

DATA SHEET

mifare[®]

Standard Card IC

MF1 IC S50

Functional Specification

Product Specification

May 2001

Revision 5.1

Functional Specification

Standard Card IC MF1 IC S50

CONTENTS

1	FEATURES.....	4
1.1	MIFARE® RF Interface (ISO/IEC 14443 A).....	4
1.2	EEPROM.....	4
1.3	Security.....	4
2	GENERAL DESCRIPTION.....	5
2.1	Contactless Energy and Data Transfer.....	5
2.2	Anticollision.....	5
2.3	User Convenience.....	5
2.4	Security.....	5
2.5	Multi-application Functionality.....	5
2.6	Delivery Options.....	6
3	FUNCTIONAL DESCRIPTION.....	6
3.1	Block Description.....	6
3.2	Communication Principle.....	7
3.2.1	REQUEST STANDARD / ALL.....	7
3.2.2	ANTICOLLISION LOOP.....	7
3.2.3	SELECT CARD.....	7
3.2.4	3 PASS AUTHENTICATION.....	7
3.2.5	MEMORY OPERATIONS.....	8
3.3	Data Integrity.....	8
3.4	Security.....	8
3.4.1	THREE PASS AUTHENTICATION SEQUENCE.....	8
3.5	RF Interface.....	8
3.6	Memory Organisation.....	9
3.6.1	MANUFACTURER BLOCK.....	10
3.6.2	DATA BLOCKS.....	10
3.6.3	SECTOR TRAILER (BLOCK 3).....	11
3.7	Memory Access.....	12
3.7.1	ACCESS CONDITIONS.....	13
3.7.2	ACCESS CONDITIONS FOR THE SECTOR TRAILER.....	13
3.7.3	ACCESS CONDITIONS FOR DATA BLOCKS.....	15
4	DEFINITIONS.....	16

Functional Specification

Standard Card IC MF1 IC S50

5	LIFE SUPPORT APPLICATIONS	16
6	REVISION HISTORY	17

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

Functional Specification

Standard Card IC MF1 IC S50

1 FEATURES

1.1 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
- Fast data transfer: 106 kbit/s
- High data integrity: 16 Bit CRC, parity, bit coding, bit counting
- True anticollision
- Typical ticketing transaction: < 100 ms (including backup management)

1.2 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

1.3 Security

- Mutual three pass authentication (ISO/IEC DIS9798-2)
- Data encryption on RF-channel with replay attack protection
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy
- Unique serial number for each device
- Transport key protects access to EEPROM on chip delivery

Functional Specification

Standard Card IC MF1 IC S50

2 GENERAL DESCRIPTION

Philips has developed the MIFARE[®] MF1 IC S50 to be used in contactless smart cards according to ISO/IEC 14443A. The communication layer (MIFARE[®] RF Interface) complies to parts 2 and 3 of the ISO/IEC 14443A standard. The security layer sports the field-proven CRYPTO1 stream cipher for secure data exchange of the MIFARE[®] Classic family.

2.1 Contactless Energy and Data Transfer

In the MIFARE[®] system, the MF1 IC S50 is connected to a coil with a few turns and then embedded in plastic to form the passive contactless smart card. No battery is needed. When the card is positioned in the proximity of the Read Write Device (RWD) antenna, the high speed RF communication interface allows to transmit data with 106 kBit/s.

2.2 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.

