DATA SHEET

mifare®

Standard 4 kByte Card IC

MF1 IC S70

Functional Specification

Product Specification

October 2002

Revision 3.1

PUBLIC

Philips Semiconductors

PHILIPS

CONTENTS

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

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

- 4 Kbyte, organised in 32 sectors with 4 blocks and 8 sectors with 16 blocks (one block consists of 16 bytes)
- 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 key set 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

2 GENERAL DESCRIPTION

Philips has developed the mifare® MF1 IC S70 to be used in contactless smart cards according to ISO/IEC 14443 A. The communication layer complies to parts 2 and 3 of the ISO/IEC 14443 A standard. The security layer supports 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 S70 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 Proximity Coupling Device (PCD) 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

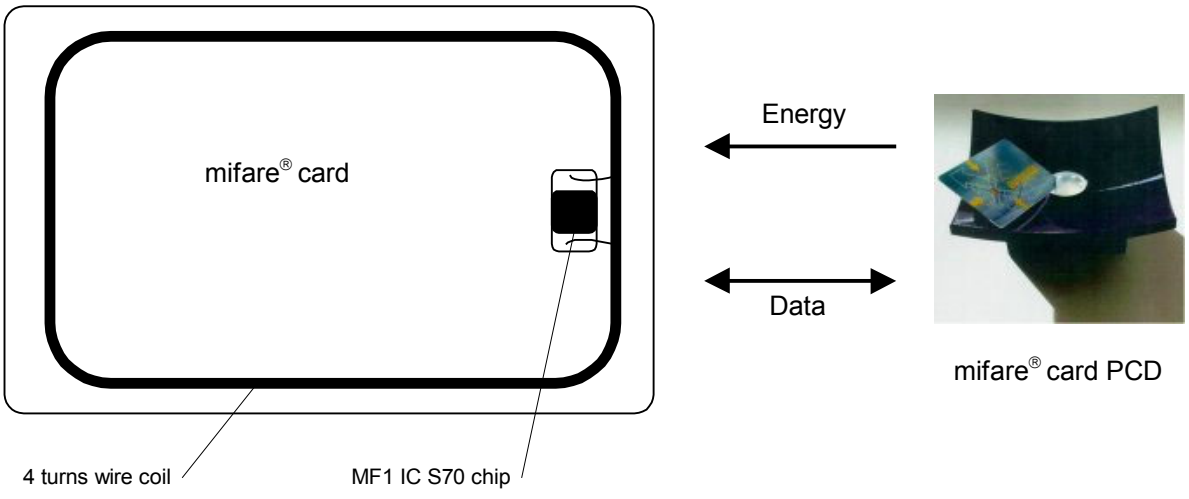
The mifare® system is designed for optimal user convenience. The high data transmission rate for example allows complete ticketing transactions to be handled in less than 100ms. Thus, the mifare® card user is not forced to stop at PCD antenna leading to a high throughput at gates and reduced boarding 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 electronic purse 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.



