MF1S70yyX

MIFARE Classic 4K - Mainstream contactless smart card IC for fast and easy solution development

Rev. 3.0 — 2 May 2011
196430

Product data sheet
COMPANY PUBLIC

1. General description

NXP Semiconductors has developed the MIFARE Classic MF1S70yyX to be used in a contactless smart card according to ISO/IEC 14443 Type A.

The MIFARE Classic 4K MF1S70yyX IC is used in applications like public transport ticketing and can also be used for various other applications.

1.1 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 interference from another card in the field.

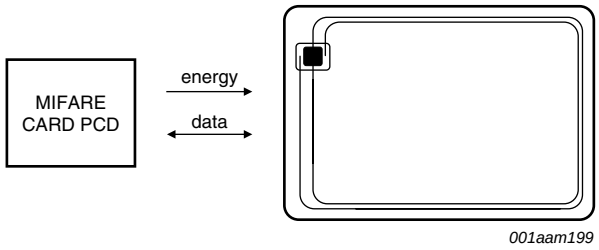


Fig 1. MIFARE card reader

1.2 Simple integration and user convenience

The MF1S70yyX is designed for simple integration and user convenience which allows complete ticketing transactions to be handled in less than 100 ms.

1.3 Security

- Manufacturer programmed 7-byte UID or 4-byte NUID identifier for each device
- Random ID support
- Mutual three pass authentication (ISO/IEC DIS 9798-2)
- Individual set of two keys per sector to support multi-application with key hierarchy

1.4 Delivery options

- 7-byte UID, 4-byte NUID
- bumped die on wafer
- MOA4 and MOA8 contactless module

2. Features and benefits

- Contactless transmission of data and supply energy
- Operating frequency of 13.56 MHz
- Data integrity of 16-bit CRC, parity, bit coding, bit counting
- Typical ticketing transaction time of < 100 ms (including backup management)
- Operating distance up to 100 mm depending on antenna geometry and reader configuration
- Data transfer of 106 kbit/s
- Anticollision

2.1 EEPROM

- 4 kB, organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks (one block consists of 16 byte)
- Data retention time of 10 years
- User definable access conditions for each memory block
- Write endurance 100000 cycles

3. Applications

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

4. Quick reference data

Table 1. Quick reference data

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance		[1]	14.9	16.9	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] LCR meter, T_{amb} = 22 °C, f_i = 13.56 MHz, 2 V RMS.

5. Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
MF1S7001XDUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID	-
MF1S7001XDUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 7-byte UID	-
MF1S7000XDA4	MOA4	plastic leadless module carrier package; 35 mm wide tape, 7-byte UID	SOT500-2
MF1S7000XDA8	MOA8	plastic leadless module carrier package; 35 mm wide tape, 7-byte UID	SOT500-4
MF1S7031XDUD	FFC Bump	8 inch wafer, 120 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID	-
MF1S7031XDUF	FFC Bump	8 inch wafer, 75 μm thickness, on film frame carrier, electronic fail die marking according to SECS-II format), Au bumps, 4-byte non-unique ID	-
MF1S7030XDA4	MOA4	plastic leadless module carrier package; 35 mm wide tape, 4-byte non-unique ID	SOT500-2
MF1S7030XDA8	MOA8	plastic leadless module carrier package; 35 mm wide tape, 4-byte non-unique ID	SOT500-4

6. Block diagram

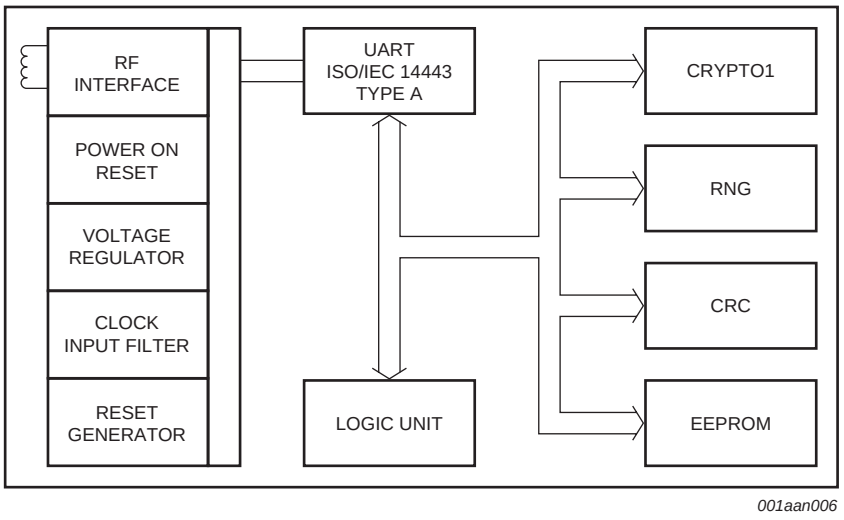


Fig 2. Block diagram of MF1S70yyX

7. Pinning information

7.1 Pinning

The pinning for the MF1S70yyXDAx is shown as an example in Figure 3 for the MOA4 contactless module. For the contactless module MOA8, the pinning is analogous and not explicitly shown.

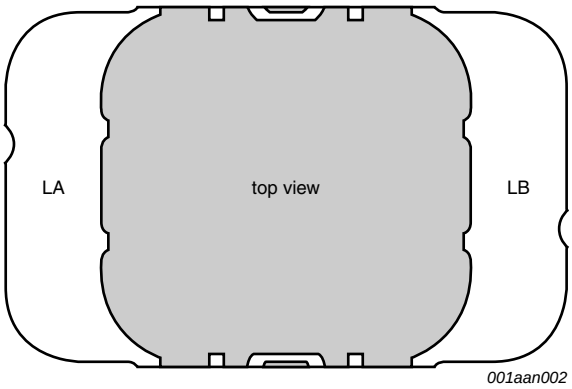


Fig 3. Pin configuration for SOT500-2 (MOA4)

Table 3. Pin allocation table

Pin	Symbol	
LA	LA	Antenna coil connection LA
LB	LB	Antenna coil connection LB

8. Functional description

8.1 Block description

The MF1S70yyX chip consists of a 4 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 MF1S70yyX. 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 MF1S70yyX is used for authentication and encryption of data exchange.
- EEPROM: 4 kB is organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks. One 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.

8.2 Communication principle

The commands are initiated by the reader and controlled by the Digital Control Unit of the MF1S70yyX. The command response is depending on the state of the IC and for memory operations also on the access conditions valid for the corresponding sector.

8.2.1 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 9.4, ATQA according to ISO/IEC 14443A).

8.2.2 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. If the 7-byte UID is used for anticollision and selection, two cascade levels need to be processes as defined in ISO/IEC 14443-3.

Remark: For the 4-byte non-unique ID product versions, the identifier retrieved from the card is not defined to be unique. For further information regarding handling of non-unique identifiers see Ref. 6.

8.2.3 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 9.4. For further details refer to the document Ref. 2.

8.2.4 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.

