MF1S5009

Mainstream contactless smart card IC for fast and easy solution development

Rev. 3 — 27 July 2010
189131

Product data sheet
PUBLIC

1. General description

NXP Semiconductors has developed the MIFARE MF1S5009 to be used in a contactless smart card according to ISO/IEC 14443 Type A. The MF1S5009 features a double size UID for early adopters among existing MIFARE Classic systems which are planning to migrate from the currently used single size UID to double size UID.

The MIFARE MF1S5009 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 and 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.

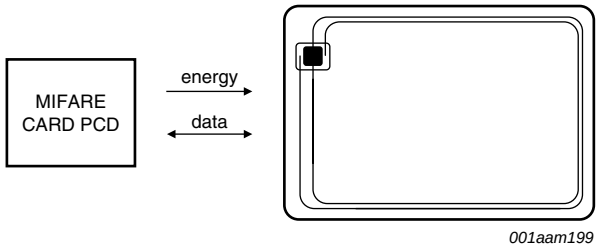


Fig 1. MIFARE card reader

1.3 Simple integration and user convenience

The MF1S5009 is designed for simple integration and user convenience which could allow complete ticketing transactions to be handled in less than 100 ms. Thus, the MF1S5009 card user is not forced to stop at the reader leading to a high throughput at gates and reduced boarding times onto busses.

1.4 Security

- Unique identifier for each device using double size UID (7 byte UID)
- Mutual three pass authentication (ISO/IEC 9798-2)
- Individual set of two keys per sector (per application) to support multi-application with key hierarchy

1.5 Delivery options

- Bumped die on wafer
- MOA4 contactless module

2. Features and benefits

2.1 MIFARE, RF Interface (ISO/IEC 14443 A)

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

2.2 EEPROM

- 1 kB, 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 time of 10 years
- Write endurance 100000 cycles

3. Applications

- Public transportation
- Access management
- Electronic toll collection
- Car parking
- School and campus cards
- Employee cards
- Internet cafés
- Loyalty

4. Ordering information

Table 1. Ordering information

Type number	Package			
	Commercial Name	Name	Description	Version
MF1S5009DUD	FFC	-	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format)	-
MF1S5009DA4	MOA4	PLLMC	plastic leadless module carrier package; 35 mm wide tape	SOT500-2

5. Block diagram

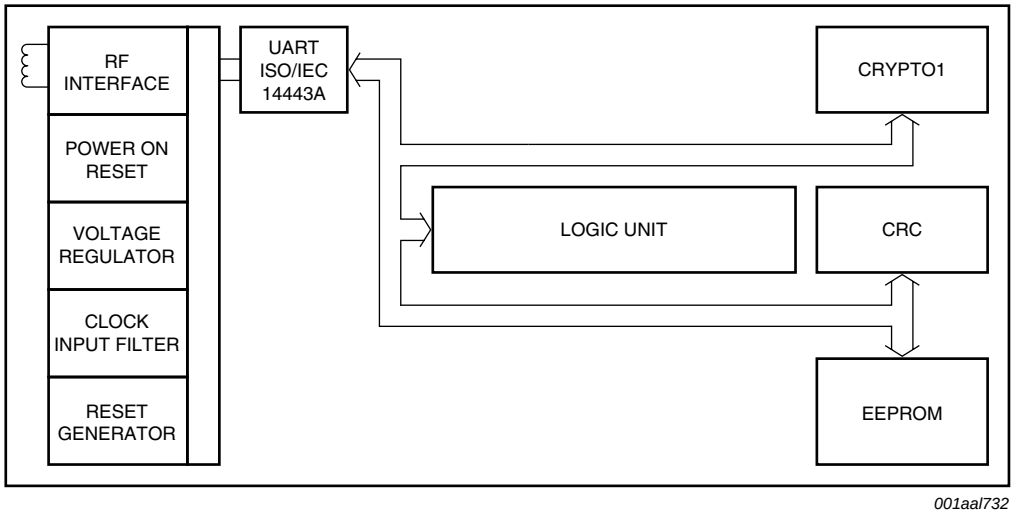


Fig 2. Block diagram

6. Pinning information

6.1 Smart card contactless module

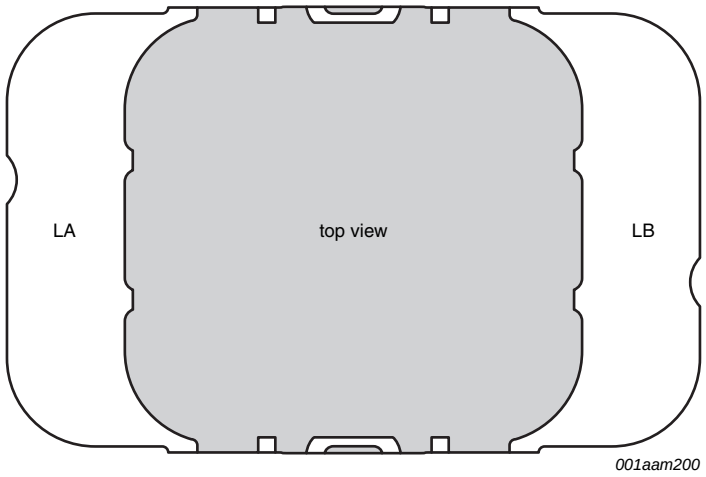


Fig 3. Contact assignments for SOT500-2 (MOA4)

Table 2. Bonding pad assignments to smart card contactless module

Contactless interface module		MF1S5009DA4
Antenna contacts	**Symbol**	**Description**
LA	LA	Antenna coil connection LA
LB	LB	Antenna coil connection LB

