
Functional Specification

Product Specification
Revision 4.0

July 1998

Philips Semiconductors

PHILIPS

Contents

MIFARE® is a registered trademark of Philips Electronics N.V.

1 General Description

The contactless MIFARE® 1 S50 smart card IC has been especially tailored to meet the requirements of a payment card which can be used for ticketing systems in public transport and comparable applications. MIFARE® 1 S50 IC is a true multi-application smart card IC with the functionality of a processor realised with hardwired logic.
Special emphasis has been placed on user convenience, speed, reliability, security against fraud and cost effectiveness.

User convenience and speed

A transaction between the card (card IC) and the reader defined by the system integrator or the service provider takes place when the card holder approximates the card to the reader. The permissible distance between antenna (target) and card is up to 100 mm free air. On the one hand, this enables users to carry out the transaction fast and conveniently. On the other, card holders decide in a distinct action whether they want a transaction to happen or not.
Philips has developed a high speed RF communication interface with 106 Kbaud data rate for MIFARE®. Due to this high speed a complete ticketing transaction can be handled in less than 0.1 seconds. Thus, the MIFARE® card user needs not to stop at the reader target (antenna) leading to a high throughput at gates and reduced boarding times onto busses.
Additional user comfort is added, since MIFARE® cards typically have the size of a credit card and do not have to be taken out of the wallet during the transaction, even if there are coins in the wallet.

Anticollision

Basically, if more than one card enters the operating field, which is very likely to happen, the fast anticollision algorithm prevents that data transmitted between the different cards and the target is being confused. Cards can be selected individually. An ongoing transaction with a selected card is not corrupted by cards remaining in the field or cards moved into or out of the field. Possible data corruption caused by more than one card in the field or fraud are avoided.
For example, if MIFARE® card users have more than one MIFARE® card in their wallet, the anticollision algorithm enables the system to select the appropriate card for the transaction.

Security

Mutual challenge and response authentication, data ciphering and message authentication checks protect the system from any kind of fraud and make it attractive for electronic purse applications. These mechanisms are carried out very fast and add only little to transaction time. Serial numbers which can not be altered guarantee uniqueness of the cards.

Multi-functionality

The multifunctional memory structure of MIFARE® 1 S50 cards IC allows the use of the card in multi-application systems. The different applications are securely separated by user definable key sets and access conditions.

Reliability

High reliability of the system is achieved by using solid state components without any moving mechanical parts. The MIFARE® cards are passive, i.e. they are working without battery. Further, the extremely simple construction of a card which consist only of a coil with few turns and a chip embedded in plastic does its share to accomplish this. In addition,
the contactless technology avoids that contacts become worn out and reduces risk and cost of vandalism.

1.1 Features of the MIFARE® System

- Operating frequency: 13.56 MHz
- High speed: Baudrate 106 kBaud
- Anticollision: The ability to handle more than one card in the field at the same time.
- Operating distance: up to 100mm (depending on antenna geometry) to allow convenient and fast transaction

- Half duplex communication protocol using handshake

- Data integrity via contactless communication link by
  - Anticollision
  - 16 Bit CRC per block
  - 16 Bit Parity per block (one per Byte)
  - Bit count checking
  - Bit coding to distinguish between "1", "0", and no information
  - Channel monitoring (Protocol sequence and bit stream analysis)

- Multi-Card-operation supporting:
  - Anticollision: allows the handling of more than one card in the field at the same time; inhibits accidental read or write and data corruption due to more than one card in the field
  - Dynamic read + write: during communication with one card other cards may enter or leave the RF field
  - Fast anticollision protocol: an increase of only 1.0 ms of the total transaction time for each additional card

1.2 MF1 IC S50 Card IC:

- State of the art chip technology: high speed CMOS EEPROM process
- Single chip construction with no external components besides a simple coil is required for card.
- No battery Contactless energy and data transmission

Security

- Mutual three pass authentication (ISO/IEC DIS9798-2)
- Data encryption on RF-channel with replay attack protection
- Individual key set per sector (per application) to support multi-application with key hierarchy
- Unique card serial number
- Transport key

Multi-application memory

- 8 KBit EEPROM memory, no battery,
- 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.
- Each sector has its own secret file for a set of keys for systems using key hierarchies.
- Access to memory zones are flexible user definable by a variety of access conditions.
- Arithmetic capability: increase and decrease
- Data retention of 10 years.
- write endurance 100.000 cycles

Typical Transaction Time

- Identification of a card 3 ms (Start-up, Answer to Request, Anticollision, Select)
- Read Block (16 Bytes) 2.5 ms (excl. Authentication)
  4.5 ms (incl. Authentication)
- Write Block + Control Read min 8.5 ms (excl. Authentication)
  min 10.5 ms (incl. Authentication)
- Typical Ticketing Transaction < 100 ms
  Identification of card +
  6 Blocks read (768 bit, 2 Sector Authentication) +
  2 Blocks write (256 bit) with Backup Management
- Transaction possible with moving card