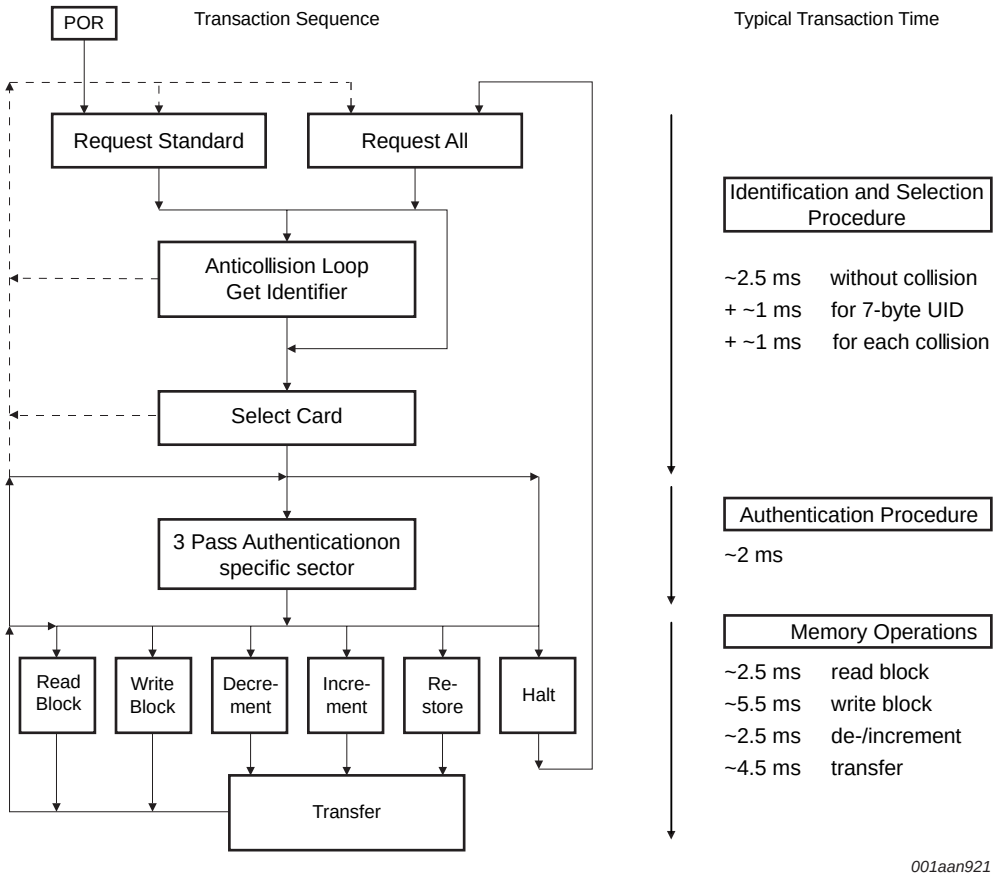


Fig 4. Three pass authentication

8.2.5 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 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 an internal data-register
- Transfer: Writes the contents of the temporary internal data-register to a value block

8.3 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)

8.4 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 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.

8.5 RF interface

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

For operation, the carrier field from the reader always needs to be present (with short pauses when transmitting), as 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).

8.6 Memory organization

The 4096 × 8 bit EEPROM memory is organized in 32 sectors of 4 blocks and 8 sectors of 16 blocks. One block contains 16 bytes.

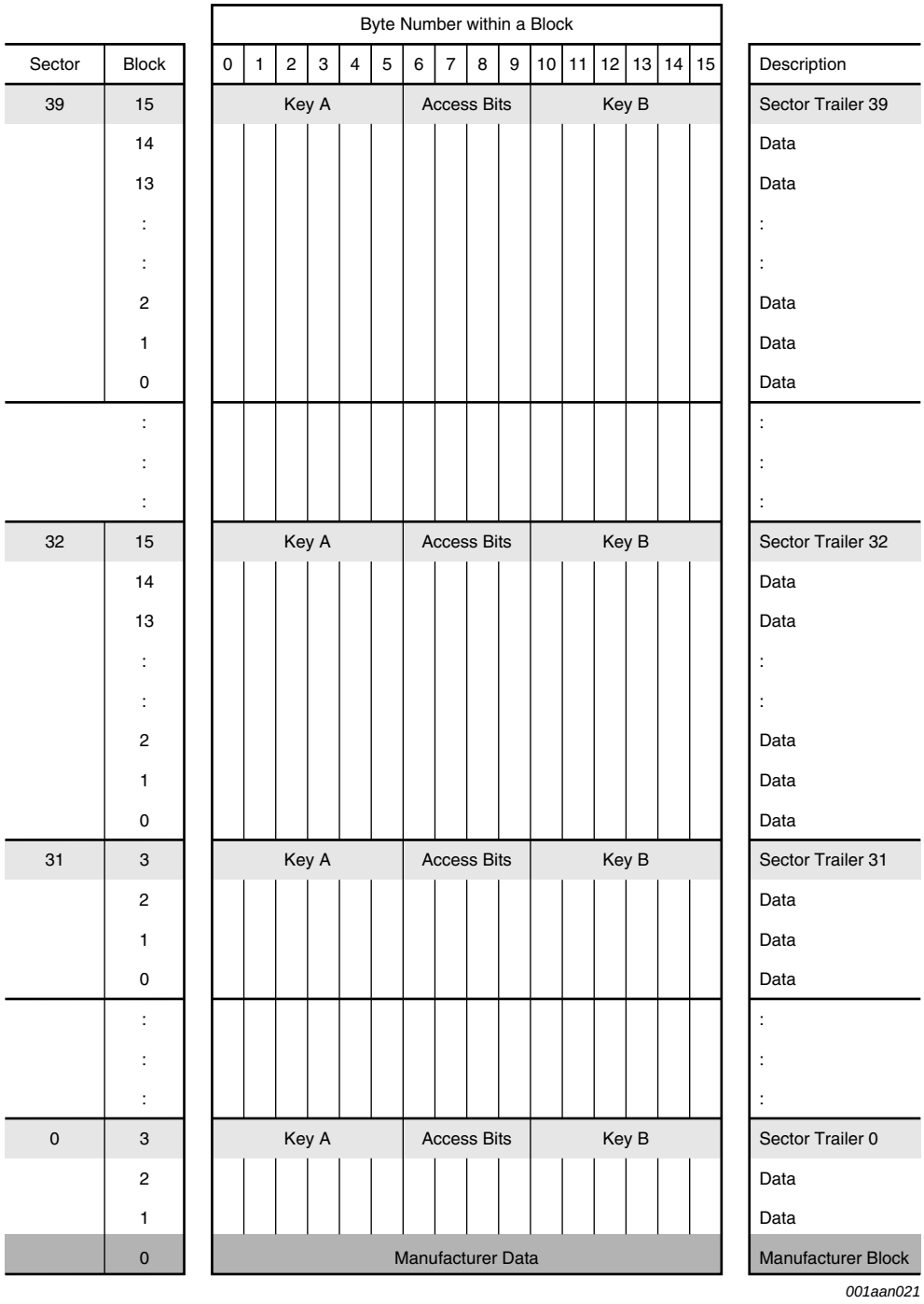


Fig 5. Memory organization

8.6.1 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. The manufacturer block is shown in Figure 6 and Figure 7 for the 4-byte NUID and 7-byte UID version respectively.

