

APPLICATION NOTE

AN02105

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

Revision 1.2

2002 September 06
067512

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

CONTENTS

1	INTRODUCTION	3
2	SECURE ACCESS PRINCIPLE	4
2.1	Security levels	4
3	GENERAL REQUIREMENTS AND SPECIFICATIONS	5
3.1	Access condition matrix (ACM)	5
3.2	Read access	5
3.3	Write access	5
3.4	Block 0 access	5
4	GENERATION OF THE MF_PASSWORD	6
4.1	Start Value	6
4.2	Loading of DES Keys	6
4.3	EXAMPLES	8
4.4	Generation Tools	9
5	REVISION HISTORY	10

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

1 INTRODUCTION

This application note describes the handling of the secure access to the MIFARE[®] memory on Dual Interface Smart Card ICs.

The Dual Interface Smart Card ICs use 1 KByte or 4 KByte (configuration B1 or B4) of their build-in EEPROM to store the content of the MIFARE[®] memory. A build-in MIFARE[®] OS provides a fully MIFARE[®] compliant command set via the contactless interface. Additionally two commands called eePasswordRead and eePasswordWrite are supported by the MIFARE[®] OS. They have to be used by the User Operating System (User OS) to get an access to the content of the MIFARE[®] memory.

An access to the MIFARE[®] memory using the commands eePasswordRead and eePasswordWrite is only possible when knowing a password depending on the MIFARE[®] keys of the relevant sector. Therefore the knowledge of the same secret keys is necessary for accessing the EEPROM area from the User OS.

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

2 SECURE ACCESS PRINCIPLE

For secure access a special password called MF_password is needed that is checked every time the User OS wants to access the MIFARE® memory. The User OS has to call the function **eePasswordRead** or **eePasswordWrite**. The password and the data are passed as parameters to the functions.

The User OS can store the MF_password in the User OS EEPROM area or receive this password from the reader terminal when an access to the MIFARE® memory shall be performed. In case of loading the MF_password from the reader terminal the user operating system has to guarantee the secure loading of the MF_password.

The following security checks will be done by the eePasswordRead/Write functions:

- check the Access Condition Matrix (ACM) for a correct value (14h)
- check of the block address
- verify the MF_password
- perform read / write access to MIFARE® memory.

2.1 Security levels

Using the MF_password gives the possibility to reach the same security levels as realised with the MIFARE® keys.

One MF_password per sector is needed to access the MIFARE® memory on all cards when an application uses one pair of MIFARE® keys A and B per sector that is the same for all cards. When diversified MIFARE® keys are used a unique key will be generated and stored on the card. Thus the MF_password for each card is unique.

Table 1 Comparison MIFARE® Keys / MF_password

MIFARE® keys A / B	MF_password
One key pair per sector	One MF_password per sector depending on MIFARE® keys A and B; same MF_password for every card
Diversified keys; unique for each card and sector	Diversified MF_password depending on diversified MIFARE® keys A and B; unique MF_password for each card and sector

NOTE: The MF_password will always be calculated based on the MIFARE® keys A and B. Therefore in the MIFARE®sector trailer access conditions for key B MUST be configured as NOT READABLE by a MIFARE® application. This means using the MIFARE® memory in the expanded memory configuration, where key B memory space is used as data, is NOT allowed.

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

3 GENERAL REQUIREMENTS AND SPECIFICATIONS

The following conditions and restrictions are valid for the `eePasswordRead/Write` routines:

- the MIFARE[®] access conditions in the MIFARE[®] sector trailers will **NOT** be checked
- the same MF_password will allow read and write access.

3.1 Access condition matrix (ACM)

To indicate that a sector of the EEPROM memory is configured to grant a MF_password restricted access for the User OS, the value 14 h has to be defined in the ACM (part of ROM) of the Dual Interface Smart Card IC.

3.2 Read access

The function `eePasswordRead` has access to data blocks 0 to 2 in the MIFARE[®] sectors 0 to 31 respectively data blocks 0 to 14 in the MIFARE[®] sectors 32 to 39. A read access to the MIFARE[®] sector trailers is NOT allowed.

After all checks are passed the function will read one data block (16 bytes) that was specified when calling the function. The data read will be stored at the memory location that was defined as a parameter in the function call.

3.3 Write access

The function `eePasswordWrite` has access to blocks 0 to 3 of sector 0 to 31 respectively blocks 0 to 15 in sectors 32 to 39. Therefore it is possible to write data blocks and also MIFARE[®] sector trailers.

After passing the security checks the function will write one data block (16 bytes). The block address has to be specified when calling the function.