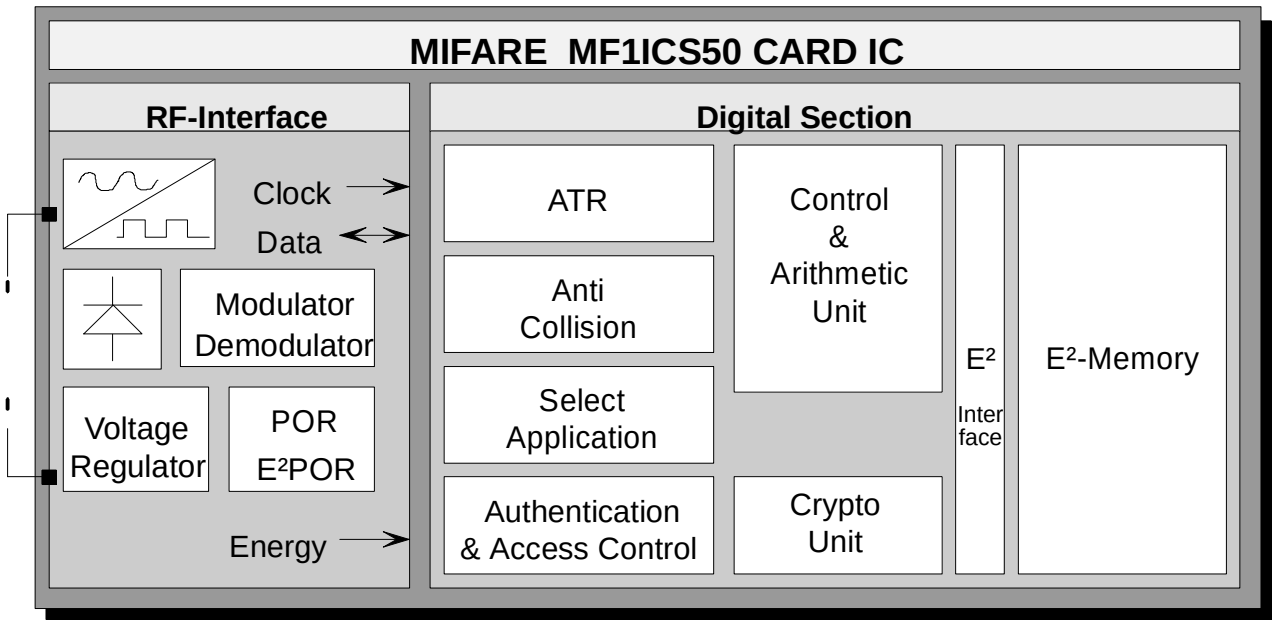
Delivery options

The MIFARE® 1 standard card IC (MF1 IC S50) is available as:

Delivery Option	Related ADDENDUM
Chip Card Module	ADDENDUM MIFARE® MF1MOA2S50 Contactless Chip Card Module Specification
Die on 5“ Wafer	ADDENDUM MIFARE® Standard Card IC MF1ICS50 03 Wafer Specification
Die on 6“ Wafer	ADDENDUM MIFARE® Standard Card IC MF1ICS50 04 Wafer Specification