2.6 Delivery Options

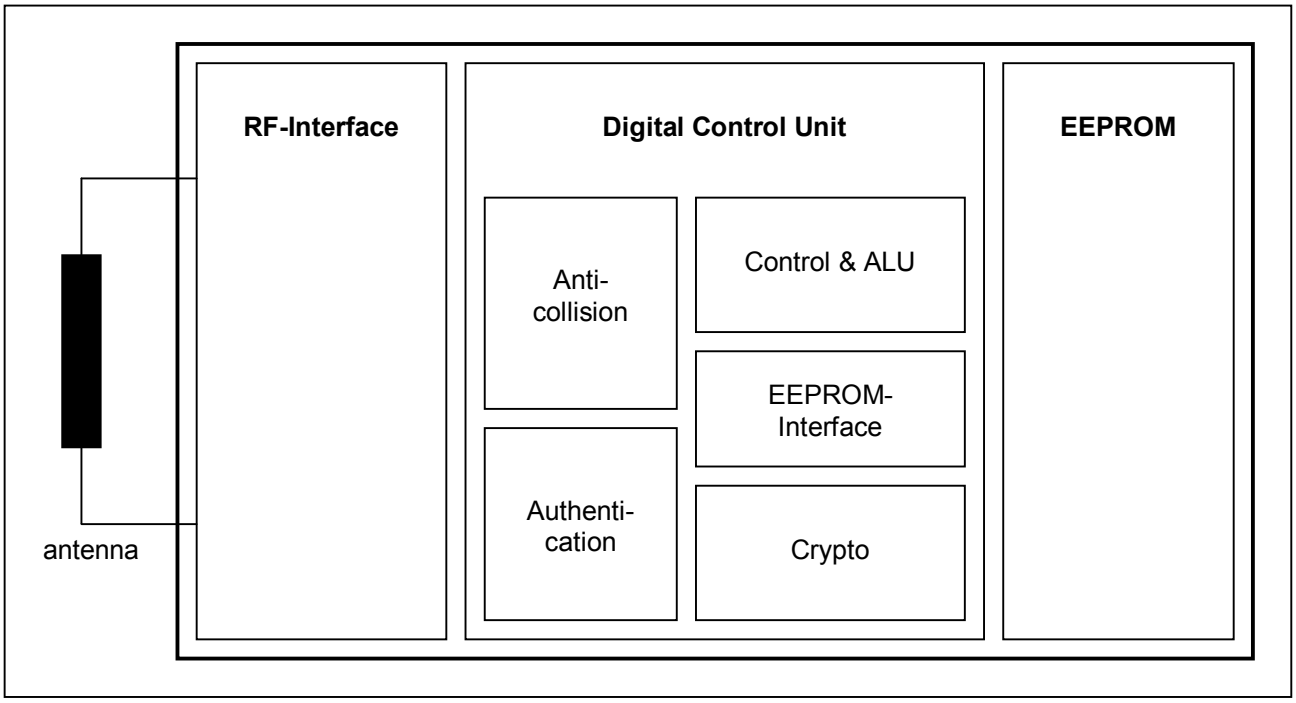
- Die on wafer: MF1ICS70W/V5D
- Bumped die on wafer: MF1ICS70W/V4D
- Chip Card Module: MF1MOA2S70/D

3 FUNCTIONAL DESCRIPTION

3.1 Block Description

The MF1 IC S70 chip consists of the 4 Kbytes 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 S70. No further external components are necessary. (For details on antenna design please refer to the document *mifare® (Card) 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: 4 Kbytes are organised in 32 sectors with 4 blocks each and 8 sectors with 16 blocks each. One block contains 16 bytes. The last block of each sector is called “sector trailer”, which contains two secret keys and programmable access conditions for each sector.



3.2 Communication Principle

The commands are initiated by the PCD and controlled by the Digital Control Unit of the MF1 IC S70 according to the access conditions valid for the corresponding sector.

3.2.1 ANSWER TO REQUEST

After Power On Reset (POR) of a card it can answer to a request command - sent by the PCD 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