2.3 User Convenience

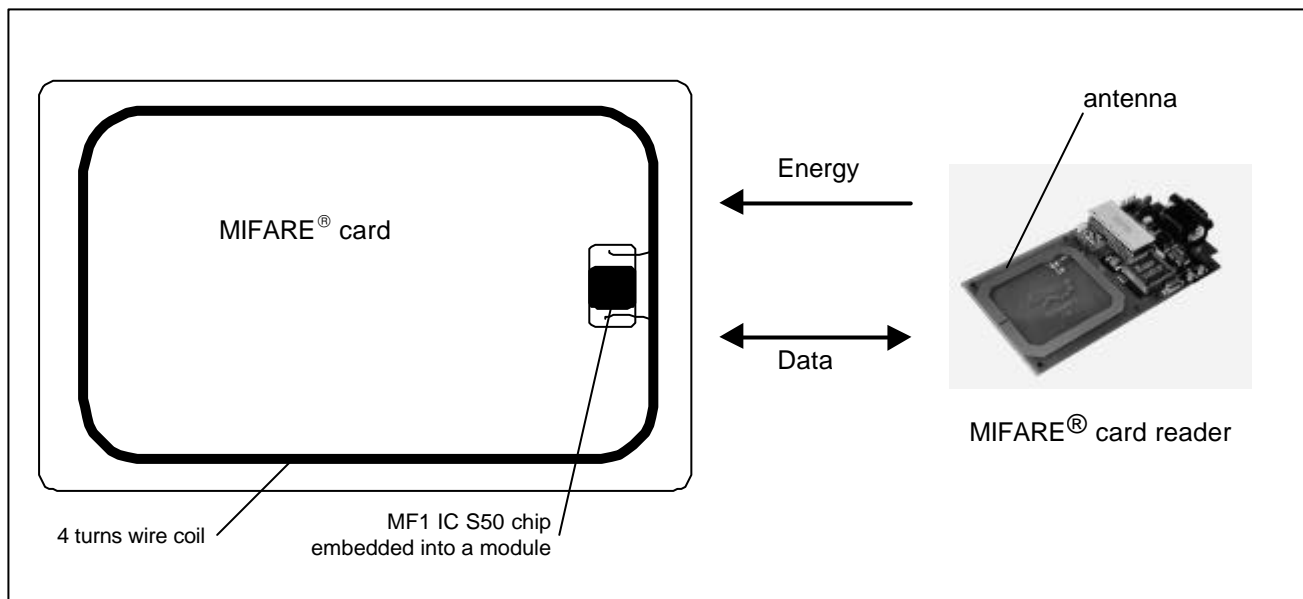
The MIFARE[®] system is designed for optimal user convenience. The high data transmission rate for example allows complete ticketing transactions to be handled in less than 100 ms. Thus, the MIFARE[®] card user is not forced to stop at the RWD antenna leading to a high throughput at gates and reduced boarding times onto busses. The MIFARE[®] card may also remain in the wallet during the transaction, even if there are coins in it.

2.4 Security

Special emphasis has been placed on security against fraud. Mutual challenge and response authentication, data ciphering and message authentication checks protect the system from any kind of tampering and thus make it attractive for ticketing applications. Serial numbers, which can not be altered, guarantee the uniqueness of each card.

2.5 Multi-application Functionality

The MIFARE[®] system offers real multi-application functionality comparable to the features of a processor card. Two different keys for each sector support systems using key hierarchies.



Functional Specification

Standard Card IC MF1 IC S50

2.6 Delivery Options

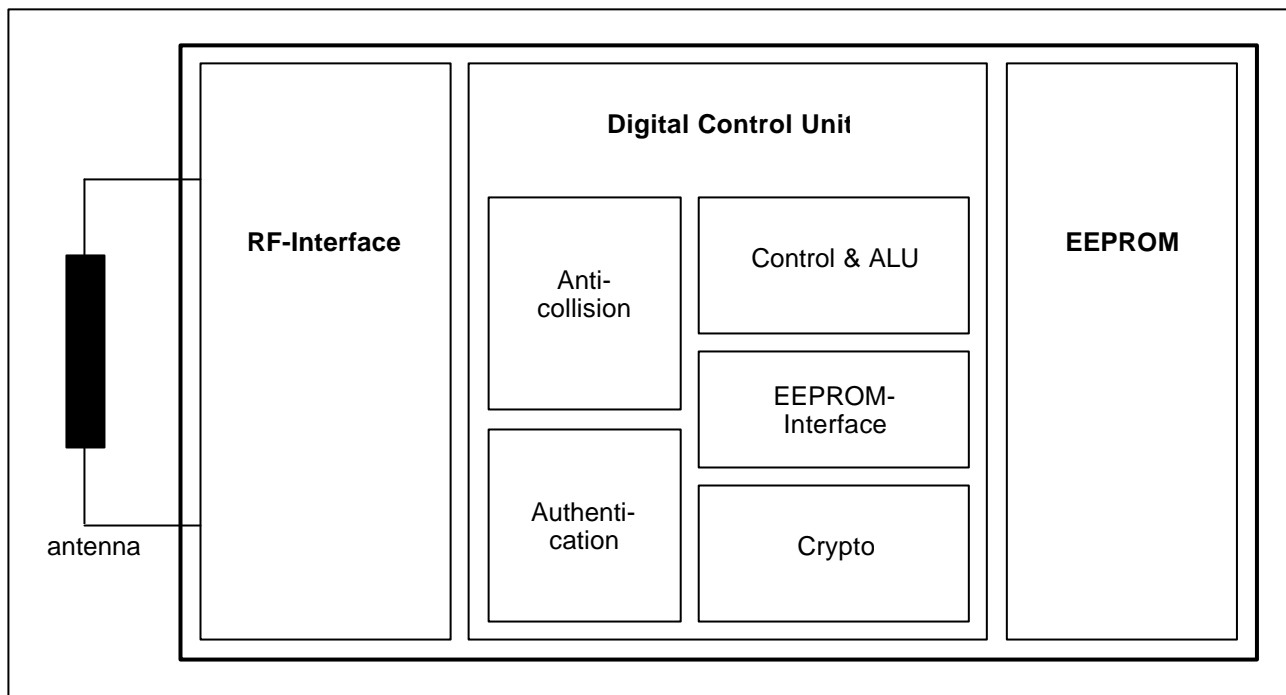
- Die on wafer
- Bumped die on wafer
- Chip Card Module