2 Functional Description

2.1 Block Description

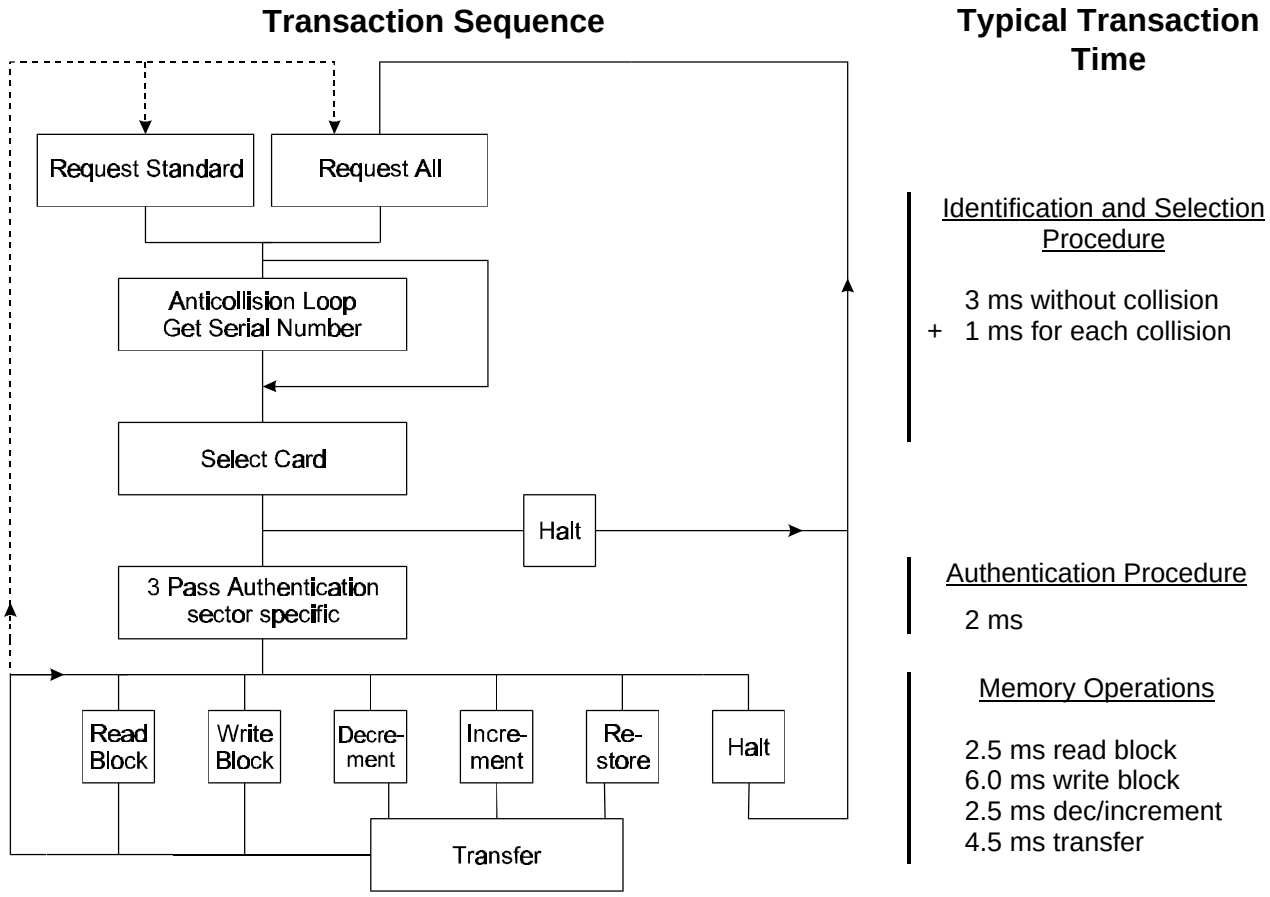


The electronic unit of a card comprises just an antenna (coil) and the IC (MIFARE® 1 MF1ICS50) and no further external components.

2.2 Antenna:

The card antenna consists of a few windings and thus, it is very suitable for integration into an ISO card. (refer to the document *MIFARE® Card IC Coil Design Guide*).

2.3 Communication scheme RWD ↔ Card



Answer to Request :

With the Answer to Request sequence the MIFARE® RWD (Read Write Device) requests all MIFARE® cards in the antenna field. When a card is in the operating range of a RWD, the RWD continues communication with the appropriate protocol.

Anticollision loop:

In the Anticollision loop the serial number of the card is read. If there are several cards in the operating range of a RWD they can be distinguished by their different 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 Answer to Request and Anticollision loop.

Select Card:

With the Select Card command the RWD selects one individual card for further authentication and memory related operations. The card returns the Answer to Select (ATS) code, which determines the individual type of the selected card.

Refer to the document *MIFARE® Standardised Card Type Identification Procedure* for further details.

Access Specification

After identification and selection of one card the RWD specifies the memory location of the following access.

3 Pass Authentication

The appropriate access key for the previously specified access is used for 3 Pass Authentication (see 2.5). Any communication after authentication is automatically encrypted at the sender and decrypted by the receiver.

Read/Write

After authentication any of the following operations may be performed:

READ	reads one block
WRITE	writes one block
DECREMENT	decrements the contents of one block and stores the result in the data-register
INCREMENT	increments the contents of one block and stores the result in the data-register
TRANSFER	writes the contents of the data-register to one block
RESTORE	stores the contents of one block in the data-register

2.4 Data Integrity

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

- Anticollision
- 16 Bit CRC per block
- 16 Bit Parity per block (one per Byte)
- Bit count checking
- Bit coding to distinguish between "1", "0", and no information
- Channel monitoring (Protocol sequence and bit stream analysis)