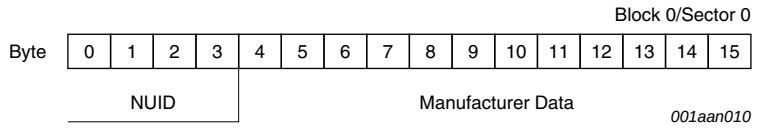


Fig 6. Manufacturer block for MF1S703yX with 4-byte NUID

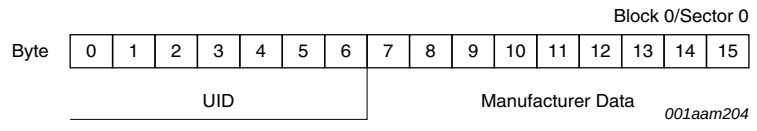


Fig 7. Manufacturer block for MF1S700yX with 7-byte UID

8.6.2 Data blocks

One block consists of 16 bytes. The first 32 sectors contain 3 blocks and the last 8 sectors 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
- value blocks

Value blocks can be used for e.g. electronic purse applications, where additional commands like increment and decrement for direct control of the stored value are provided

A successful authentication has to be performed to allow any memory operation.

Remark: The default content of the data blocks at delivery is not defined.

8.6.2.1 Value blocks

Value blocks allow performing electronic purse functions (valid commands are: read, write, increment, decrement, restore, transfer). 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 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.

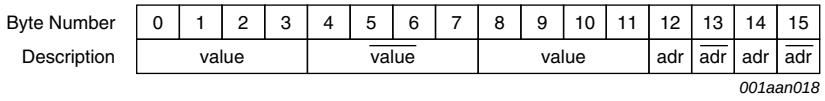


Fig 8. Value blocks

An example of a valid value block format for the decimal value 1234567d and the block address 17d is shown in Table 4. First, the decimal value has to be converted to the hexadecimal representation of 0012D687h. The LSByte of the hexadecimal value is stored in Byte 0, the MSByte in Byte 3. The bit inverted hexadecimal representation of the value is FFED2978h where the LSByte is stored in Byte 4 and the MSByte in Byte 7.

The hexadecimal value of the address in the example is 11h, the bit inverted hexadecimal value is EEh.

Table 4. Value block format example

Byte Number	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
Description		**value**				**value**				**value**			**adr**	**adr**	**adr**	**adr**
Values [hex]	84	D6	12	00	78	29	ED	FF	84	D6	12	00	11	EE	11	EE

8.6.3 Sector trailer

The sector trailer is always the last block in one sector. For the first 32 sectors this is block 3 and for the remaining 8 sectors it is block 15. Each sector has a sector trailer containing the

- secret keys A (mandatory) and B (optional), which return logical “0”s when read and
- the access conditions for the blocks of that sector, which are stored in bytes 6...9. The access bits also specify the type (data 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. The access bits for the sector trailer have to be configured accordingly, see Section 8.7.2.

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.

When the sector trailer is read, the key bytes are blanked out by returning logical zeros. If key B is configured to be readable, the data stored in bytes 10 to 15 is returned, see Section 8.7.2.

All keys are set to FFFF FFFF FFFFh at chip delivery.

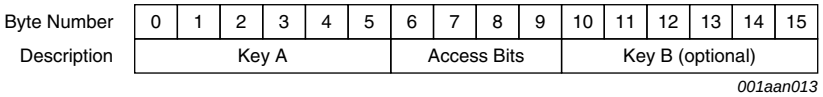


Fig 9. Sector trailer

8.7 Memory access

Before any memory operation can be done, the card has to be selected and authenticated as described in Section 8.2. The possible memory operations for an addressed block depend on the key used during authentication and the access conditions stored in the associated sector trailer.

Table 5. 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

8.7.1 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 irreversibly blocked.

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

The internal logic of the MF1S70yyX ensures that the commands are executed only after a successful authentication.

Table 6. Access conditions

Access Bits	Valid Commands		Block (sectors 0 - 31)	Block(s) (sectors 32-39)	Description
$C1_3$, $C2_3$, $C3_3$	read, write	→	3	15	sector trailer
$C1_2$, $C2_2$, $C3_2$	read, write, increment, decrement, transfer, restore	→	2	10-14	data block(s)
$C1_1$, $C2_1$, $C3_1$	read, write, increment, decrement, transfer, restore	→	1	5-9	data block(s)
$C1_0$, $C2_0$, $C3_0$	read, write, increment, decrement, transfer, restore	→	0	0-4	data block(s)

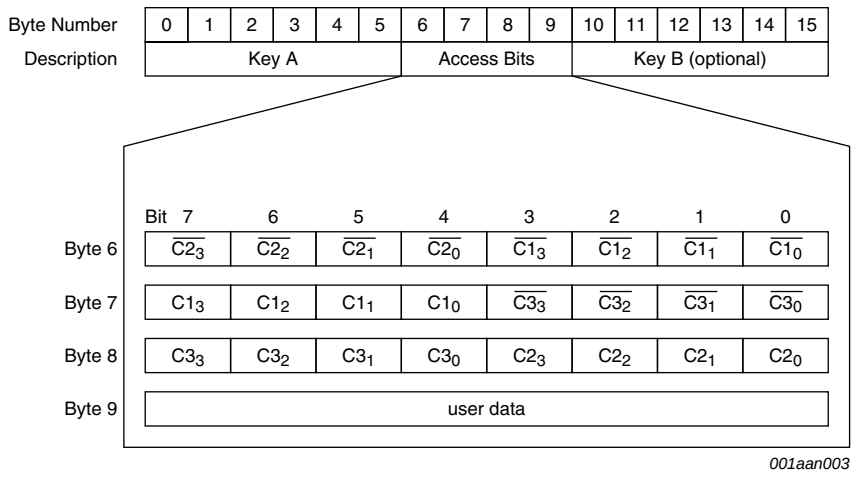


Fig 10. Access conditions

8.7.2 Access conditions for the sector trailer

Depending on the access bits for the sector trailer (block 3, respectively block 15) 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 the transport configuration, new cards must be authenticated with key A. Since the access bits themselves can also be blocked, special care has to be taken during the personalization of cards.

Table 7. 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

8.7.3 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. With access condition ‘001’ only read and decrement are possible which reflects a non-rechargeable card. For access condition ‘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 8. 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	key A|B	key A|B	key A|B	transport configuration[1]
0	1	0	key A|B	never	never	never	read/write block[1]
1	0	0	key A|B	key B	never	never	read/write block[1]
1	1	0	key A|B	key B	key B	key A|B	value block[1]
0	0	1	key A|B	never	never	key A|B	value block[1]
0	1	1	key B	key B	never	never	read/write block[1]
1	0	1	key B	never	never	never	read/write block[1]
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 (see grey marked lines in Table 7). As a consequences, if the reader authenticates any block of a sector which uses such access conditions for the Sector Trailer and using key B, the card will refuse any subsequent memory access after authentication.