7. Mechanical specification

Table 3. Specifications

Wafer	
diameter	200 mm typical (8 inches)
maximum diameter after foil expansion	210 mm
thickness	120 μm ± 15 μm
flatness	not applicable
Potential Good Dies per Wafer (PGDW)	18482
Wafer backside	
material	Si
treatment	ground and stress relieve
roughness	R_a max = 0.2 μm
	R_t max = 2 μm
Chip dimensions	
step size	x = 1231 μm
	y = 1280 μm

Table 3. Specifications

gap between chips[1]	typical = 15 μm
	minimum = 5 μm
Passivation	
type	sandwich structure
material	nitride
thickness	1.75 μm
Au bump (substrate connected to VSS)	
material	> 99.9 % pure Au
hardness	35 to 80 HV 0.005
shear strength	>70 MPa
height	18 μm
height uniformity	within a die = ±2 μm
	within a wafer = ±3 μm
	wafer to wafer = ±4 μm
flatness	minimum = ±1.5 μm
size	LA, LB = 69 μm × 69 μm
	P1;TP2;VSS[2] = 58 μm × 58 μm
size variation	±5 μm
under bump metallization	sputtered TiW

[1] The gap between chips may vary due to changing foil expansion.

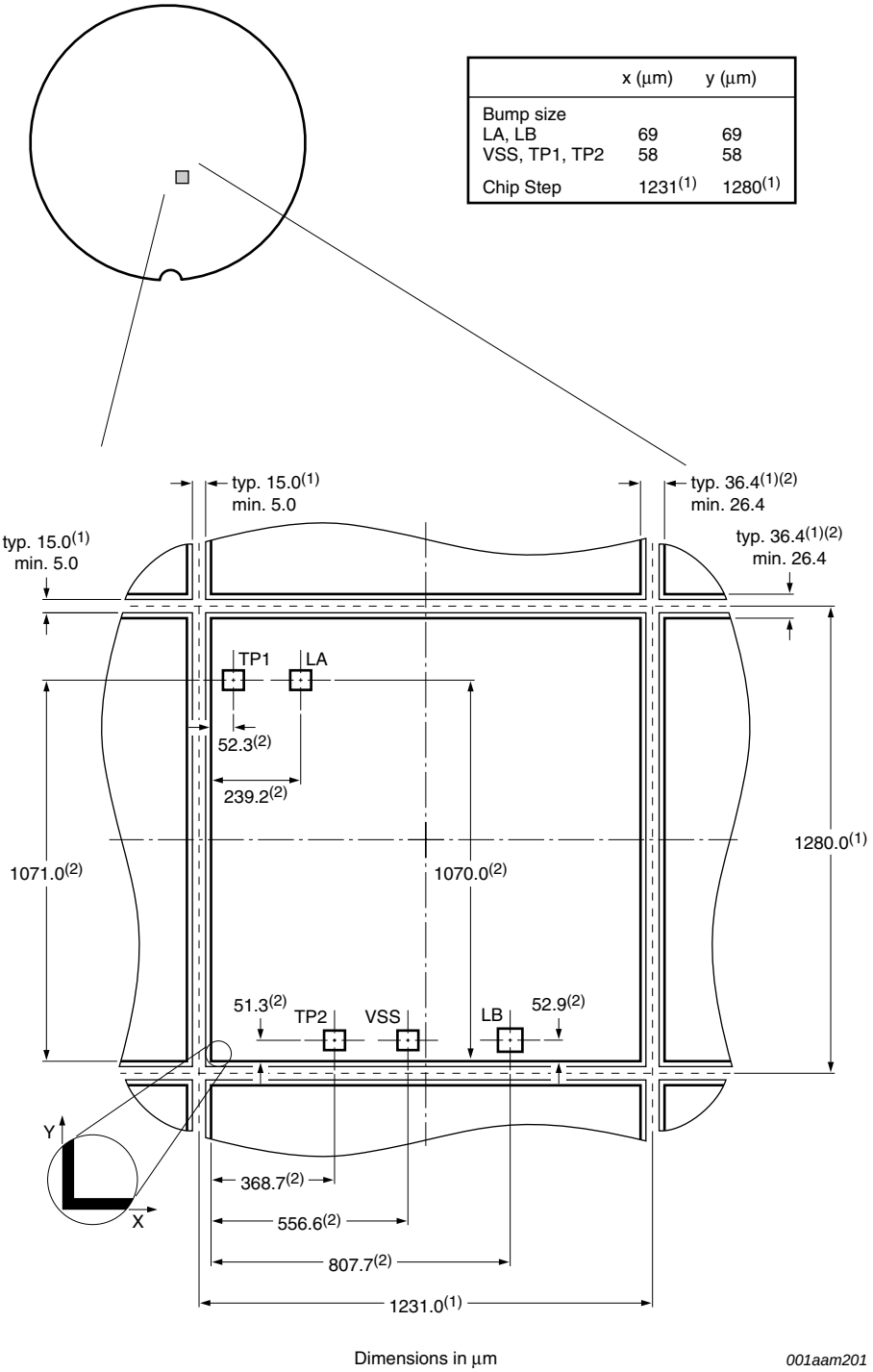
[2] Pads P1, TP2 and VSS are disconnected when wafer is sawn.

7.1 Fail die identification

Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/visual inspection.

No ink dots are applied.

8. Chip orientation and bond pad locations



(1) The air gap may vary due to varying foil expansion

(2) Measured from outer sealring edge (see detail)

All dimensions in µm

Fig 4. Chip orientation and bond pad locations

9. Functional description

9.1 Block description

The MF1S5009 chip consists of a 1 kB EEPROM, RF interface and Digital Control Unit. Energy and data are transferred via an antenna consisting of a coil with a small number of turns which is directly connected to the MF1S5009. No further external components are necessary. Refer to the document Ref. 1 for details on antenna design.