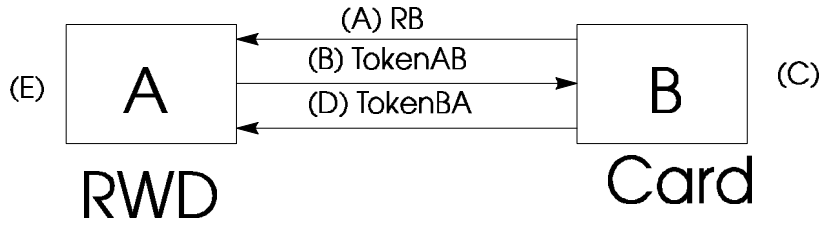
2.5 Security

To provide a very high security level three pass authentication (according to ISO 9798-2) and encryption based on a stream cipher algorithm with random generator, serial number and 48 Bit keys are integrated in the RWD`s Interface ASIC and the cards. Keys in the cards are read protected but can be altered, provided one knows the actual key. This gives the possibility to any system integrator who knows the transport key of any card to program his own secret keys. Splitting the card's memory into several sections with separate access keys makes the system open for multi-functionality (same cards for different applications).
Since there are two different keys (Key A and Key B) per sector available with corresponding access conditions available MIFARE® 1 S50 card IC provides the possibility of a system with key hierarchy. Key A for example can be used for protecting the decrement function and Key B the usually more sensible increment function.

Three pass authentication:

In this authentication mechanism uniqueness /timeliness is controlled by generating and checking random numbers.

Illustration of the authentication mechanism:



The tokens are structured as follows:

$TokenAB = eK_{AB}(R_A \| R_B \| B \| Text2)$.
$TokenBA = eK_{AB}(R_B \| R_A \| Text4)$.

NOTE - The inclusion of the parameter B in TokenAB is necessary to prevent a so called reflection attack. Such an attack is characterised by the fact that an intruder "reflects" the challenge R_B to B pretending to be A.

(A) B sends a random number R_B

(B) A sends Token AB to B.

(C) On receipt of the message containing Token AB, B verifies Token AB by deciphering the enciphered part and checking the correctness of the distinguishing identifier B and that the random number RB, sent to A in step (A), agrees with the random number contained in TokenAB.

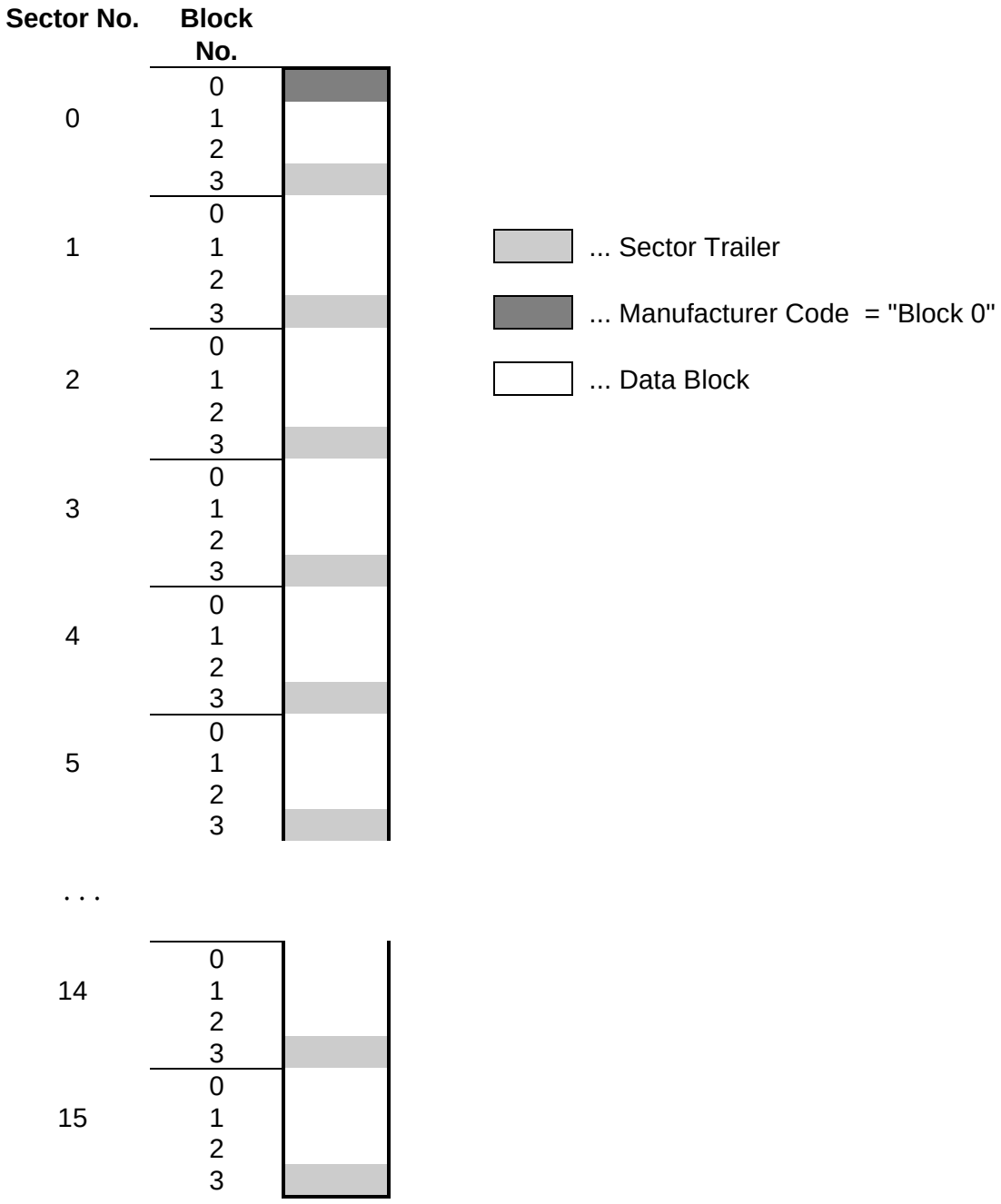
(D) B sends TokenBA to A.