9. Command overview

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

9.1 MIFARE Classic 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 9.

Table 9. 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
Select CL1	Select CL1	93h 70h
Anticollision CL2	Anticollision CL2	95h 20h
Select CL2	Select CL2	95h 70h
Halt	Halt	50h 00h
Authentication with Key A	-	60h
Authentication with Key B	-	61h
Personalize UID Usage	-	40h
MIFARE Read	-	30h
MIFARE Write	-	A0h
MIFARE Decrement	-	C0h
MIFARE Increment	-	C1h
MIFARE Restore	-	C2h
MIFARE Transfer	-	B0h

All commands use the coding and framing as described in Ref. 3 and Ref. 4 if not otherwise specified.

9.2 Timings

The timing shown in this document are not to scale and values are rounded to 1 μs.

All 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.

The frame delay time from PICC to PCD must be at least 87 μs.

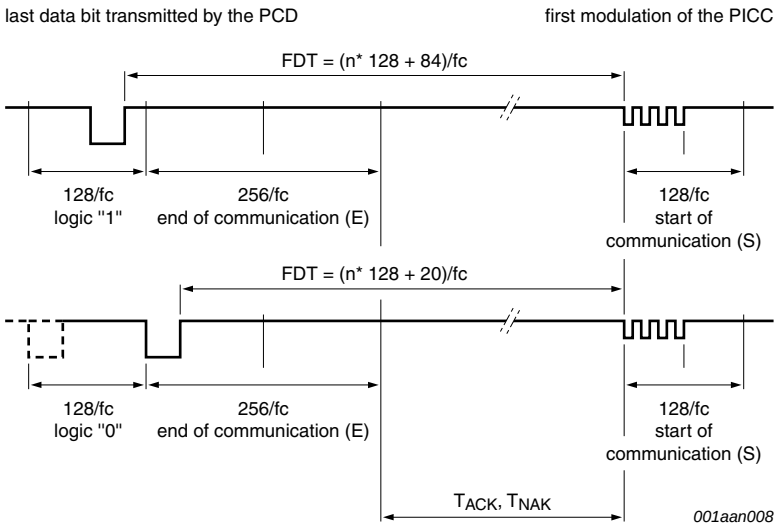


Fig 11. Frame Delay Time (from PCD to PICC) and T_{ACK} and T_{NAK}

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

9.3 MIFARE Classic ACK and NAK

The MIFARE Classic uses a 4 bit ACK / NAK as shown in Table 10.

Table 10. MIFARE ACK and NAK

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

9.4 ATQA and SAK responses

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

The MF1S70yyX answers to a REQA or WUPA command with the ATQA value shown in Table 11 and to a Select CL1 command (CL2 for the 7-byte UID variant) with the SAK value shown in Table 12.

Table 11. ATQA response of the MF1S70yyX

		Bit Number														
Sales Type	**Hex Value**	**16**	**15**	**14**	**13**	**12**	**11**	**10**	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
MF1S700yX	00 42h	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
MF1S703yX	00 02h	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Table 12. SAK response of the MF1S70yyX

		Bit Number							
Sales Type	**Hex Value**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
MF1S70yyX	18h	0	0	0	1	1	0	0	0

10. UID Options and Handling

The MF1S70yyX product family offers two delivery options for the UID which is stored in block 0 of sector 0.

- 7-byte UID
- 4-byte NUID (Non-Unique ID)

This section describes the MIFARE Classic MF1S70yyX operation when using one of the 2 UID options with respect to card selection, authentication and personalization. See also Ref. 6 for details on how to handle UIDs and NUIDs with MIFARE Classic products.

10.1 7-byte UID Operation

All MF1S70**0**yXDyy products are featuring a 7-byte UID. This 7-byte UID is stored in block 0 of sector 0 as shown in Figure 7. The behaviour during anti-collision, selection and authentication can be configured during personalization for this UID variant.

10.1.1 Personalization Options

The 7-byte UID variants of the MF1S70yyX can be operated with four different functionalities, denoted as UIDFn (UID Functionality n).

1. UIDF0: anti-collision and selection with the double size UID according to ISO/IEC 14443-3
2. UIDF1: anti-collision and selection with the double size UID according to ISO/IEC 14443-3 and optional usage of a selection process shortcut
3. UIDF2: anti-collision and selection with a single size random ID according to ISO/IEC 14443-3
4. UIDF3: anti-collision and selection with a single size NUID according to ISO/IEC 14443-3 where the NUID is calculated out of the 7-byte UID

The anti-collision and selection procedure and the implications on the authentication process are detailed in Section 10.1.2 and Section 10.1.3.

The default configuration at delivery is option 1 which enables the ISO/IEC 14443-3 compliant anti-collision and selection. This configuration can be changed using the ‘Personalize UID Usage’ command. The execution of this command requires an authentication to sector 0. Once this command has been issued and accepted by the PICC, the configuration is automatically locked. A subsequently issued ‘Personalize UID Usage’ command is not executed and a NAK is replied by the PICC.

Remark: As the configuration is changeable at delivery, it is strongly recommended to send this command at personalization of the card to prevent unwanted changes in the field. This should also be done if the default configuration is used.

Remark: The configuration only becomes effective only after PICC unselect or PICC field reset.

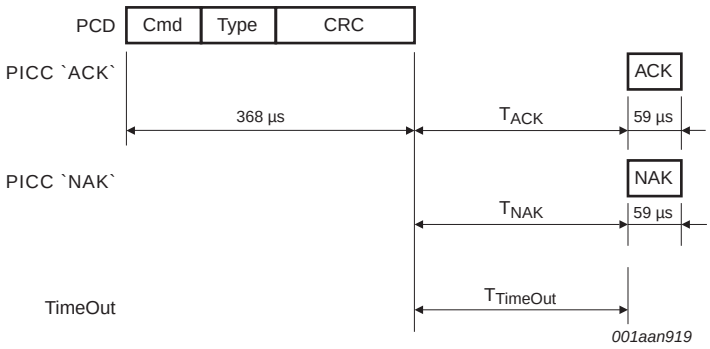


Fig 12. Personalize UID Usage

Table 13. Personalize UID Usage command

Name	Code	Description	Length
Cmd	40h	Set anti-collision, selection and authentication behaviour	1 byte
Type	-	Encoded type of UID usage: UIDF0: 00h UIDF1: 40h UIDF2: 20h UIDF3: 60h	1 byte
CRC	-	CRC according to Ref. 4	2 bytes
ACK, NAK	see Table 10	see Section 9.3	4-bit

Table 14. Personalize UID Usage timing

These times exclude the end of communication of the PCD.

	T_{ACK} min	T_{ACK} max	T_{NAK} min	T_{NAK} max	$T_{TimeOut}$
Personalize UID Usage	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	10 ms

10.1.2 Anti-collision and Selection

Depending on the chosen personalization option there are certain possibilities to perform anti-collision and selection. To bring the MIFARE Classic into the ACTIVE state according to ISO/IEC 14443-3, the following sequences are available.