- RF interface:
  - Modulator/demodulator
  - Rectifier
  - Clock regenerator
  - Power-On Reset (POR)
  - Voltage regulator
- Anticollision: Multiple cards in the field may be selected and managed 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 and 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 MF1S5009 is used for authentication and encryption of data exchange.
- EEPROM: 1 kB 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.

9.2 Communication principle

The commands are initiated by the reader and controlled by the Digital Control Unit of the MF1S5009 according to the access conditions valid for the corresponding sector.

9.2.1 Request standard / all

After Power On Reset (POR) the card answers to a request REQA or wakeup WUPA command with the answer to request code (see Section 10.4, ATQA according to ISO/IEC 14443A).

9.2.2 Anticollision loop

In the anticollision loop the identifier of a card is read. If there are several cards in the operating field of the reader, they can be distinguished by their identifier and one can be selected (select card) for further transactions. The unselected cards return to the idle state and wait for a new request command.

The anticollision is done with two cascade levels as defined in ISO/IEC 14443-3, see also Ref. 6.

9.2.3 Select card

With the select card command the reader selects one individual card for authentication and memory related operations. The card returns the Select Acknowledge (SAK) code which determines the type of the selected card, see Section 10.4. For further details refer to the document Ref. 2, the handling of double size UIDs in MIFARE Classic is described in Ref. 6.

9.2.4 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.

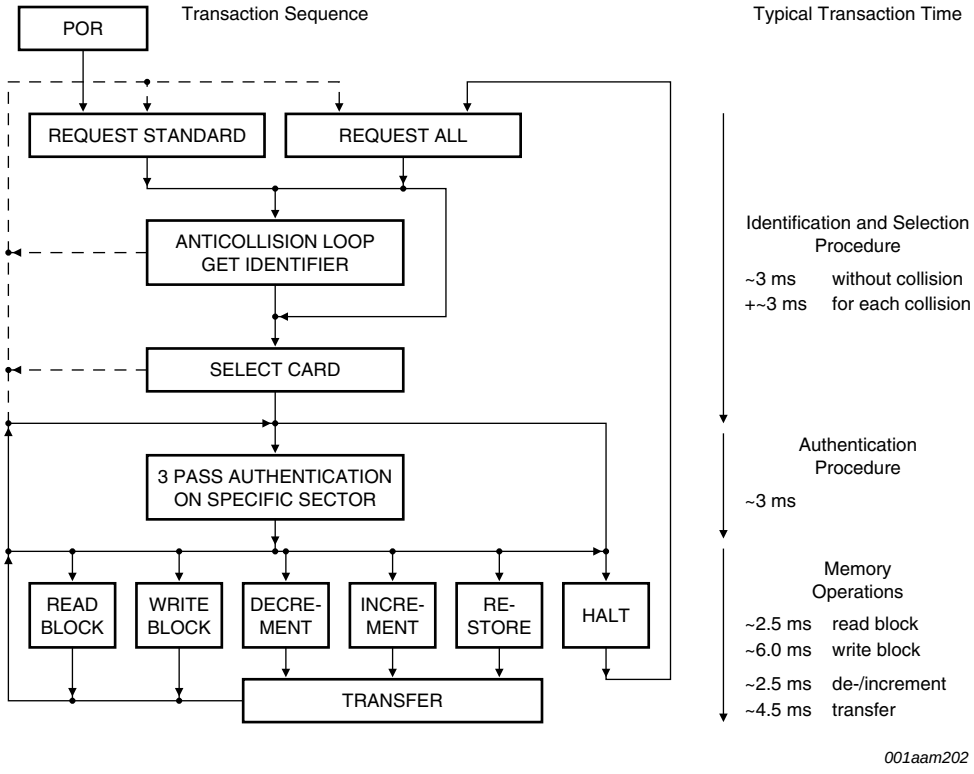


Fig 5. Three pass authentication

9.2.5 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

9.3 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)

9.4 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.

9.5 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).

9.6 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”.

		Byte Number within a Block															
Sector	Block	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

001aam203

Fig 6. Memory organization

9.6.1 Manufacturer block

This is the first data block (block 0) of the first sector (sector 0). It contains the IC manufacturer data. This block is programmed and write protected in the production test.

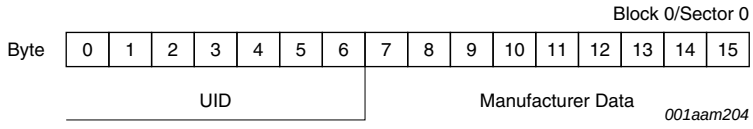


Fig 7. Manufacturer block

9.6.2 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.

9.6.2.1 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.

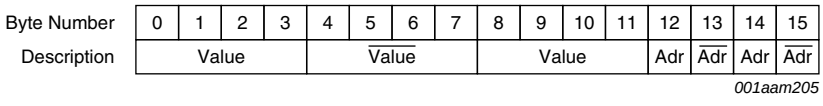


Fig 8. Value blocks

9.6.3 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.

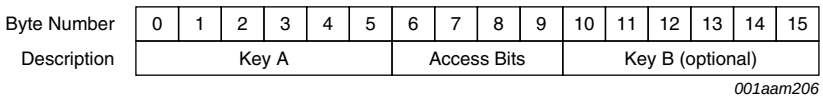


Fig 9. Sector trailer

9.7 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.

Table 4. 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

9.7.1 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 MF1S5009 ensures that the commands are executed only after an authentication procedure or never.