(E) On receipt of the message containing Token BA , A verifies TokenBA by deciphering the enciphered part and checking that the random number R_B, received from A in step (A) agrees with the random number contained in TokenBA and that the random number R_A, sent to B in step (B), agrees with the random number contained in TokenBA.

2.6 Memory Organisation and Access Conditions

The MF1ICS50 IC has integrated a 8192 Bit EEPROM which is split into 16 sectors with 4 blocks. One block consists of 16 bytes (1 Byte = 8 Bit).

Memory Organisation:



2.6.1 Sector Trailer (Block 3):

Bit No. Byte No.	7 6 5 4 3 2 1 0
0	KEYSECXA
1	
2	
3	
4	
5	
6	ACCESS CONDITIONS
7	
8	
9	
10	KEYSECXB (optional)
11	
12	
13	
14	
15	

X ... Sector No. (0 to 15)
Y ... Block No. (0 to 3)

bit#	7	6	5	4	3	2	1	0
→	C2X3_b	C2X2_b	C2X1_b	C2X0_b	C1X3_b	C1X2_b	C1X1_b	C1X0_b
	C1X3	C1X2	C1X1	C1X0	C3X3_b	C3X2_b	C3X1_b	C3X0_b
	C3X3	C3X2	C3X1	C3X0	C2X3	C2X2	C2X1	C2X0
→	BX7	BX6	BX5	BX4	BX3	BX2	BX1	BX0

_b stands for inversion; e.g. C1X0_b=INV(C1X0)

The fourth block of any sector is the Sector Trailer. The Sector Trailer contains access Key A (KEYSECXA) an optional Key B (KEYSECXB) and the access conditions for the four blocks of that sector. If Key B is not needed, the last 6 Bytes of block 3 can be used as data bytes. The corresponding access condition settings are marked grey below.
C1XY to C3XY which are stored twice for safety reasons define the access condition independently for the sector's four blocks. The last byte of the access conditions may be used to store some specific application data (e.g. location of the write backup block).

- Access condition for the Sector Trailer (Y = 3)

			KEYSECXA		ACCESS COND.		KEYSECXB	
C1X3	C2X3	C3X3	read	write	read	write	read	write
0	0	0	never	key A	key A	never	key A	key A
0	1	0	never	never	key A	never	key A	never
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
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

incr, decr, transfer, restore : never

NOTE: Key A|B means key A or key B;
If key B may be read (all grey marked lines) the memory space for Key B is used for data storage and it shall not be used for authentication because all further memory access operations will fail.

Since the transport access conditions (after chip manufacturing) equal to 001, new cards must not be authenticated with Key B !

- Access condition for Data Blocks (Y = 0 to 2)

C1XY	C2XY	C3XY	read	write	incr	decr, transfer, restore
0	0	0	keyA|B[1]	key A|B[1]	key A|B[1]	key A|B[1]
0	1	0	keyA|B[1]	never	never	never
1	0	0	keyA|B[1]	key B[1]	never	never
1	1	0	keyA|B[1]	key B[1]	key B[1]	key A|B[1]
0	0	1	keyA|B[1]	never	never	key A|B[1]
0	1	1	key B[1]	key B[1]	never	never
1	0	1	key B[1]	never	never	never
1	1	1	never	never	never	never

The process of decrement and increment of a block's data is performed and controlled by the Card-IC.