Sequence 1: ISO/IEC 14443-3 compliant anti-collision and selection using the cascade level 1 followed by the cascade level 2 SEL command

Sequence 2: using cascade level 1 anti-collision and selection procedure followed by a Read command from block 0

Sequence 3: ISO/IEC 14443-3 compliant anti-collision and selection using the cascade level 1 SEL command

Remark: The Read from Block 0 in Sequence 2 does not require a prior authentication to Sector 0 and is transmitted in plain data. For all other sequences, the readout from Block 0 in Sector 0 is encrypted and requires an authentication to that sector.

Table 15. Available activation sequences for 7-byte UID options

UID Functionality	Available Activation Sequences
UIDF0	Sequence 1
UIDF1	Sequence 1, Sequence 2
UIDF2	Sequence 3
UIDF3	Sequence 3

10.1.3 Authentication

During the authentication process, 4-byte of the UID are passed on to the MIFARE Classic Authenticate command of the contactless reader IC. Depending on the activation sequence, those 4-byte are chosen differently.

Table 16. Input parameter to MIFARE Classic Authenticate

UID Functionality	Input to MIFARE Classic Authenticate Command
Sequence 1	CL2 bytes (UID3...UID6)
Sequence 2	CL1 bytes (CT, UID0...UID2)
Sequence 3	4-byte NUID/RID (UID0...UID3)

10.2 4-byte UID Operation

All MF1S70**3**yXDyy products are featuring a 4-byte NUID. This 4-byte NUID is stored in block 0 of sector 0 as shown in Figure 6.

10.2.1 Anti-collision and Selection

The anti-collision and selection process for the product variants featuring 4-byte NUIDs is done according to ISO/IEC 14443-3 Type A using cascade level 1 only.

10.2.2 Authentication

The input parameter to the MIFARE Classic Authenticate command is the full 4-byte UID retrieved during the anti-collision procedure. This is the same as for the activation Sequence 3 in the 7-byte UID variant.

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 13, Figure 14 and Table 17.

Table 18 shows the required timing.

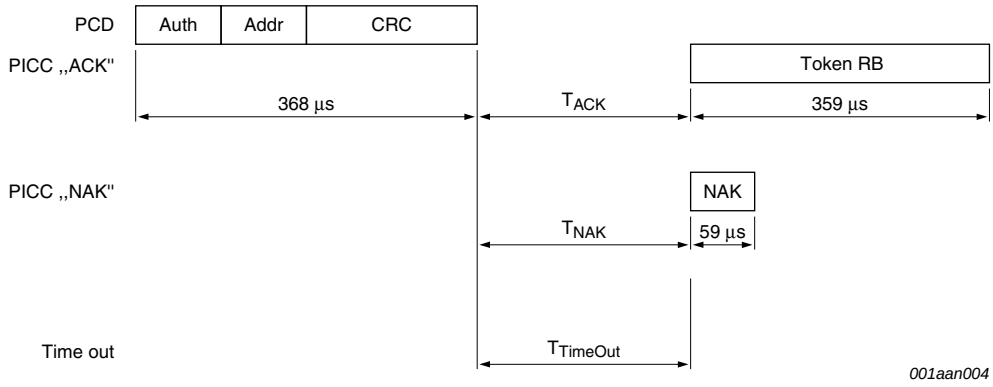


Fig 13. MIFARE Authentication part 1

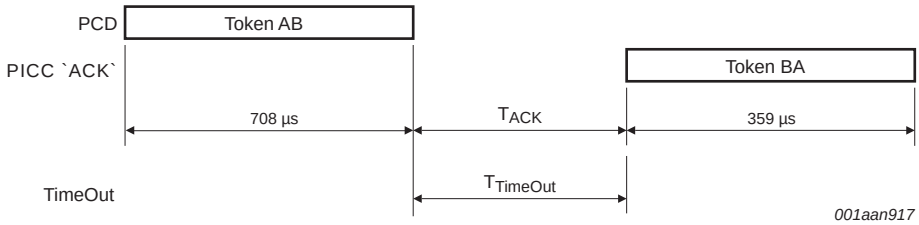


Fig 14. MIFARE Authentication part 2

Table 17. 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 (encrypted data)	8 bytes
Token BA	-	Challenge 2 (encrypted data)	4 bytes
NAK	see Table 10	see Section 9.3	4-bit

Table 18. 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	71 µs	$T_{TimeOut}$	71 µs	$T_{TimeOut}$	1 ms
Authentication part 2	71 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 time 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). The 4-byte input parameter for the MIFARE Classic Authentication is detailed in Section 10.1.3 and Section 10.2.2.

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 15 and Table 19.

Table 20 shows the required timing.

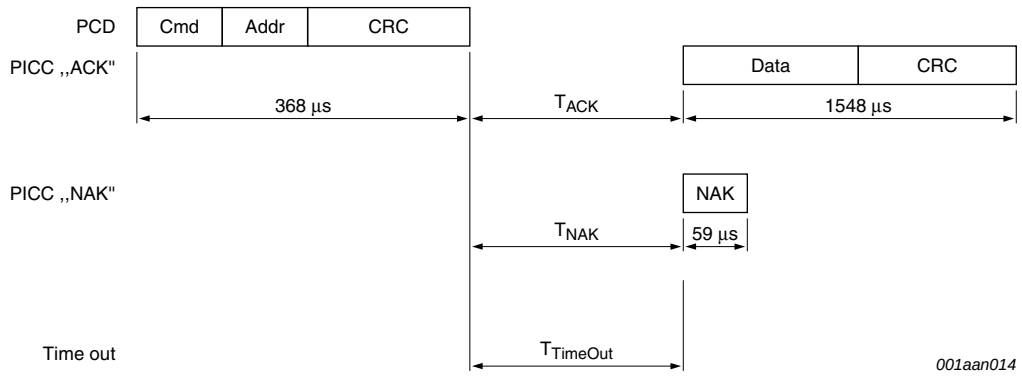


Fig 15. MIFARE Read

Table 19. 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 10	see Section 9.3	4-bit

Table 20. 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 4K block. It needs two pairs of command-response. These two parts, MIFARE Write part 1 and part 2 are shown in Figure 16 and Figure 17 and Table 21.

Table 22 shows the required timing.