3.4 Block 0 access

A write access to block 0 of sector 0 is not allowed for the MF2ICD8x ICs because the sector 0 contains read only information (UID, SAK and ATQ).

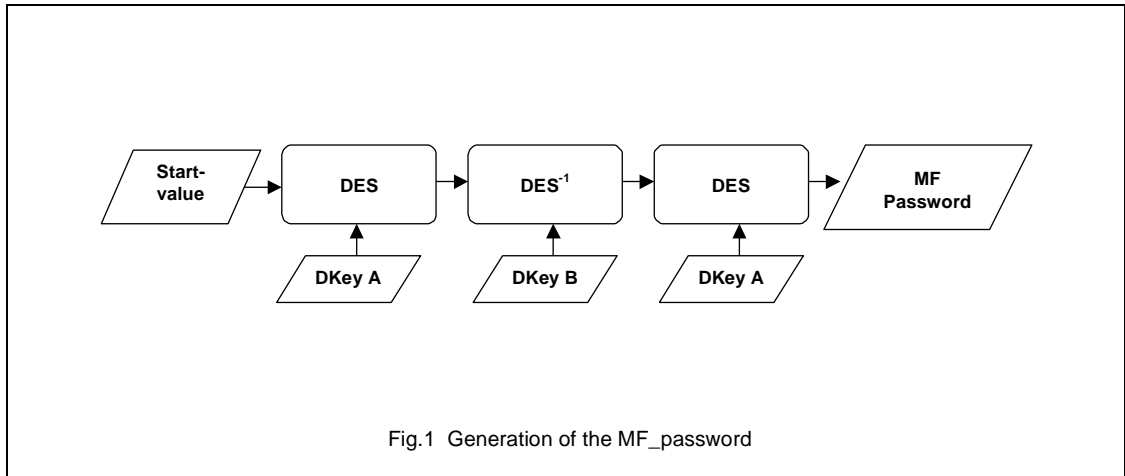
For P8RFxxxx ICs a write access to block 0 of sector 0 is possible, but the written data can not be read with a MIFARE[®] read command, because the (UID, SAK and ATQ) information is stored in the security row of the smart card IC.

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

4 GENERATION OF THE MF_PASSWORD

The MF_password will be generated using Triple-DES encryption based on the Data Encryption Standard (DES) algorithm.



4.1 Start Value

A fixed start value of 8 bytes will be used. All 8 bytes of the start value have a value of 00h.

4.2 Loading of DES Keys

The keys DkeyA and DkeyB used for encryption are derived from the MIFARE[®] keys A and B of the respective MIFARE[®] sector. To expand the key length of 48 bits of the MIFARE[®] keys to 64 bits used for Triple-DES encryption the following conventions will be used:

Representation of the MIFARE[®] Sector Trailer:

LSByte	MSByte	LSByte	MSByte
KEY A	Access Conditions	KEY B	

Representation of bits of the MIFARE[®] Key (each consists of 6 Bytes):

BYTE 5 MSBYTE			BYTE 4			BYTE 3			BYTE 2			BYTE 1			BYTE 0 LSBYTE		
K ₅₇	...	K ₅₀	K ₄₇	...	K ₄₀	K ₃₇	...	K ₃₀	K ₂₇	...	K ₂₀	K ₁₇	...	K ₁₀	K ₀₇	...	K ₀₀

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

The 6 bytes MIFARE® key will be mapped to the 64 bit Triple-DES keys DkeyB in the following way:

Table 2 Mapping of MIFARE® key to Triple DES key DkeyB

DES KEY BYTE	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
7	K ₅ 6	K ₅ 5	K ₅ 4	K ₅ 3	K ₅ 2	K ₅ 1	K ₅ 0	P
6	K ₄ 6	K ₄ 5	K ₄ 4	K ₄ 3	K ₄ 2	K ₄ 1	K ₄ 0	P
5	K ₃ 6	K ₃ 5	K ₃ 4	K ₃ 3	K ₃ 2	K ₃ 1	K ₃ 0	P
4	K ₂ 6	K ₂ 5	K ₂ 4	K ₂ 3	K ₂ 2	K ₂ 1	K ₂ 0	P
3	K ₁ 6	K ₁ 5	K ₁ 4	K ₁ 3	K ₁ 2	K ₁ 1	K ₁ 0	P
2	K ₀ 6	K ₀ 5	K ₀ 4	K ₀ 3	K ₀ 2	K ₀ 1	K ₀ 0	P
1	0	K ₅ 7	K ₄ 7	K ₃ 7	K ₂ 7	K ₁ 7	K ₀ 7	P
0	0	0	0	0	0	0	0	P