- Transport code

For transportation, KEYSECXA and the access conditions are predefined by the manufacturer as follows:

C1X0, C2X0, C3X0 = 0 0 0 block 0 (data block)
C1X1, C2X1, C3X1 = 0 0 0 block 1 (data block)
C1X2, C2X2, C3X2 = 0 0 0 block 2 (data block)
C1X3, C2X3, C3X3 = 0 0 1 block 3 (Sector Trailer)

KEYSECXA . secret key, known only by
the manufacturer and system integrator

2.6.2 Manufacturer Code (Block 0 of Sector 0)

The first block of the memory is reserved for manufacturer data like 32 bit serial number. This is a read only block. In many documents it is named "Block 0".

2.6.3 Data Block (Block 0 to 3 except "Block 0")

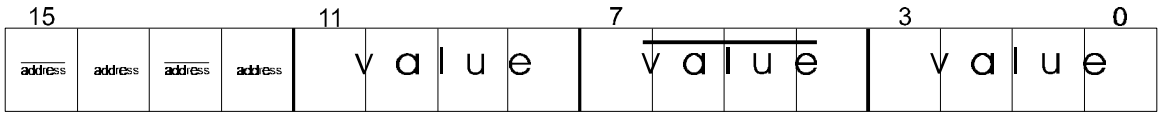
Access conditions for the Data Blocks are defined in the Sector Trailers. According to these conditions data can be read, written, incremented, decremented, transferred or restored either with Key A, Key B or never.

[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.

In the MF1ICS50 IC two types of Data Blocks are used:

a) read/write blocks
are used to read and write general 16 bytes of data.

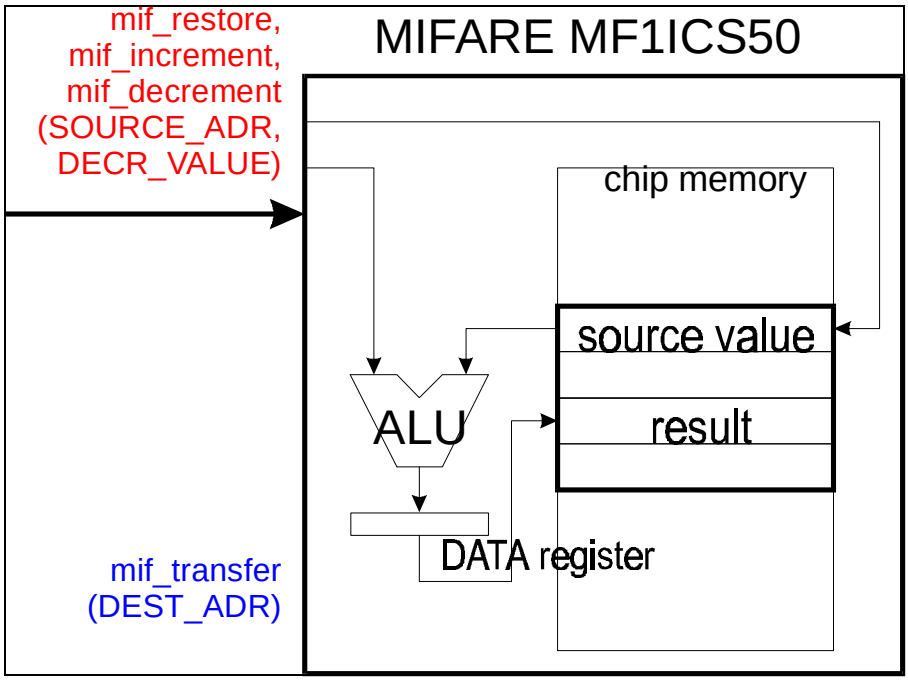
b) value blocks
are used for electronic purse functions (read, increment, decrement, transfer, restore). The maximum size of a value is 4 byte including sign bit, even when a complete 16 byte block has to be reserved. To provide error detection and correction capability, any value is stored 3 times into one value block. The remaining 4 bytes are reserved to some extent for check bits.



value: 32 bit signed 2th complement format stored 3 times
(the consistency of the 3 occurrences of the value is internally checked before the chip can perform any calculation)

address: 8 bit arbitrary address byte stored 4 times
(this byte is not internally interpreted)

A value blocks is first time generated by a WRITE instruction to the desired address. The value may be used for subsequent DECREMENT / INCREMENT / RESTORE instructions.



The result of a calculation instruction is temporally stored in a buffer register. For updating the memory with the calculation result the TRANSFER instruction has to be issued. The chip refuses calculations if any error in the block format could be detected.

2.6.4 Key management and Multi-functionality

The described memory organization makes it possible to appoint different sectors to different applications and to prevent data corruption by using application specific secret keys. Keys can only be altered by a RWD which has stored the actual Key A or Key B if this is allowed according to access conditions. Otherwise the actual key cannot be changed anymore.