3 FUNCTIONAL DESCRIPTION

3.1 Block Description

The MF1 IC S50 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 MF1 IC S50. No further external components are necessary. (For details on antenna design please refer to the document *MIFARE^a 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 field-proven CRYPTO1 stream cipher of the MIFARE[®] Classic family ensures a secure data exchange
- EEPROM: 1 Kbyte are 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.



Functional Specification

Standard Card IC MF1 IC S50

3.2 Communication Principle

The commands are initiated by the RWD and controlled by the Digital Control Unit of the MF1 IC S50 according to the access conditions valid for the corresponding sector.

3.2.1 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).

3.2.2 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 RWD, they can be distinguished by their unique serial numbers and one can be selected (select card) for further transactions. The unselected

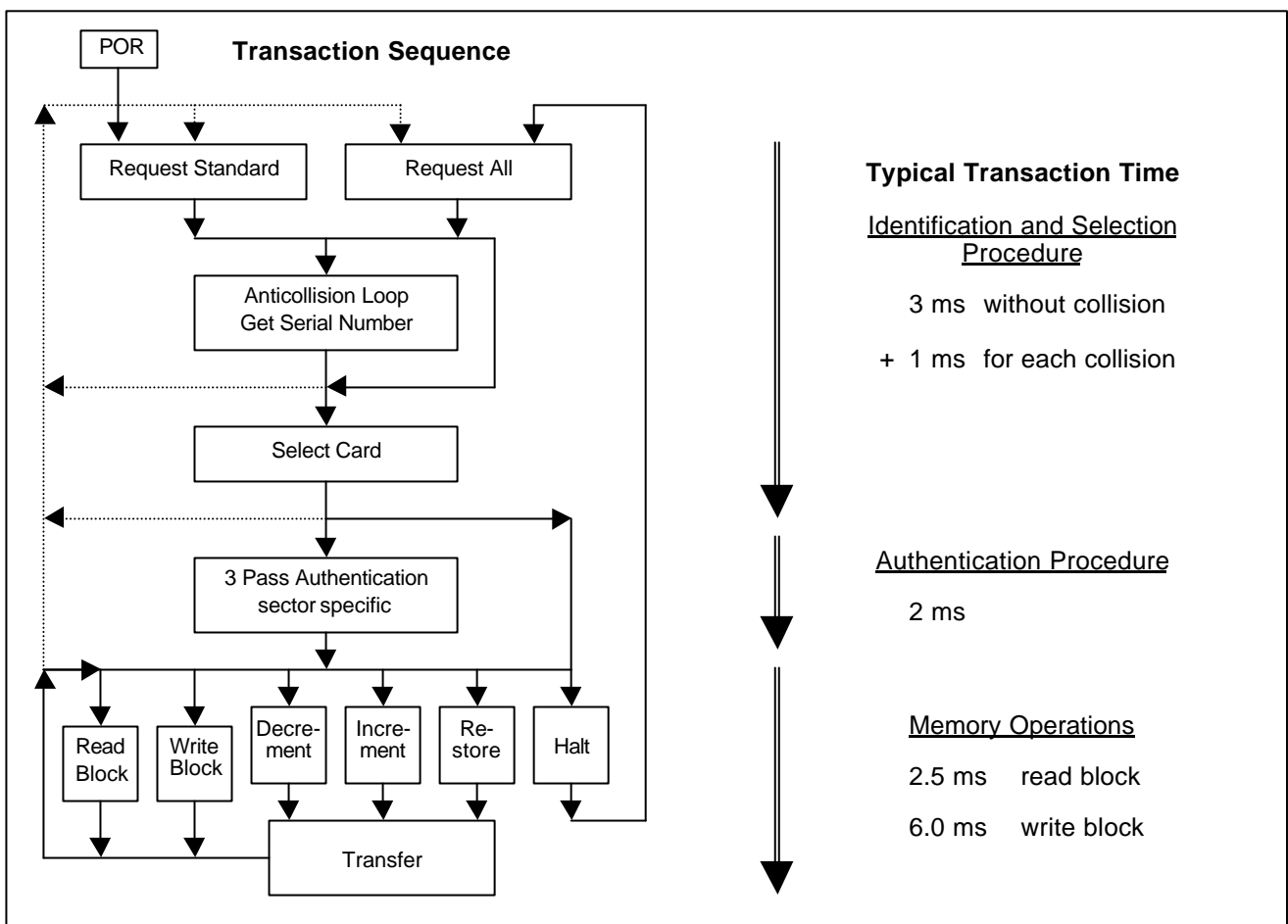
cards return to the standby mode and wait for a new request command.

