SHORT FORM SPECIFICATION

mifare DES*Fire*

Contactless Multi-Application IC with DES and 3DES Security

MF3 IC D40

Preliminary Short Form Specification

September 2003

Revision 2.0

PUBLIC

Philips Semiconductors

PHILIPS

Short Form Specification mifare DES*Fire* MF3 IC D40

CONTENTS

1 FEATURES

1.1 RF Interface: ISO 14443 Type A

- Contactless transmission of data and powered by the RF-field (no battery needed)
- Operating distance: Up to 100 mm (depending on antenna geometry)
- Operating frequency: 13.56 MHz
- Fast data transfer: 106 kbit/s, 212 kbit/s, 424 kbit/s
- High data integrity: 4 Byte MAC, 16 Bit CRC, parity, bit coding, bit counting
- True deterministic anticollision
- 7 byte unique identifier (cascade level two according to ISO 14443-3)
- Uses ISO 14443-4 transport protocol

1.2 Non - Volatile Memory

- 4 kbyte NV-Memory
- NV-Memory write time 2 ms (1 ms erase, 1 ms program)
- Data retention of 10 years
- Write endurance 100 000 cycles

1.3 NV-Memory Organisation

- Flexible file system
- Up to 28 applications simultaneously on one PICC
- Up to 16 files in each application

1.4 Security

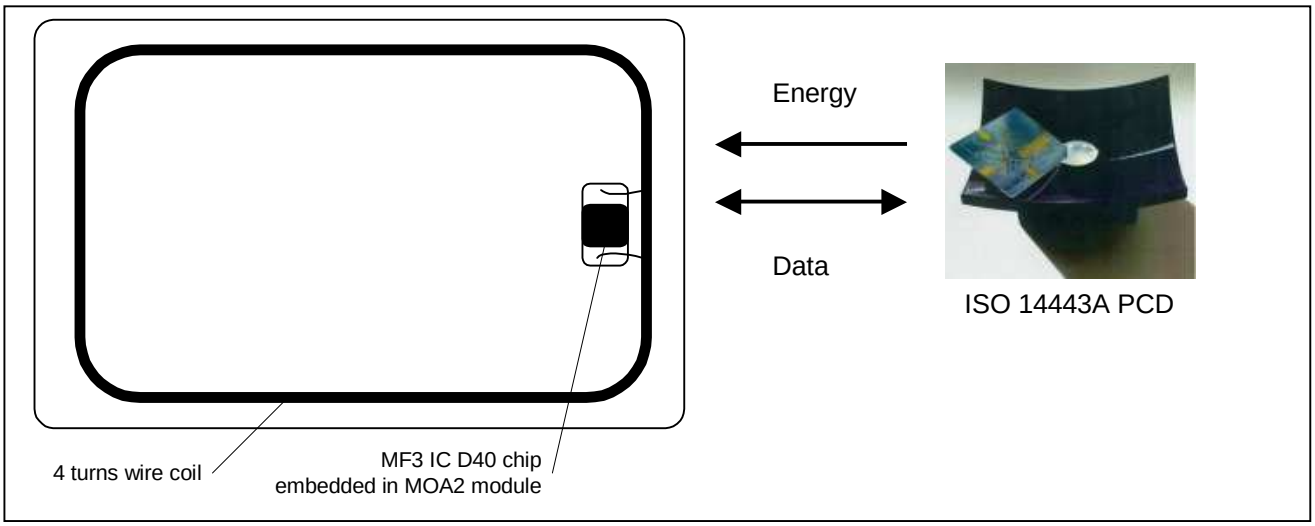
- Unique 7 Byte serial number for each device
- Mutual three pass authentication
- Hardware DES/3DES Data encryption on RF-channel with replay attack protection
- Data Authenticity by 4 Byte MAC
- Authentication on Application level

2 GENERAL DESCRIPTION

Philips has developed the MIFARE® DESFire (MF3 IC D40) to be used with Proximity Coupling Devices (PCDs) according to ISO14443 Type A. The transport protocol complies to part ISO 14443-4. The MF3 IC D40 is primarily designed for secure contactless transport applications and related loyalty programs.

2.1 Contactless Energy and Data Transfer

In the MIFARE® system, the MF3 IC D40 is connected to a coil consisting of a few turns embedded in a standard ISO smart card. No battery is needed. When the card is positioned in the proximity of the PCD antenna, the high speed RF communication interface allows to transmit data with up to 424 kbit/s.