Note:

Before the execution of a command the correct format of the Access Conditions is checked by the Card-IC. Thus, when programming the Sector Trailer the card needs to be fixed within the operating range of a RWD's antenna to prevent interruption of the write operation because any unsuccessful write operation may lead to blocking the whole sector.

2.7 Memory contents after IC test

2.7.1 Block 0 (manufacturer block):

byte															byte
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Serial number				CB	manufacturer data										

CB: “serial number check byte“ CB = byte 0 ^ byte 1 ^ byte 2 ^ byte 3 (^ ... XOR)

2.7.2 Data Blocks:

Data blocks: contain variable data.
(blocks 1,2 / 4,5,6 / 8,9,10 / 12,13,14 / 16,17,18 / 20,21,22 / 24,25,26 / 28,29,30 / 32,33,34 / 36,37,38 / 40,41,42 / 44,45,46 / 48,49,50 / 52,53,54 / 56,57,58 / 60,61,62)

2.7.3 Sector Trailers:

Note: The initial state of sector trailers after IC test can be modified depending on the personalisation done e.g. at the card manufacturer.

default coding:

byte															byte
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
transport key A						FF	07	80	xx	transport key B					

(blocks 3 / 7 / 11 / 15 / 19 / 23 / 27 / 31 / 35 / 39 / 43 / 47 / 51 / 55 / 59 / 63)
Byte 9 of all sector trailers is not defined. Its memory contents after IC test can vary.

3 Release Notes

This document refers to MIFARE® 1 **MF1ICS50** 03 / 04 silicon (revision 03 and 04).
It comprises all MIFARE® 1 S50 silicon delivered by PHILIPS Semiconductors since 1998.
For previous revisions of MIFARE® 1 silicon the dedicated documents are available on request.

3.1 Serial Numbers

Unique serial number (4 Byte)
MF1 ICS50 03/04
xx xx xx x**2** hex

3.2 Answer to SELECT command (ATS Code)

Answer to Select (ATS Code)
MF1 ICS50 03/04
0x08

Note: The ATS code may be used to identify the card IC type (for details refer to the document: *MIFARE® Standardised Card IC Type Identification Procedure*).