Table 5. 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

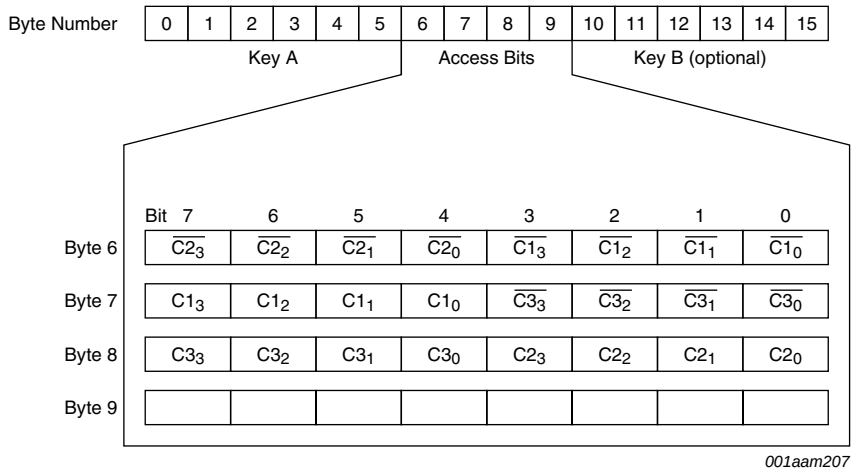


Fig 10. Access conditions

9.7.2 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 6. 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[1]
0	1	0	never	never	key A	never	key A	never	Key B may be read[1]
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[1]
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	

[1] for this access condition key B is readable and may be used for data

9.7.3 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

Table 7. 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.

10. Command overview

The MIFARE card activation follows the ISO/IEC 14443-3 type A. After the MIFARE card has been selected, it can either be deactivated using the ISO/IEC 14443 Halt command, or the MIFARE commands can be performed. For more details about the card activation refer to Ref. 4.

10.1 MIFARE command overview

All MIFARE Classic commands use the MIFARE Crypto1 and require an authentication.

All available commands for the MIFARE Classic are shown in Table 8.

Table 8. Command overview

Command	ISO/IEC 14443	Command code (hexadecimal)
Request	REQA	26h (7 bit)
Wake-up	WUPA	52h (7 bit)
Anticollision CL1	Anticollision CL1	93h 20h
Anticollision CL2	Anticollision CL2	95h 20h
Select CL1	Select CL1	93h 20h
Select CL2	Select CL2	95h 20h
Halt	Halt	50h 50h
Authentication with Key A	-	60h
Authentication with Key B	-	61h
MIFARE Read	-	30h
MIFARE Write	-	A0h
MIFARE Decrement	-	C0h
MIFARE Increment	-	C1h
MIFARE Restore	-	C2h
MIFARE Transfer	-	B0h
Halt	-	50h 00h

All the commands use the coding and framing as described in Ref. 3 and Ref. 4 (e.g. parity) if not otherwise specified.

10.2 Timings

In this document the timing shown is not to scale and rounded to 1 μs.

All the given times refer to the data frames including start of communication and end of communication, but do not include the encoding (like the Miller pulses).

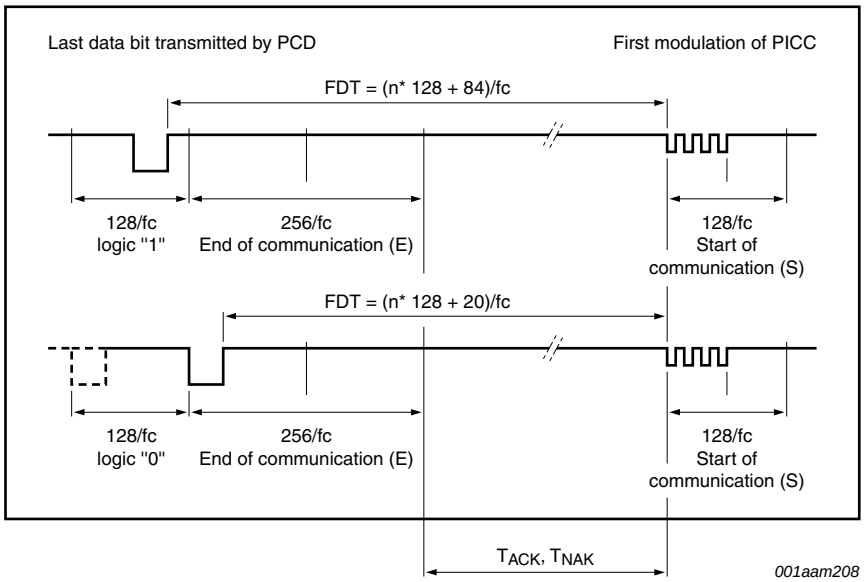
Consequently a data frame sent by the PCD contains the start of communication (1 “start bit”) and the end of communication (one logic 0 + 1 bit length of unmodulated carrier).

A data frame sent by the PICC contains the start of communication (1 “start bit”) and the end of communication (1 bit length of no subcarrier).

All timing can be measured according to ISO/IEC 14443-3 frame specification as shown for the Frame Delay Time in Figure 11. For more details refer to Ref. 3 and Ref. 4.

FDTPCD2PICC = Frame delay time PCD to PICC.

FDTPICC2PCD = Frame delay time PICC to PCD (must be at least 87 μS).



(1) Measurement of the FDT (Frame Delay Time) from PCD to PICC

Fig 11. Frame Delay Time (from PCD to PICC), and T_{ACK} and T_{NAK}

Remark: Due to the coding of commands, the measured timings usually exclude (a part of) the end of communication. This needs to be considered, when comparing the given times with the measured ones.

10.3 MIFARE ACK and NAK

The MIFARE Classic uses a 4 bit ACK / NAK as shown in Table 9.

Table 9. MIFARE ACK and NAK

Code (4-bit)	ACK/NAK
Ah	Acknowledge (ACK)
0h to 9h	NAK
Bh to Fh	NAK

10.4 ATQA and SAK responses

For details on the type identification procedure please refer to Ref. 2.