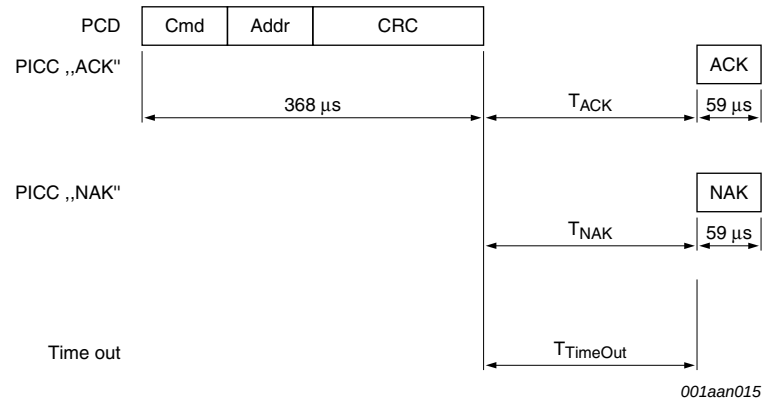


Fig 16. MIFARE Write part 1

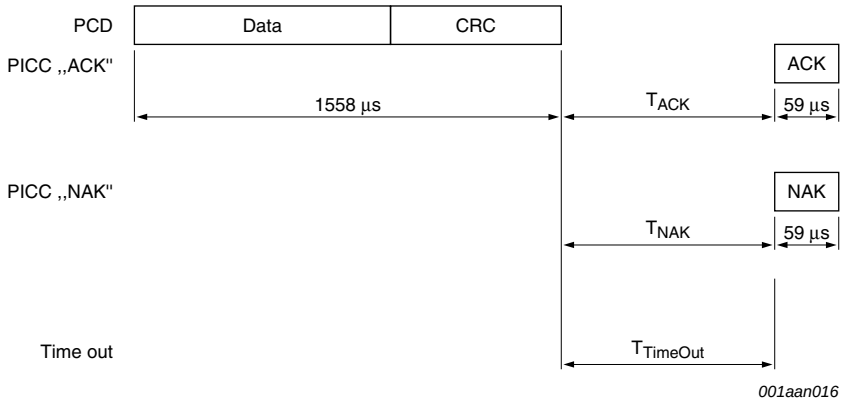


Fig 17. MIFARE Write part 2

Table 21. MIFARE Write command

Name	Code	Description	Length
Cmd	A0h	Write 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 10	see Section 9.3	4-bit

Table 22. 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 according to Ref. 4. There is no maximum time 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.

All three commands are responding with a NAK to the first command part if the addressed block is not formatted to be a valid value block, see Section 8.6.2.1.

The two parts of each command are shown in Figure 18 and Figure 19 and Table 23.

Table 24 shows the required timing.

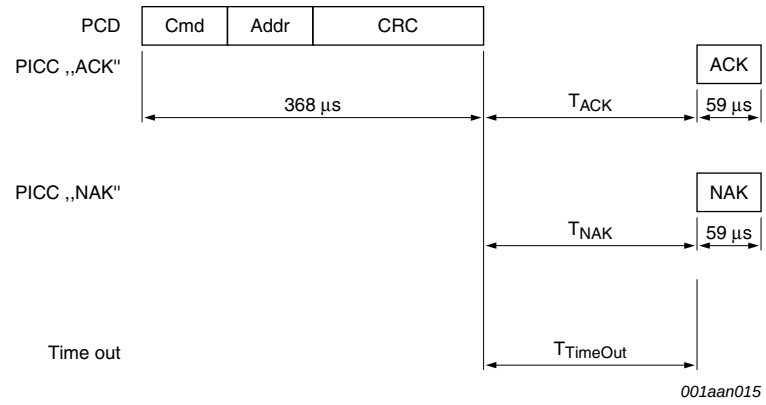
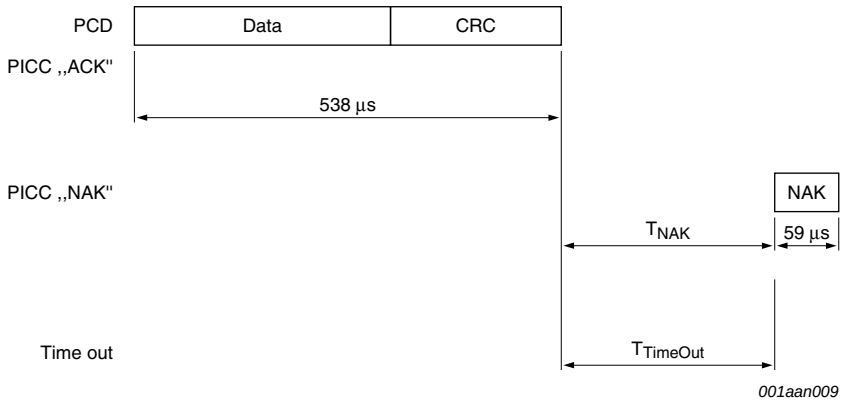


Fig 18. MIFARE Increment, Decrement, Restore part 1



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

Fig 19. MIFARE Increment, Decrement, Restore part 2

Table 23. 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 10	see Section 9.3	4-bit

Table 24. 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 according to Ref. 4. There is no maximum time 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 20 and Table 25.

Table 26 shows the required timing.

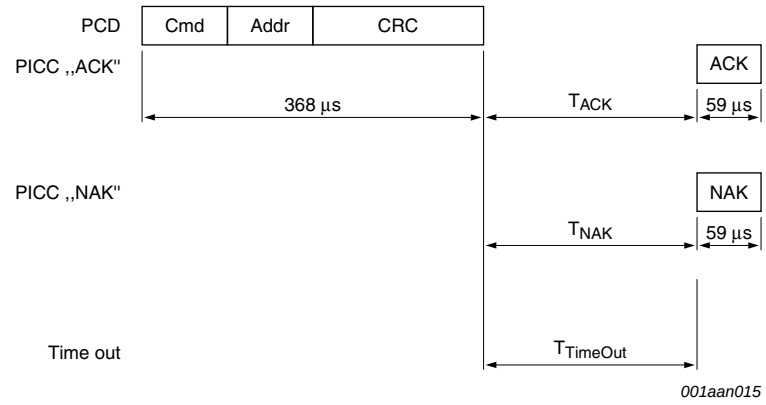


Fig 20. MIFARE Transfer

Table 25. 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 10	see Section 9.3	4-bit

Table 26. 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

Stresses above one or more of the limiting values may cause permanent damage to the device. Exposure to limiting values for extended periods may affect device reliability.

Table 27. Limiting values

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		-	120	mW
T_{stg}	storage temperature		−55	125	°C
T_{amb}	ambient temperature		−25	70	°C
V_{ESD}	electrostatic discharge voltage on LA/LB	[1]	2	-	kV
I_{lu}	latch-up current		±100	-	mA

[1] ANSI/ESDA/JEDEC JS-001; Human body model: C = 100 pF, R = 1.5 kΩ

13. Characteristics

Table 28. Characteristics

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
C_i	input capacitance		[1]	14.9	16.9	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] LCR meter, T_{amb} = 22 °C, f_i = 13.56 MHz, 2 V RMS.

14. Wafer specification

For more details on the wafer delivery forms see Ref. 9.

Table 29. Wafer specifications MF1S70yyXDUy

Wafer		
diameter		200 mm typical (8 inches)
maximum diameter after foil expansion		210 mm
thickness	MF1S70yyXDUD	120 μm ± 15 μm
	MF1S70yyXDUF	75 μm ± 10 μm
flatness		not applicable
Potential Good Dies per Wafer (PGDW)		est. 66264
Wafer backside		
material		Si
treatment		ground and stress relieve
roughness		R_a max = 0.5 μm
		R_t max = 5 μm
Chip dimensions		
step size[1]		x = 659 μm
		y = 694 μm
gap between chips[1]		typical = 19 μm
		minimum = 5 μm
Passivation		
type		sandwich structure
material		PSG / nitride
thickness		500 nm / 600 nm
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, VSS, TEST[2] = 66 μm × 66 μm
size variation		±5 μm
under bump metallization		sputtered TiW

[1] The step size and the gap between chips may vary due to changing foil expansion

[2] Pads VSS and TESTIO are disconnected when wafer is sawn.