2.2 Delivery Types

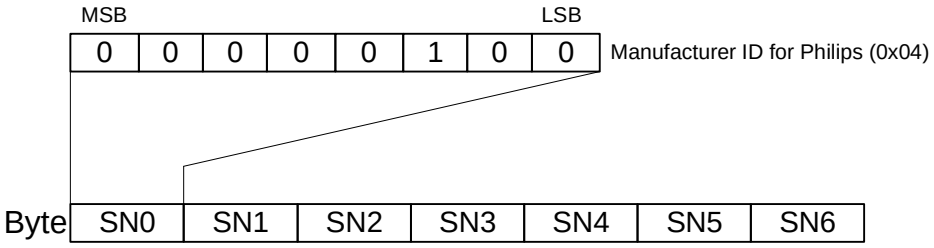
- Dies on 8” wafer, sawn on FFC, 150µm thickness
- Au-Bumped Dies on 8” wafer, sawn on FFC, 150µm thickness
- MOA2 Contactless Chip Card Module
- MOA4 Contactless Chip Card Module

2.3 Anticollision

An intelligent anticollision mechanism allows to handle more than one PICC in the field simultaneously. The anticollision algorithm selects each PICC individually and ensures that the execution of a transaction with a selected PICC is performed correctly without data corruption resulting from other PICCs in the field.

2.4 UID / Serial Number

The unique 7 byte serial number (UID) is programmed into a locked part of the NV-memory which is reserved for the manufacturer. Due to security and system requirements these bytes are write-protected after having been programmed by the IC manufacturer at production time.



7 Byte unique Serial Number

According to ISO14443-3 the first anticollision loop will return the cascade tag 0x88 and the first 3 bytes of the UID, SN0 to SN2 and BCC. The second anticollision loop will return bytes SN3 to SN6 and BCC.

SN0 holds the Manufacturer ID for Philips (04h) according to ISO14443-3 and ISO 7816-6 AM1.

2.5 Memory Organisation

The 4 kbyte NV-memory is organised using a flexible file system. This file system allows a maximum of 28 different applications on one single PICC. Each application provides up to 16 files. Every application is represented by it's 3 bytes **A**pplication **ID**entifier, **AID**.

Five different file types are supported, see chapter 2.6.

Each file can be created either at PICC initialisation (card production / card printing), at PICC personalisation (vending machine) or in the field.

If a file or application becomes obsolete in operation, it can be permanently invalidated.

Commands which have impact on the file structure itself (e.g. creation or deletion of applications, change of keys...) activate an automatic rollback mechanism, which protects the file structure from getting corrupted.

If this rollback is necessary, it is done without user interaction before carrying out further commands.

To ensure data integrity on application level, a transaction oriented backup is implemented for all file types with backup. It is possible to mix file types with and without backup within one application, whereby backup is possible only for files 0 .. 7, files 8 .. 15 do not feature backup mechanisms.

2.6 Available File Types

The files within an application can be of different types as:

- Standard Data Files
- Backup Data Files
- Value Files with Backup
- Linear Record Files with Backup
- Cyclic Record Files with Backup

2.7 Security

The 7 byte UID is unchangeably programmed into each device during production. It cannot be altered and ensures the uniqueness of each device.

The UID may be used to derive diversified keys for each ticket. Diversified PICC keys contribute to gain an effective anti-cloning mechanism.

Prior to data transmission a mutual three pass authentication can be done between PICC and PCD depending on the configuration employing either DES or 3DES.

Data Transmission between PICC and PCD can be done on three levels of security:

- Plain data transfer
- Plain data transfer with DES/3DES cryptographic checksum (MAC)
- DES/3DES encrypted data transfer (additional CRC integrity checksum before encryption)

Access to user data is granted on application level. For each application up to 14 different user definable keys can be assigned to control access to data stored in the PICC.

There are four different Access Rights stored for each file within each application:

- Read Access (GetValue, Debit for Value files)
- Write Access (GetValue, Debit, LimitedCredit for Value files)
- Read&Write Access (GetValue, Debit, LimitedCredit, Credit for Value files)
- ChangeAccessRights

Each access right represents a link to one of the keys stored within the respective application's key file.

If such a link is set to a number between 0 and 13 (max. 14 keys), this references a certain key within the application's key file, provided that the key exists (configuring a non-existing key is not allowed).