The MF1S5009 answers to a REQA or WUPA command with the ATQA value shown in Table 10 and to a Select CL1 command with the SAK value shown in Table 11.

Table 10. ATQA response of the MF1S5009

		Bit Number															
Response	**Hex Value**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
ATQA	$00\ 44_h$	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0

Table 11. SAK response of the MF1S5009

		Bit Number							
Response	**Hex Value**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
SAK	08_h	0	0	0	0	1	0	0	0

11. MIFARE classic commands

11.1 MIFARE Authentication

The MIFARE authentication is a 3-pass mutual authentication which needs two pairs of command-response. These two parts, MIFARE authentication part 1 and part 2 are shown in Figure 12, Figure 13 and Table 12.

Table 13 shows the required timing.

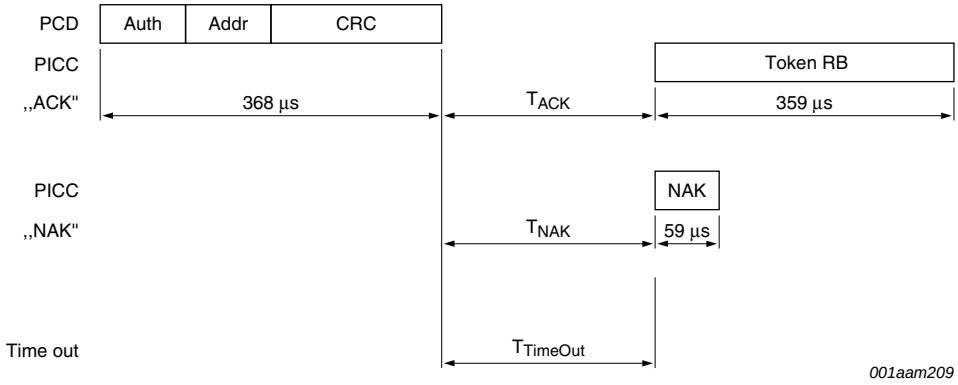


Fig 12. MIFARE Authentication part 1

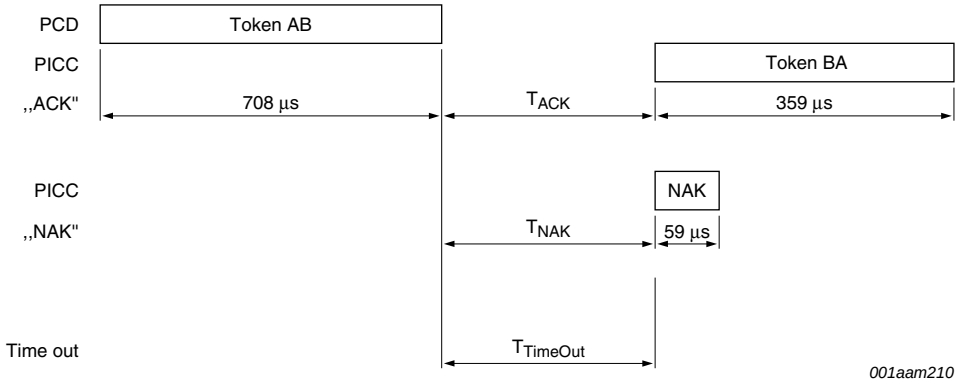


Fig 13. MIFARE Authentication part 2

Table 12. MIFARE authentication command

Name	Code	Description	Length
Auth (with Key A)	60h	Authentication with Key A	1 byte
Auth (with Key B)	61h	Authentication with Key B	1 byte
Addr	-	MIFARE Block address (00h to FFh)	1 byte
CRC	-	CRC according to Ref. 4	2 bytes
Token RB	-	Challenge 1 (Random Number)	4 bytes
Token AB	-	Challenge 2 (Random Number)	8 bytes
Token BA	-	Challenge 2 (Random Number)	4 bytes
NAK	see Table 9	see Section 10.3	4-bit

Table 13. MIFARE authentication timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
Authentication part 1	661 µs	$T_{TimeOut}$	661 µs	$T_{TimeOut}$	1 ms
Authentication part 2	113 µs	$T_{TimeOut}$	113 µs	$T_{TimeOut}$	1 ms

Remark: The minimum required time between MIFARE Authentication part 1 and part 2 is the minimum required FDT according to Ref. 4. There is no maximum specified.

Remark: The MIFARE authentication and encryption requires an MIFARE reader IC (e.g. the CL RC632). For more details about the authentication command refer to the corresponding data sheet (e.g. Ref. 5).

11.2 MIFARE Read

The MIFARE Read requires a block address, and returns the 16 bytes of one MIFARE Classic block. The command structure is shown in Figure 14 and Table 14.

Table 15 shows the required timing.

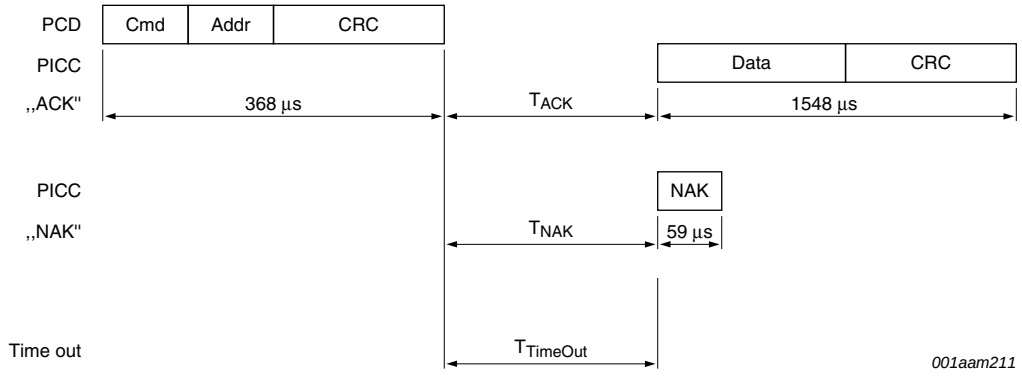


Fig 14. MIFARE Read

Table 14. MIFARE Read command

Name	Code	Description	Length
Cmd	30h	Read one block	1 byte
Addr	-	MIFARE Block address (00h to FFh)	1 byte
CRC	-	CRC according to Ref. 4	2 bytes
Data	-	Data content of the addressed block	16 bytes
NAK	see Table 9	see Section 10.3	4-bit