3.2.3 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. Please refer to the document *MIFARE[®] Standardised Card Type Identification Procedure* for further details.

3.2.4 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.



Functional Specification

Standard Card IC MF1 IC S50

3.2.5 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

3.3 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
- Bit count checking
- Bit coding to distinguish between "1", "0", and no information
- Channel monitoring (protocol sequence and bit stream analysis)

3.4 Security

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

3.4.1 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.

3.5 RF Interface

The RF-interface is according to the standard for contactless smart cards ISO/IEC 14443A.

The carrier field from the RWD 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).

Functional Specification

Standard Card IC MF1 IC S50

3.6 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".

Sector	Block	Byte Number within a Block																Description
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
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

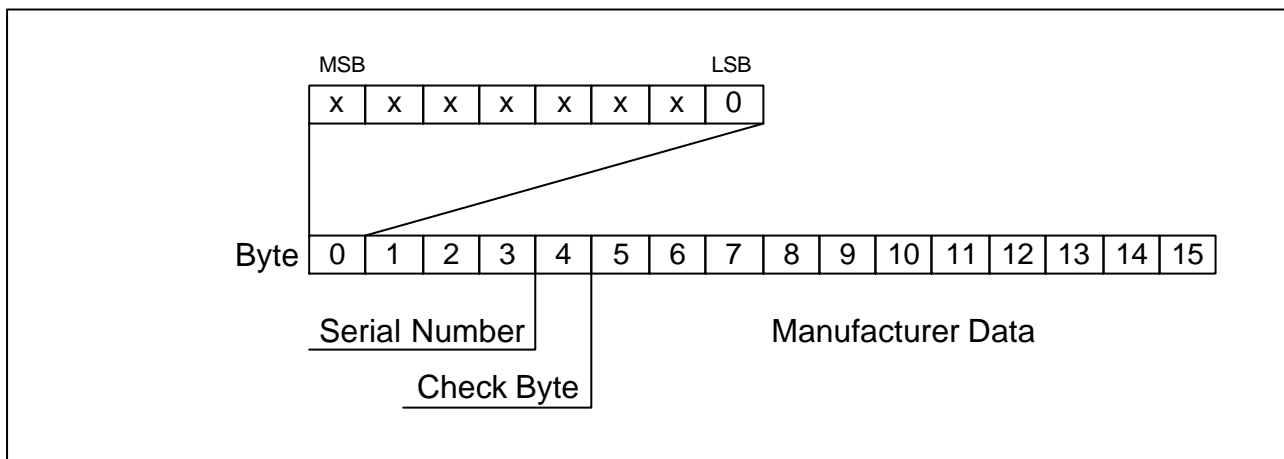
Functional Specification

Standard Card IC MF1 IC S50

3.6.1 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.



3.6.2 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.

3.6.2.1 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.
- 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	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Description	Value				Value				Value				Adr	$\overline{\text{Adr}}$	Adr	$\overline{\text{Adr}}$