Definitions

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

Life support applications

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

Philips Semiconductors - a worldwide company

Argentina: see South America
Australia: 34 Waterloo Road, NORTHRYDE, NSW 2113,
Tel. +612 9805 4455, Fax. +612 9805 4466
Austria: Computerstraße 6, A-1101 WIEN, P.O.Box 213,
Tel. +431 60 101, Fax. +431 30 101 1210
Belarus: Hotel Minsk Business Centre, Bld. 3, r.1211, Volodarski Str. 6,
220050 MINSK, Tel. +375172 200 733, Fax. +375172 200 773
Belgium: see The Netherlands
Brazil: see South America
Bulgaria: Philips Bulgaria Ltd., Energoproject, 15th floor,
51 James Bourchier Blvd., 1407 SOFIA
Tel. +3592 689 211, Fax. +3592 689 102
Canada: Philips Semiconductors/Components,
Tel. +1800 234 7381
China/Hong Kong: 501 Hong Kong Industrial Technology Centre,
72 Tat Chee Avenue, Kowloon Tong, HONG KONG,
Tel. +85223 19 7888, Fax. +85223 19 7700
Colombia: see South America
Czech Republic: see Austria
Denmark: Prags Boulevard 80, PB 1919, DK-2300 COPENHAGEN S,
Tel. +4532 88 2636, Fax. +4531 57 1949
Finland: Sinikalliontie 3, FIN-02630 ESPOO,
Tel. +3589 61 5800, Fax. +3589 61 580/xxx
France: 4 Rue du Port-aux-Vins, BP 317, 92156 SURESNES Cedex, 04552-903
Tel. +331 40 99 6161, Fax. +331 40 99 6427
Germany: Hammerbrookstraße 69, D-20097 HAMBURG,
Tel. +4940 23 53 60, Fax. +4940 23 536 300
Greece: No. 15, 25th March Street, GR 17778 TAVROS/ATHENS,
Tel. +301 4894 339/239, Fax. +301 4814 240
Hungary: see Austria
India: Philips INDIA Ltd., Shivsagar Estate, A Block, Dr. Annie Besant Rd.
Worli, MUMBAI 400018, Tel. +9122 4938 541, Fax. +9122 4938 722
Indonesia: see Singapore
Ireland: Newstead, Clonskeagh, DUBLIN 14,
Tel. +3531 7640 000, Fax. +3531 7640 200
Israel: RAPAC Electronics, 7 Kehilat Saloniki St., TEL AVIV 61180,
Tel. +9723 645 0444, Fax. +9723 649 1007
Italy: Philips Semiconductors, Piazza IV Novembre 3,
20124 MILANO, Tel. +392 6752 2531, Fax. +392 6752 2557
Japan: Philips Bldg. 13-37, Kohnan 2-chome, Minato-ku, TOKYO 108,
Tel. +813 3740 5130,Fax. +813 3740 5077
Korea: Philips House, 260-199, Itaewon-dong, Yonsan-ku, SEOUL,
Tel. +822 709 1412, Fax. +822 709 1415
Malaysia: No. 76 Jalan Universiti, 46200 PETALING JAYA, Selangor,
Tel. +60 3750 5214, Fax. +603 757 4880
Mexico: 5900 Gateway East, Suite 200, EL PASO, Texas 79905,
Tel. +9 5800 234 7381
Middle East: see Italy
Netherlands: Postbus 90050, 5600 PB EINDHOVEN, Bldg. VB,
Tel. +3140 27 82785, Fax +3140 27 88399
New Zealand: 2 Wagener Place, C.P.O. Box 1041, AUCKLAND,
Tel. +649 849 4160, Fax. +649 849 7811
Norway: Box 1, Manglerud 0612, OSLO,
Tel. +4722 74 8000, Fax. +4722 74 8341
Philippines: Philips Semiconductors Philippines Inc.,
106 Valero St. Salcedo Village, P.O.Box 2108 MCC, MAKATI,
Metro MANILA, Tel. +632 816 6380, Fax. +632 817 3474
Poland: Ul. Lukiska 10, PL 04-123 WARSZWA,
Tel. +4822 612 2831, Fax. +4822 612 2327
Portugal: see Spain
Romania: see Italy
Russia: Philips Russia, Ul. Usatcheva 35A, 119048 MOSCOW,
Tel. +7095 247 9145, Fax. +7095 247 9144
Singapore: Lorong 1, Toa Payoh, SINGAPORE 1231,
Tel. +65350 2538, Fax. +65251 6500
Slovakia: see Austria
Slovenia: see Italy
South Africa: S.A. Philips Pty Ltd., 195-215 Main Road Martindale,
2092 JOHANNESBURG, P.O.Box 7430 Johannesburg 2000,
Tel. +2711 470 5911, Fax. +2711 470 5494
South America: Rua do Rocio 220, 5th floor, Suite 51,
Sao Paulo, SAO PAULO - SP, Brazil,
Tel. +5511 821 2333, Fax. +5511 829 1849
Spain: Balmes 22, 08007 BARCELONA,
Tel. +343 301 6312, Fax. +343 301 4107
Sweden: Kottbygatan 7, Akalla, S-16485 STOCKHOLM,
Tel. +468 632 2000, Fax. +468 632 2745
Switzerland: Allmendstraße 140, CH-8027 ZÜRICH,
Tel. +411 488 2686, Fax. +411 481 7730
Taiwan: Philips Taiwan Ltd., 2330F, 66,
Chung Hsiao West Road, Sec. 1, P.O.Box 22978,
TAIPEI 100, Tel. +8862 382 4443, Fax. +8862 382 4444
Thailand: Philips Electronics (Thailand) Ltd.,
209/2 Sanpavuth-Bangna Road Prakanong, BANGKOK 10260,
Tel. +662 745 4090, Fax. +662 398 0793
Turkey: Talapasa Cad. No. 5, 80640 GÜLTEPE/ISTANBUL,
Tel. +90212 279 2770, Fax. +90212 282 6707
Ukraine: Philips Ukraine, 4 Patrice Lumumba Str., Building B, Floor 7,
252042 KIEV, Tel. +38044 264 2776, Fax. +38044 268 0461
United Kingdom: Philips Semiconductors Ltd., 276 Bath Road, Hayes,
MIDDLESEX UM3 5BX, Tel. +44181 730 5000, Fax. +44181 754 8421
United States: 811 Argues Avenue, SUNNYVALE, CA94088-3409,
Tel. +1800 234 7381
Uruguay: see South America
Vietnam: see Singapore
Yugoslavia: Philips, Trg N. Pasica 5/v, 11000 BEOGRAD,
Tel. +38111 625 344, Fax. +38111 635 777

Published by:
Philips Semiconductors Gratkorn GmbH, Mikron-Weg 1, A-8101 Gratkorn, AustriaFax: +43 3124 299 - 270

For all other countries apply to: Philips Semiconductors, Marketing & Sales Communications, Internet: http://www.semiconductors.philips.com
Building BE-p, P.O.Box 218, 5600 MD EINDHOVEN, The Netherlands, Fax: +3140 27 24825

Philips Semiconductors

PHILIPS