Table 15. MIFARE Read timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
Read	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	5 ms

11.3 MIFARE Write

The MIFARE Write requires a block address, and writes 16 Bytes of data into the addressed MIFARE Classic 1K block. It needs two pairs of command-response. These two parts, MIFARE Write part 1 and part 2 are shown in Figure 15, Figure 16 and Table 16.

Table 17 shows the required timing.

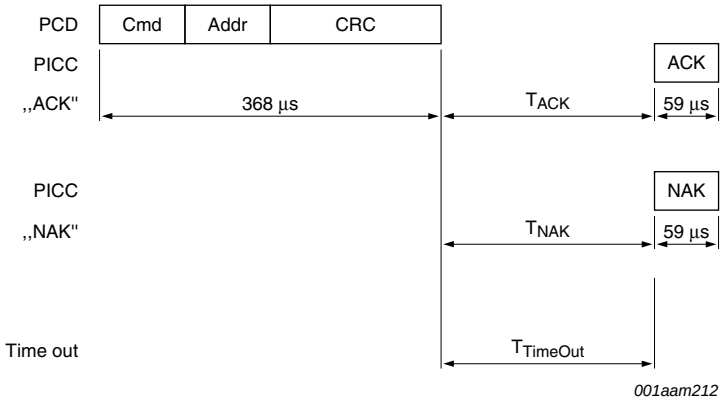


Fig 15. MIFARE Write part 1

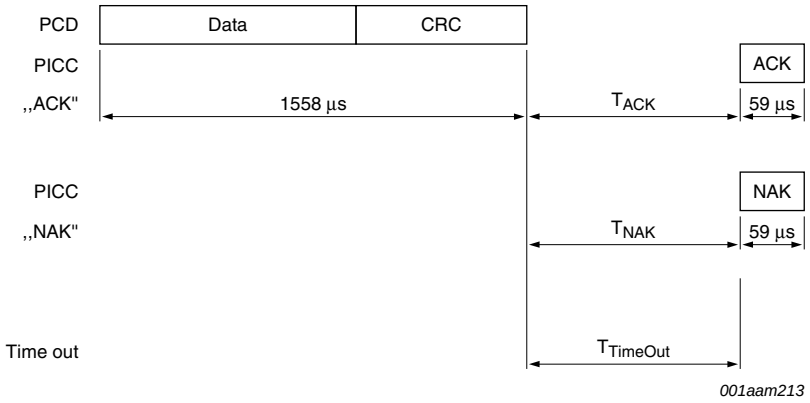


Fig 16. MIFARE Write part 2

Table 16. MIFARE Write command

Name	Code	Description	Length
Cmd	A0h	Read one block	1 byte
Addr	-	MIFARE Block or Page address (00h to FFh)	1 byte
CRC	-	CRC according to Ref. 4	2 bytes
Data	-	Data	16 bytes
NAK	see Table 9	see Section 10.3	4-bit

Table 17. MIFARE Write timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
Write part 1	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	5 ms
Write part 2	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	10 ms

Remark: The minimum required time between MIFARE Write part 1 and part 2 is the minimum required FDT acc. to Ref. 4. There is no maximum specified.

11.4 MIFARE Increment, Decrement and Restore

The MIFARE Increment requires a source block address and an operand. It adds the operand to the value of the addressed block, and stores the result in a volatile memory.

The MIFARE Decrement requires a source block address and an operand. It subtracts the operand from the value of the addressed block, and stores the result in a volatile memory.

The MIFARE Restore requires a source block address. It copies the value of the addressed block into a volatile memory.

These two parts of each command are shown in Figure 17, Figure 18 and Table 18.

Table 19 shows the required timing.

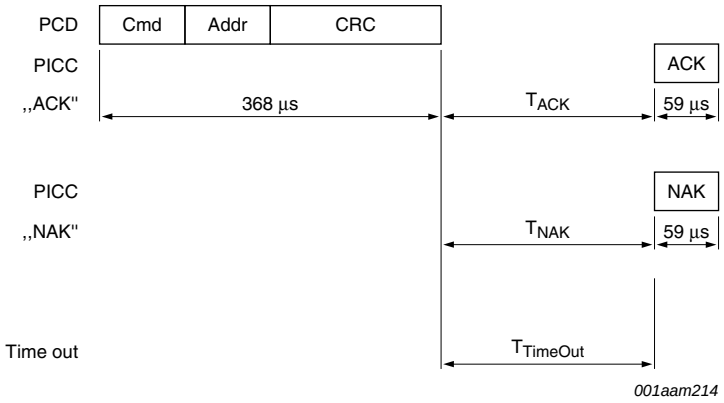
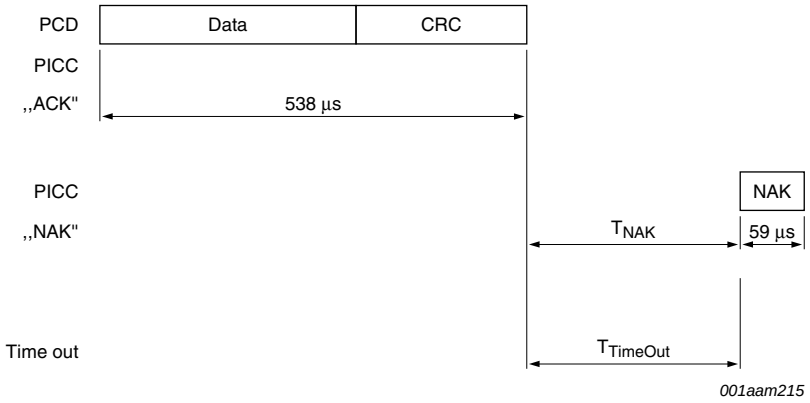