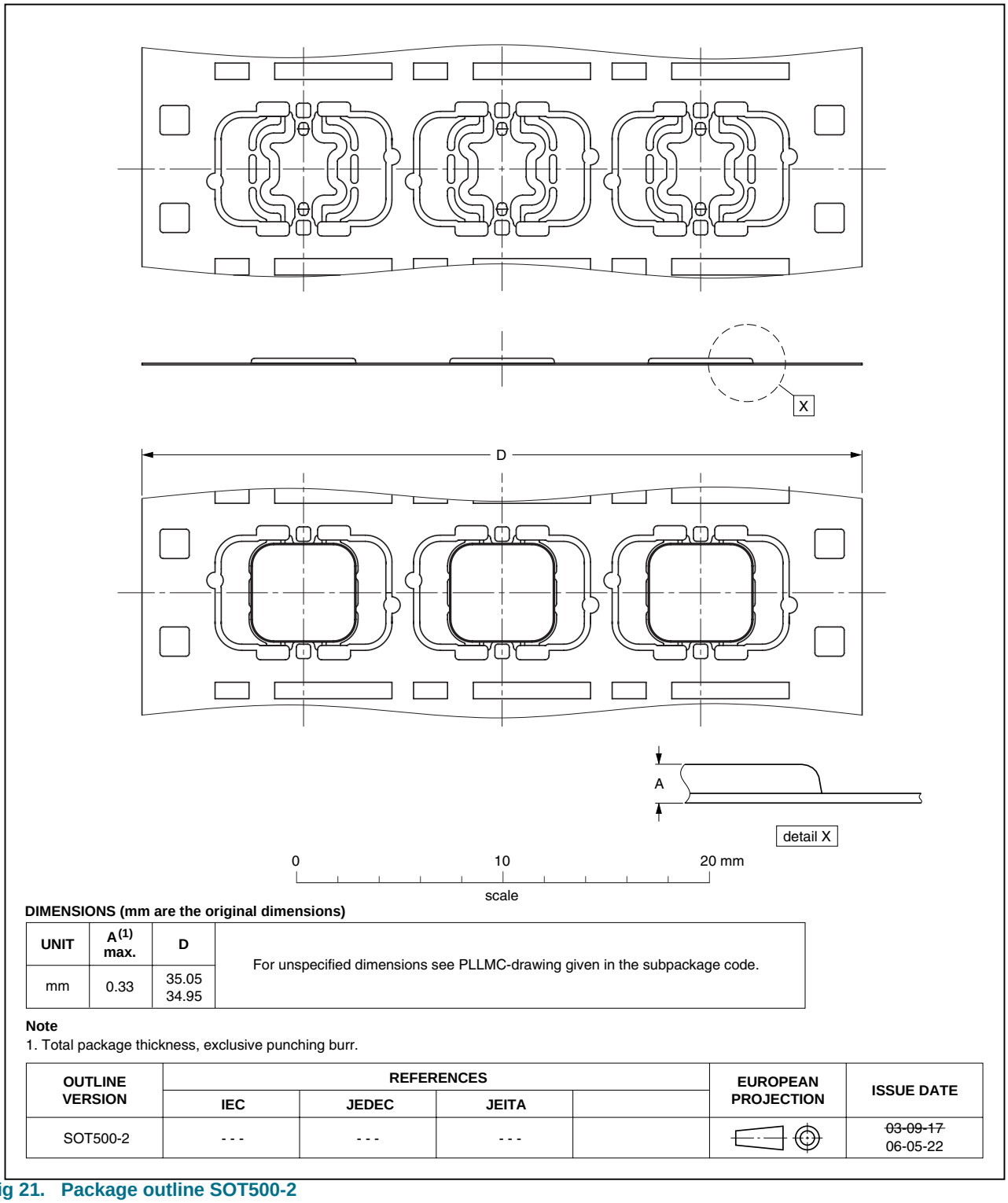
14.1 Fail die identification

Electronic wafer mapping covers the electrical test results and additionally the results of mechanical/visual inspection. No ink dots are applied.

14.2 Package outline

For more details on the contactless modules MOA4 and MOA8 please refer to Ref. 7 and Ref. 8.

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.