Functional Specification

Standard Card IC MF1 IC S50

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

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

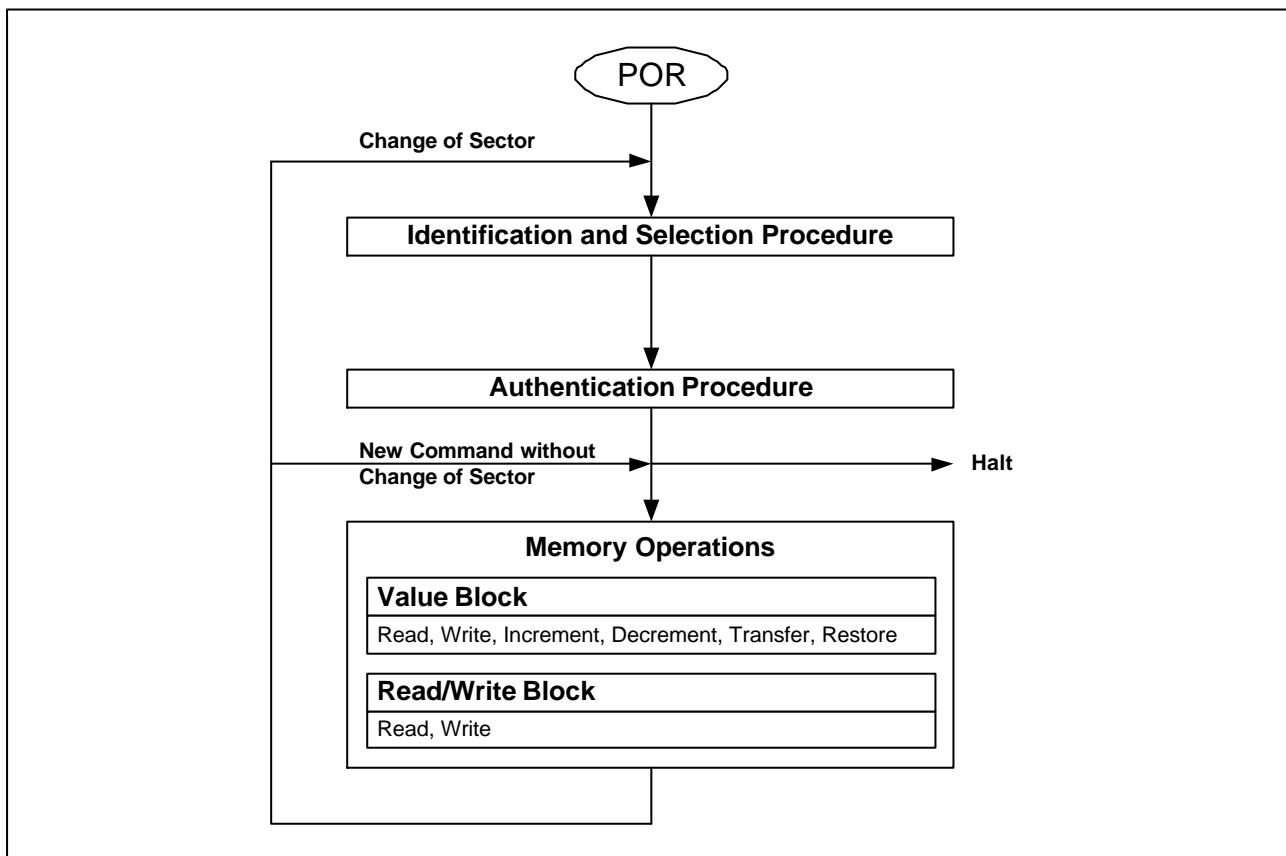
Functional Specification

Standard Card IC MF1 IC S50

3.7 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.



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

Functional Specification

Standard Card IC MF1 IC S50

access bits is specified as 'never', 'key A', 'key B' or key A|B' (key A or key B).

configuration, new cards must be authenticated with key A.

On chip delivery the access conditions for the sector

Since the access bits themselves can also be blocked, special care should be taken during personalization of cards.

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

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	

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

Functional Specification

Standard Card IC MF1 IC S50

3.7.3 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 und 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 authentication¹.

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.

Functional Specification

Standard Card IC MF1 IC S50

4 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.	

5 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.

Functional Specification**Standard Card IC MF1 IC S50**

6 REVISION HISTORY**Table 1** Functional Specification MF1 IC S50 Revision History

REVISION	DATE	CPCN	PAGE	DESCRIPTION
5.1	0501	2001 05013	9, 10	New Coding Manufacturer Block
5.0	1199			New Layout: Revised. Includes MF1 IC S50 05 silicon.
1.0		-		Initial version.

Functional Specification

Standard Card IC MF1 IC S50

NOTES

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,
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,
04552-903 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, Austria Fax: +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 Electronics N.V. 1997

SCB52

All rights are reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner.

The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without any notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent- or other industrial or intellectual property rights.

**Philips
Semiconductors**



PHILIPS