Fig 17. MIFARE Increment, Decrement and Restore part 1



(1) Increment, Decrement and Restore part 2 does not acknowledge

Fig 18. MIFARE Increment, Decrement and Restore part 2

Table 18. MIFARE Increment, Decrement and Restore command

Name	Code	Description	Length
Cmd	C1h	Increment	1 byte
Cmd	C0h	Decrement	1 byte
Cmd	C2h	Restore	1 byte
Addr	-	MIFARE source block address (00h to FFh)	1 byte
CRC	-	CRC according to Ref. 4	2 bytes
Data	-	Operand (4 byte signed integer)	4 bytes
NAK	see Table 9	see Section 10.3	4-bit

Table 19. MIFARE Increment, Decrement and Restore timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
Increment, Decrement, and Restore part 1	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	5 ms
Increment, Decrement, and Restore part 2	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	5 ms

Remark: The minimum required time between MIFARE Increment, Decrement, and Restore part 1 and part 2 is the minimum required FDT acc. too Ref. 4. There is no maximum specified.

Remark: The MIFARE Increment, Decrement, and Restore commands require a MIFARE Transfer to store the value into a destination block.

Remark: The MIFARE Increment, Decrement, and Restore command part 2 does not provide an acknowledgement, so the regular time out has to be used instead.

11.5 MIFARE Transfer

The MIFARE Transfer requires a destination block address, and writes the value stored in the volatile memory into one MIFARE Classic block. The command structure is shown in Figure 19 and Table 20.

Table 21 shows the required timing.

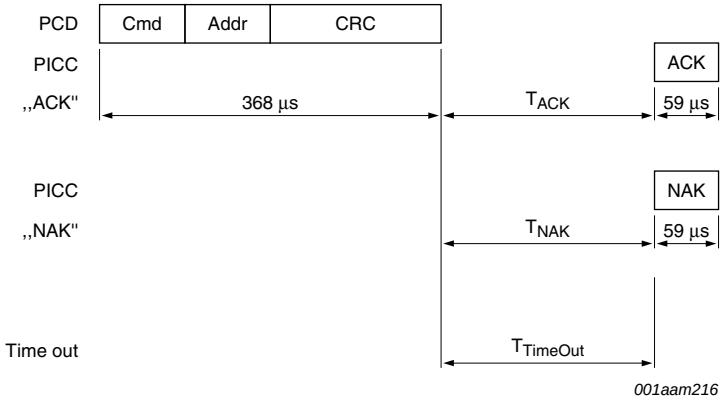


Fig 19. MIFARE Transfer

Table 20. MIFARE Transfer command

Name	Code	Description	Length
Cmd	B0h	Write value into destination block	1 byte
Addr	-	MIFARE destination block address (00h to FFh)	1 byte
CRC	-	CRC according to Ref. 4	2 bytes
NAK	see Table 9	see Section 10.3	4-bit

Table 21. MIFARE Transfer timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
Transfer	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	10 ms

12. Limiting values

Table 22. Limiting values [1][2]

In accordance with the Absolute Maximum Rating System (IEC 60134).

Symbol	Parameter		Min	Max	Unit
I_I	input current		-	30	mA
P_{tot}/pack	total power dissipation per package		-	200	mW
T_{stg}	storage temperature		−55	+125	°C
T_{amb}	ambient temperature		−25	+70	°C
V_{ESD}	electrostatic discharge voltage	[3]	2	-	kV
I_{lu}	latch-up current		±100	-	mA

[1] Stresses above one or more of the limiting values may cause permanent damage to the device

[2] Exposure to limiting values for extended periods may affect device reliability

[3] MIL Standard 883-C method 3015; Human body model: C = 100 pF, R = 1.5 kΩ

13. Characteristics

Table 23. Characteristics [1][2]

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance		[3]	15.0	17.0	19.0	pF
f_i	input frequency			-	13.56	-	MHz
EEPROM characteristics							
t_{ret}	retention time	T_{amb} = 22 °C		10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C		100000	200000	-	cycle