Note

1. P.....Parity Bit (Parity Bit is not checked by the MIFARE® PRO DES co-processor)

DkeyA will be generated the following way:

Table 3 Mapping of MIFARE® key to Triple-DES key DkeyA

DES KEY BYTE	BIT 7	BIT 6	BIT 5	BIT 4	BIT 3	BIT 2	BIT 1	BIT 0
7	0	0	0	0	0	0	0	P
6	0	K ₀ 7	K ₁ 7	K ₂ 7	K ₃ 7	K ₄ 7	K ₅ 7	P
5	K ₅ 6	K ₅ 5	K ₅ 4	K ₅ 3	K ₅ 2	K ₅ 1	K ₅ 0	P
4	K ₄ 6	K ₄ 5	K ₄ 4	K ₄ 3	K ₄ 2	K ₄ 1	K ₄ 0	P
3	K ₃ 6	K ₃ 5	K ₃ 4	K ₃ 3	K ₃ 2	K ₃ 1	K ₃ 0	P
2	K ₂ 6	K ₂ 5	K ₂ 4	K ₂ 3	K ₂ 2	K ₂ 1	K ₂ 0	P
1	K ₁ 6	K ₁ 5	K ₁ 4	K ₁ 3	K ₁ 2	K ₁ 1	K ₁ 0	P
0	K ₀ 6	K ₀ 5	K ₀ 4	K ₀ 3	K ₀ 2	K ₀ 1	K ₀ 0	P

Note

1. P.....Parity Bit (Parity Bits are not checked by the DES co-processor)

Table 4 Representation of bytes of the MIFARE® Password (consists of 8 Bytes in DES data register)

DDAT	LSB							MSB
MF_PASSWORD	BYTE 0	BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6	BYTE 7
RAM ADDRESS	Addr. + 0	Addr. + 1	Addr. + 2	Addr. + 3	Addr. + 4	Addr. + 5	Addr. + 6	Addr. + 7

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

4.3 EXAMPLES

Table 5 Mapping of MIFARE® key to Triple-DES key DkeyB

MIFARE® KEYS (LSB -> MSB)		TRIPLE-DES KEYS (LSB -> MSB)		MF_PASSWORD (LSB -> MSB)
KeyA	FF FF FF FF FF FF	DKeyA	FE FE FE FE FE FE 7E 00	0B 54 57 07 45 FE 3A E7
KeyB	FF FF FF FF FF FF	DKeyB	00 7E FE FE FE FE FE FE	
KeyA	A0 A1 A2 A3 A4 A5	DKeyA	40 42 44 46 48 4A 7E 00	8C 7F 46 D7 6C E0 12 66
KeyB	B0 B1 B2 B3 B4 B5	DKeyB	00 7E 60 62 64 66 68 6A	
KeyA	4D 3A 99 C3 51 DD	DKeyA	9A 74 32 86 A2 BA 1A 00	D8 09 C4 6A 74 84 A1 34
KeyB	1A 98 2C 7E 45 9A	DKeyB	00 44 34 30 58 FC 8A 34	

Notes:

1. Initial Value: 00 00 00 00 00 00 00 00
2. The DES parity bits are regarded as 0
3. **When implementing an algorithm to calculate the MF_password out of the MIFARE keys, take special care of the bit order in DES key A byte no. 6 !**

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

4.4 Generation Tools

Philips offers an assembler function which can be used to generate MF_passwords on the card.

A simple PC-tool is provided that allows to calculate the MF_password for a given MIFARE® key pair. The tool also shows the calculated Triple-DES keys DKeyA and DKeyB.



Fig.2 Generation tool

Secure Access to MIFARE Memory on Dual Interface Smart Card ICs

AN02105

5 REVISION HISTORY

Table 6 Secure Access to MIFARE Memory on Dual Interface Smart Card ICs Revision History

REVISION	DATE	CPCN	PAGE	DESCRIPTION
1.0	2002 Jan	-		Initial version.
1.1	2002 Apr	-	5	Add hint for sector 9 restrictions.
1.2	2002 Sep	-	8	Contents updated. - Section 4.3 "EXAMPLES": added in Table 4 new Mifare Keys: Key A: 4D 3A 99 C3 51 DDand Key B: 1A 98 2C 7E 45 9A ... and added new Table Note 3

Philips Semiconductors – a worldwide company

Contact information

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

© Koninklijke Philips Electronics N.V. 2002

SCA74

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

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

Let's make things better.

Philips
Semiconductors



PHILIPS