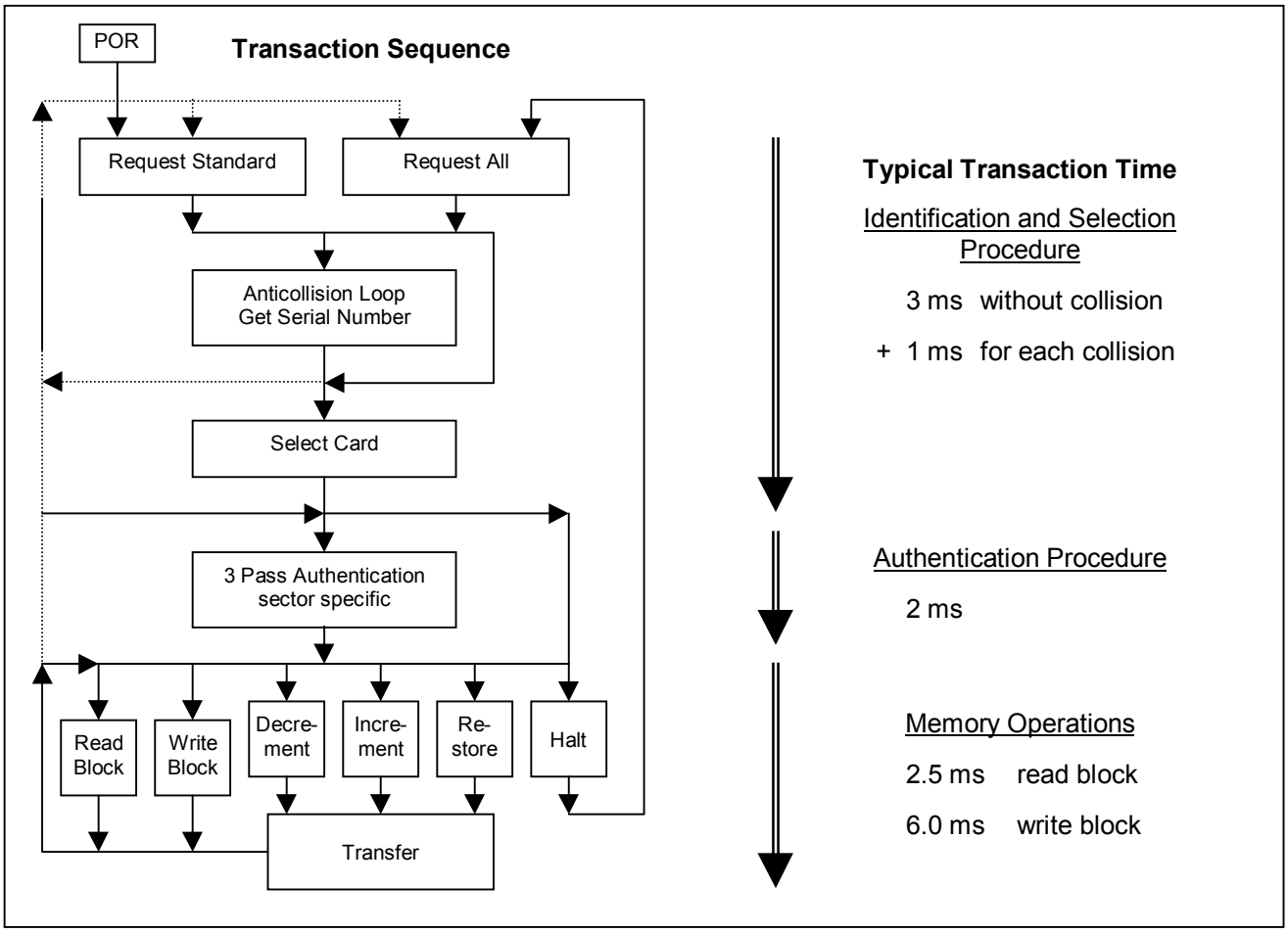
In the anticollision loop the serial number of a card is read. If there are several cards in the operating range of the PCD, they can be distinguished by their unique serial numbers and one can be selected (select card) for further transactions. The unselected cards return to the standby mode and wait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

3.2.3 SELECT CARD

With the select card command the PCD selects one individual card for authentication and memory related operations. The card returns the Answer To Select (ATS) code (=18h), which determines the type of the selected card. Please refer to the document *mifare® Standardized Card Type Identification Procedure* for further details.

3.2.4 3 PASS AUTHENTICATION

After selection of a card the PCD 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.



3.2.5 MEMORY OPERATIONS

After successful 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 an internal data-register
- Increment: Increments the contents of a block and stores the result in an internal data-register
- Restore: Moves the contents of a block into the internal data-register
- Transfer: Writes the contents of the internal data-register to a block

3.3 Data Integrity

Following mechanisms are implemented in the contactless communication link between PCD 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 PCD 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 PCD (pass one).
c) The PCD calculates the response using the secret key and additional input. The response, together with a random challenge from the PCD, is then transmitted to the card (pass two).
d) The card verifies the response of the PCD by comparing it with its own challenge and then it calculates the response to the challenge and transmits it (pass three).
e) The PCD 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 PCD is encrypted.

3.5 RF Interface

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

The carrier field from the PCD 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).