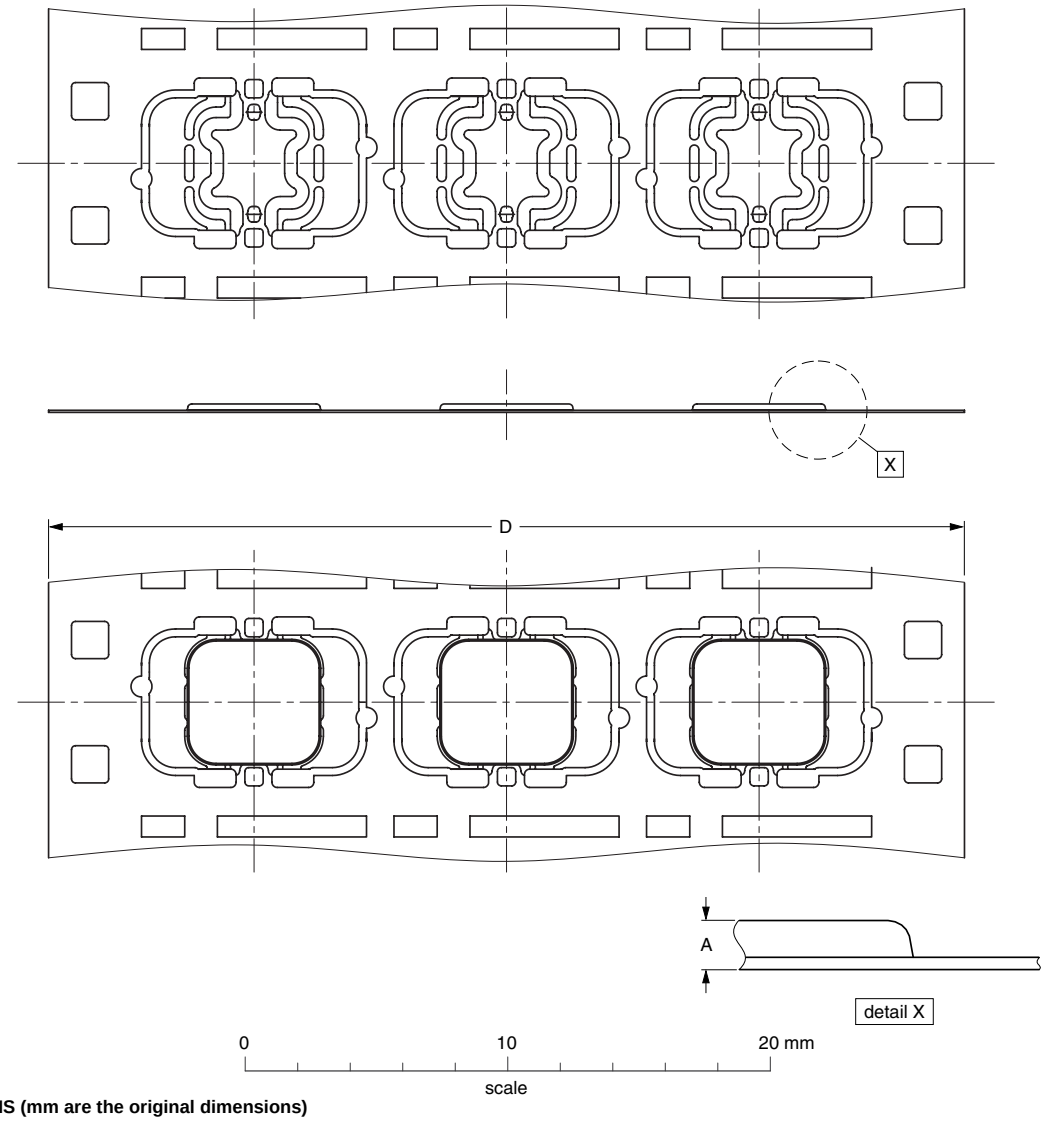
[1] Stresses above one or more of the values may cause permanent damage to the device.

[2] Exposure to limiting values for extended periods may affect device reliability.

[3] LCR meter, T_{amb} = 22 °C, f_i = 13.56 MHz, 2.8 V RMS.

14. Package outline

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-2**



DIMENSIONS (mm are the original dimensions)

UNIT	A(1) max.	D	
mm	0.33	35.05 34.95	For unspecified dimensions see PLLMC-drawing given in the subpackage code.

Note

1. Total package thickness, exclusive punching burr.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT500-2	- - -	- - -	- - -			~~03-09-17~~ 06-05-22

Fig 20. Package outline SOT500-2

15. Abbreviations

Table 24. Abbreviations and symbols

Acronym	Description
ATQA	Answer To reQuest, Type A
CRC	Cyclic Redundancy Check
EEPROM	Electrically Erasable Programmable Read-Only Memory
FFC	Film Frame Carrier
IC	Integrated Circuit
LCR	L = inductance, Capacitance, Resistance (LCR meter)
LSB	Least Significant Bit
NAK	Not AcKnowledge
NUID	Non-Unique IDentifier
NV	Non-Volatile memory
PCD	Proximity Coupling Device (Contactless Reader)
PICC	Proximity Integrated Circuit Card (Contactless Card)
REQA	REQuest command, Type A
RF	Radio Frequency
RMS	Root Mean Square
SAK	Select AcKnowledge, type A
SECS-II	SEMI Equipment Communications Standard part 2
TiW	Titanium Tungsten
UID	Unique IDentifier
WUPA	Wake-Up Protocol type A

16. References

[1] **MIFARE (Card) Coil Design Guide —** Application note, BU-ID Document number 0117**[1]

[2] **MIFARE Type Identification Procedure —** Application note, BU-ID Document number 0184**

[3] **ISO/IEC 14443-2 —** 2001

[4] **ISO/IEC 14443-3 —** 2001

[5] **MIFARE & I-Code CL RC632 Multiple protocol contactless reader IC —** Product data sheet

[6] **MIFARE and handling of UIDs —** Application note, BU-ID Document number 1907**

1. ** ... document version number

17. Revision history

Table 25. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF1S5009 v.3.1	20100727	Product data sheet	-	MF1S5009 v.3.0
Modifications:	• All drawings updated			
MF1S5009 v.3.0	20100610	Product data sheet	-	-

18. Legal information

18.1 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.

18.2 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.

Product specification — The information and data provided in a Product data sheet shall define the specification of the product as agreed between NXP Semiconductors and its customer, unless NXP Semiconductors and customer have explicitly agreed otherwise in writing. In no event however, shall an agreement be valid in which the NXP Semiconductors product is deemed to offer functions and qualities beyond those described in the Product data sheet.

18.3 Disclaimers

Limited warranty and liability — 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.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

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 life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an 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.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial 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, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

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.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

18.4 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.

19. Contact information

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

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

20. Tables

21. Figures

22. Contents

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

Date of release: 27 July 2010
189131