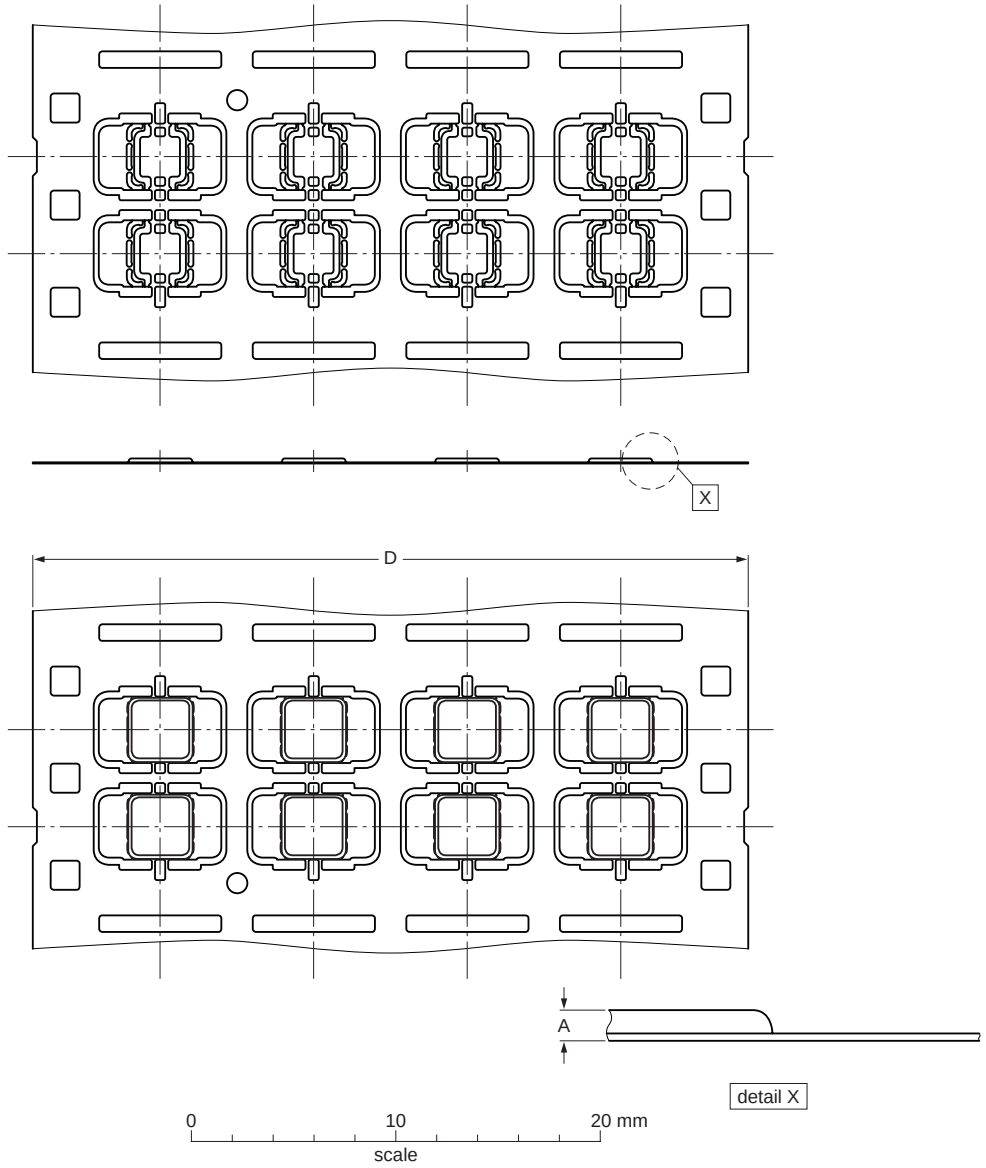
Note

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 21. Package outline SOT500-2

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-4**



Dimensions

Unit		$A^{(1)}$	D
mm	max	0.26	35.05
	nom		35.00
	min		34.95

For unspecified dimensions see PLLMC-drawing given in the subpackage code.

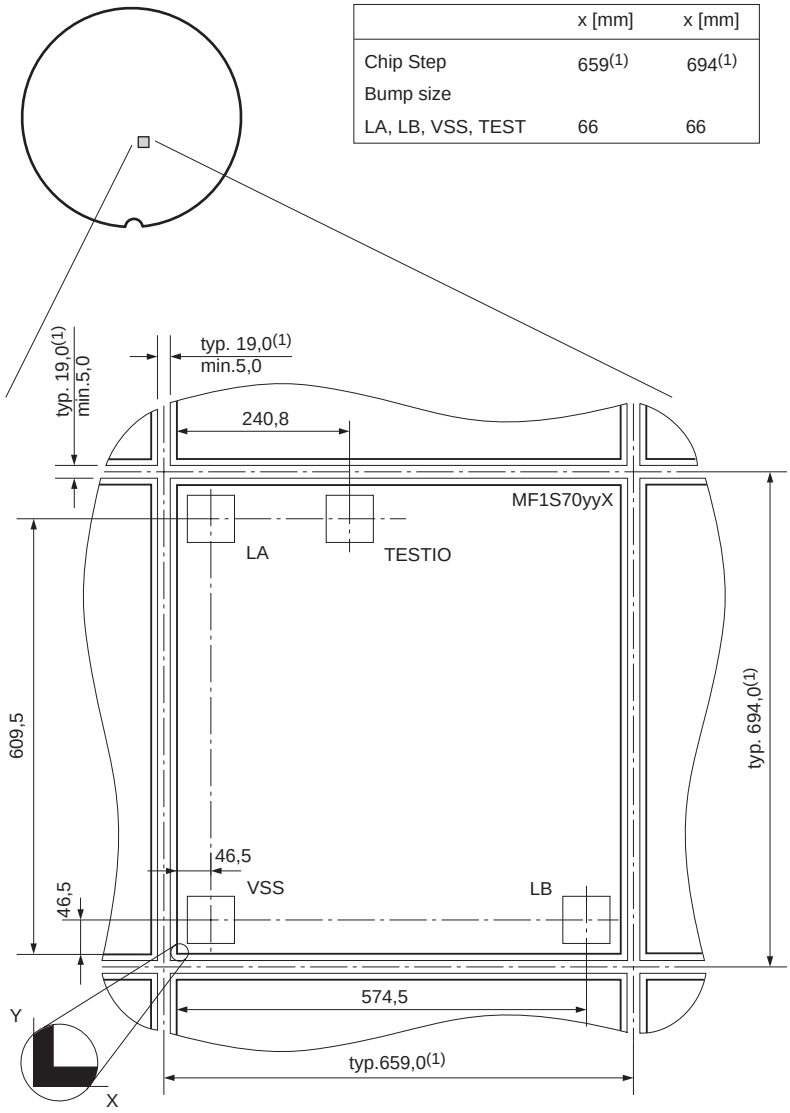
Note
1. Total package thickness, exclusive punching burr.

sot500-4_po

Outline version	References				European projection	Issue date
	IEC	JEDEC	JEITA			
SOT500-4	- - -	- - -	- - -			11-02-18

Fig 22. Package outline SOT500-4

14.3 Bare die outline



(1) the air gap and thus the step size may vary due to varying foil expansion

(2) all dimensions in mm, pad locations measured from metal ring edge (see detail)

001aan922

Fig 23. Bare die outline MF1S70yyX

15. Abbreviations

Table 30. Abbreviations and symbols

Acronym	Description
ACK	ACKnowledge
ATQA	Answer To reQuest, Type A
CRC	Cyclic Redundancy Check
CT	Cascade Tag (value 88h) as defined in ISO/IEC 14443-3 Type A
EEPROM	Electrically Erasable Programmable Read-Only Memory
FDT	Frame Delay Time
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
RID	Random ID
RF	Radio Frequency
RMS	Root Mean Square
SAK	Select AcKnowledge, type A
RNG	Random Number Generator
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**[1]

[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]

[7] **Contactless smart card module specification MOA4 —** Delivery Type Description, BU-ID Document number 0823**[1]

[8] **Contactless smart card module specification MOA8 —** Delivery Type Description, BU-ID Document number 1636**[1]

[9] **General specification for 8" wafer on UV-tape; delivery types —** Delivery Type Description, BU-ID Document number 1005**[1]

1. ** ... document version number

17. Revision history

Table 31. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF1S70YYX v.3.0	20110502	Product data sheet	-	MF1S70YYX v.2.0
Modifications:	• General update			
MF1S70YYX v.2.0	20101027	Preliminary 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.

Quick reference data — The Quick reference data is an extract of the product data given in the Limiting values and Characteristics sections of this document, and as such is not complete, exhaustive or legally binding.

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.

Bare die — All die are tested on compliance with their related technical specifications as stated in this data sheet up to the point of wafer sawing and are handled in accordance with the NXP Semiconductors storage and transportation conditions. If there are data sheet limits not guaranteed, these will be separately indicated in the data sheet. There are no post-packing tests performed on individual die or wafers.

NXP Semiconductors has no control of third party procedures in the sawing, handling, packing or assembly of the die. Accordingly, NXP Semiconductors assumes no liability for device functionality or performance of the die or systems after third party sawing, handling, packing or assembly of the die. It is the responsibility of the customer to test and qualify their application in which the die is used.

All die sales are conditioned upon and subject to the customer entering into a written die sale agreement with NXP Semiconductors through its legal department.

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: 2 May 2011
196430