3.6 Memory Organisation

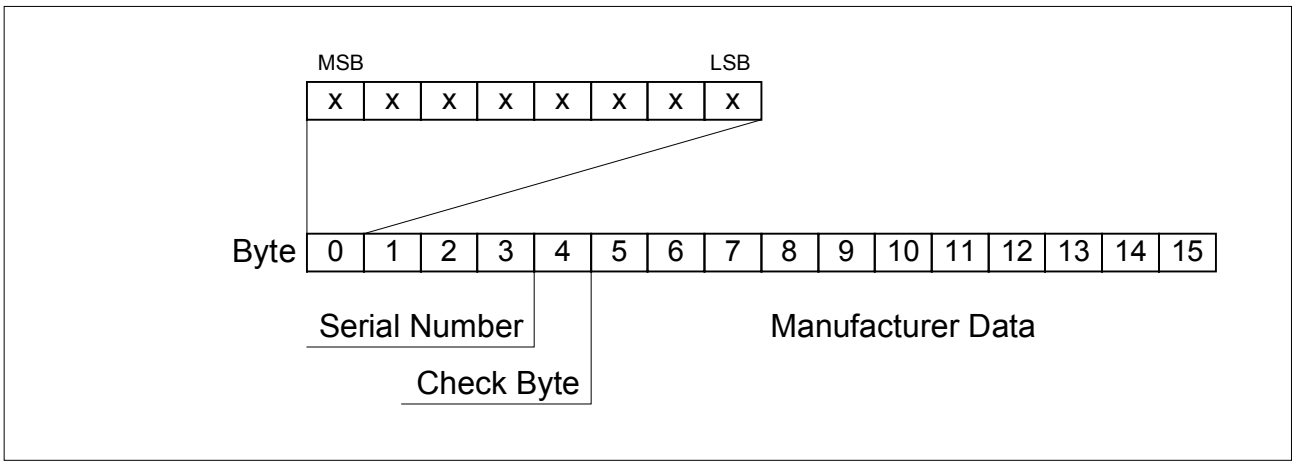
The 4 kByte EEPROM memory is organised in 32 sectors with 4 blocks and in 8 sectors with 16 blocks. One block consists of 16 bytes.

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**
39	15	Key A						Access Bits				Key B						Sector Trailer 39
	14																	Data
	13																	Data
	..																	..
	..																	..
	2																	Data
	1																	Data
	0																	Data
	..																	..
	..																	..
	..																	..
32	15	Key A						Access Bits				Key B						Sector Trailer 32
	14																	Data
	13																	Data
	..																	..
	..																	..
	2																	Data
	1																	Data
	0																	Data
31	3	Key A						Access Bits				Key B						Sector Trailer 31
	2																	Data
	1																	Data
	0																	Data
	..																	..
	..																	..
	..																	..
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Data

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

Sectors 0 .. 31 contain 3 blocks and sectors 32 .. 39 contain 15 blocks 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 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	$\overline{\text{Adr}}$

3.6.3 SECTOR TRAILER

Each sector has a sector trailer. Due to the memory configuration of the MF1 IC S70 this sector trailer is located in block 3 of each sector in the first two kByte of the NV-memory respectively in block 15 of each sector in the upper 2 kByte of the 4 kByte NV-memory.

Each sector trailer holds the

- secret keys A and B (optional) of the sector, which return logical “0”s when read and
- the access conditions for all 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 the sector trailer can be used as data bytes.

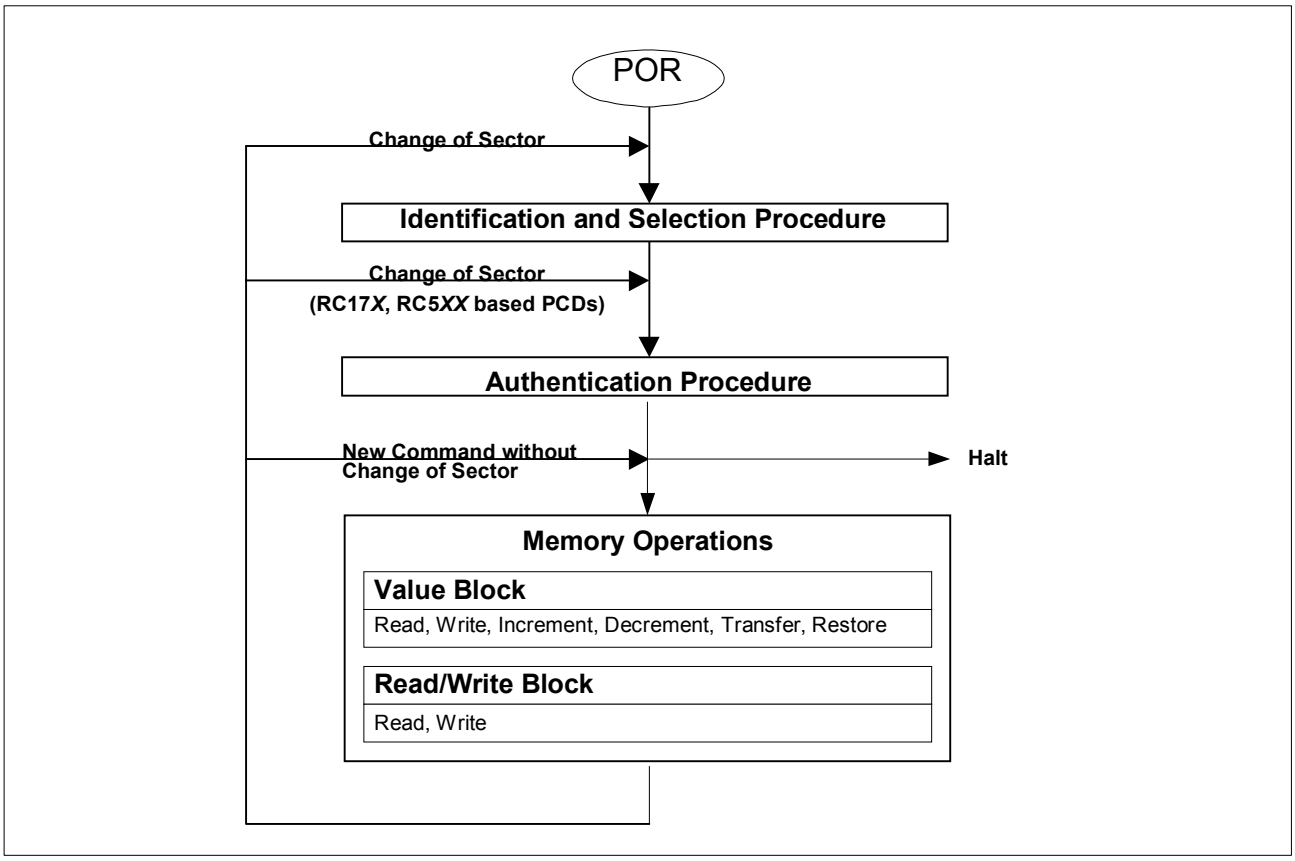
Byte 9 of the sector trailer is available for user data. For this byte apply the same access rights as for byte 6, 7 and 8.

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)					

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 data register	value
Decrement	decrements the contents of a block and stores the result in the data register	value
Transfer	writes the contents of the data register to a block	value
Restore	reads the contents of a block into the data register	value

3.7.1 ACCESS CONDITIONS

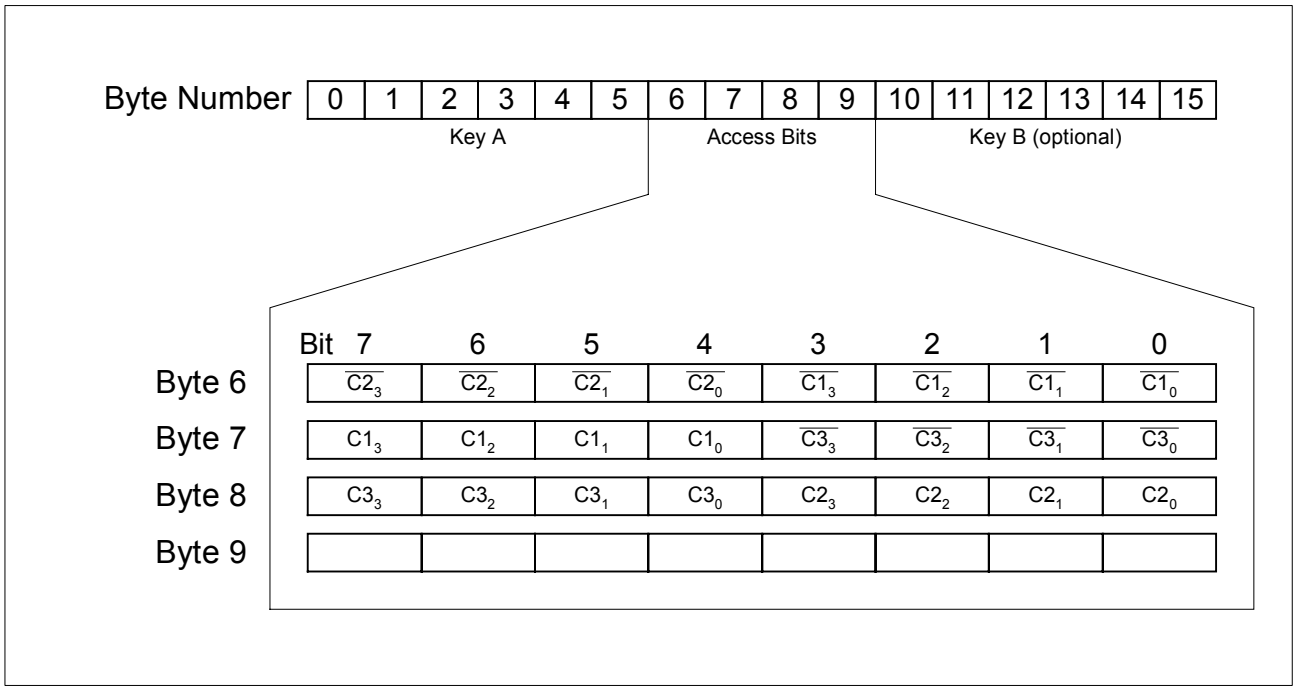
The access conditions for the data area and the sector trailer are defined by 3 bits, which are stored non-inverted and inverted in the sector trailer of the specified sector.

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.

Note: In the following description the access bits are mentioned in the non-inverted mode only.

The internal logic of the MF1 IC S70 ensures that the commands are executed only after an successful authentication procedure or never.

Access Bits	Valid Commands			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 area[1]
$C1_1\ C2_1\ C3_1$	read, write, increment, decrement, transfer, restore	→	1	data area[1]
$C1_0\ C2_0\ C3_0$	read, write, increment, decrement, transfer, restore	→	0	data area[1]



Note: 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.

[1] Note: For the first 32 sectors (first 2 Kbytes of NV-memory) the access conditions can be set individually for a data area sized one block.
For the last 8 sectors (upper 2 Kbytes of NV-memory) access conditions can be set individually for a data area sized 5 blocks.

3.7.2 ACCESS CONDITIONS FOR THE SECTOR TRAILER

Depending on the access bits for the sector trailer 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 trailer 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.

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	

3.7.3 ACCESS CONDITIONS FOR DATA AREAS

Depending on the access bits for data blocks (blocks 0 .. 2, respectively blocks 0 .. 14) 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]

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 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.

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.

6 REVISION HISTORY

Table 1 Functional Specification MF1 IC S70 Revision History

REVISION	DATE	CPCN	Chp.	DESCRIPTION
3.1	October 2002	-		Security Status Changed to PUBLIC
3.0		-	3.2.3	Product Version ATS=18hex
2.0	Nov 2001	-		Preliminary Version
1.2	October 2001	-		Updated Wording
1.1	August 2001	-		Update of Document Layout
1.0		-		Initial version.

NOTES

Philips Semiconductors - a worldwide company

Contact Information

For additional information please visit **http://www.semiconductors.philips.com**.Fax: **+31 40 27 24825**
For sales offices addresses send e-mail to: **sales.addresses@www.semiconductors.philips.com**.

 SCA74

Let's make things better.

Philips Semiconductors

PHILIPS