If the number is coded as 14 (0xE) this means “free” access. Thus the regarding access is granted always with and without a preceding authentication, directly after the selection of the respective application.

The number 15 (0xF) defines the opposite of “free” access and has the meaning “never” access. Therefore the respective linked Access Rights is always denied.

3 DESFIRE COMMAND SET

3.1 ISO 14443-3:

Command	Description
REQA	REQA and ATQA are implemented fully according to ISO14443-3.
WUPA	WAKE-UP is implemented fully according to ISO14443-3.
ANTICOLLISION / SELECT Cascade Level 1	The ANTICOLLISION and SELECT commands are implemented fully according to ISO14443-3.The response is part 1 of the UID.
ANTICOLLISION / SELECT Cascade Level 2	The ANTICOLLISION and SELECT commands are implemented fully according to ISO14443-3.The response is part 2 of the UID.

3.2 ISO 14443-4:

Command	Description
RATS	The response to the RATS command identifies the PICC type to the PCD.
PPS	The PPS command allows to individually select the communication baud rate between PCD and PICC. For DESFire it is possible to individually set the communication baud rate independently for both directions i.e. DESFire allows a non-symmetrical information interchange speed.
WTX	If the PICC needs more time than the defined FWT to respond to a PCD command it will send a request for a waiting time extension.

3.3 MF3 IC D40 Command Set – Security Related Commands:

Command	Description
Authenticate	In this procedure both, the PICC as well as the reader device, show in an encrypted way that they posses the same secret which especially means the same key. This procedure not only confirms that both entities are permitted to do operations on each other but also creates a session key which can be used to keep the further communication path secure. As the name “session key” implicitly indicates, each time a new authentication procedure is successfully completed a new key for further cryptographic operations is obtained.
Change KeySettings	Changes the master key settings on PICC and application level.
Get KeySettings	Gets information on the PICC and application master key settings. In addition it returns the maximum number of keys which can be stored within the selected application.
Change Key	Changes any key stored on the PICC.
Get KeyVersion	Reads out the current key version of any key stored on the PICC.

Note: All command & data frames are exchanged between PICC and PCD by using block format as defined in ISO 14443-4.

3.4 MF3 IC D40 Command Set – PICC Level Commands:

Command	Description
Create Application	Creates new applications on the PICC.
Delete Application	Permanently deactivates applications on the PICC.
Get Applications	Returns the Application IDentifiers of all active applications on a PICC.
Select Application	Selects one specific application for further access.
FormatPICC	Releases the PICC user memory.
Get Version	Returns manufacturing related data of the PICC.

Note: All command & data frames are exchanged between PICC and PCD by using block format as defined in ISO 14443-4.

3.5 MF3 IC D40 Command Set – Application Level Commands:

Command	Description
Get FileIDs	Returns the File IDentifiers of all active files within the currently selected application.
Get FileSettings	Get information on the properties of a specific file.
Change FileSettings	Changes the access parameters of an existing file.
Create StdDataFile	Creates files for the storage of plain unformatted user data within an existing application on the PICC.
Create BackupDataFile	Creates files for the storage of plain unformatted user data within an existing application on the PICC, additionally supporting the feature of an integrated backup mechanism.
Create ValueFile	Creates files for the storage and manipulation of 32bit signed integer values within an existing application on the PICC.
Create LinearRecordFile	Creates files for multiple storage of structural similar data, for example for loyalty programs, within an existing application on the PICC. Once the file is filled completely with data records, further writing to the file is not possible unless it is cleared.
Create CyclicRecordFile	Creates files for multiple storage of structural similar data, for example for logging transactions, within an existing application on the PICC. Once the file is filled completely with data records, the PICC automatically overwrites the oldest record with the latest written one. This wrap is fully transparent for the PCD.
DeleteFile	Permanently deactivates a file within the file directory of the currently selected application.

Note: All command & data frames are exchanged between PICC and PCD by using block format as defined in ISO 14443-4.

3.6 MF3 IC D40 Command Set – Data Manipulation Commands

Command	Description
Read Data	Reads data from Standard Data Files or Backup Data Files.
Write Data	Writes data to Standard Data Files or Backup Data Files.
Get Value	Reads the currently stored value from Value Files.
Credit	Increases a value stored in a Value File.
Debit	Decreases a value stored in a Value File.
Limited Credit	Allows a limited increase of a value stored in a Value File without having full Credit permissions to the file.
Write Record	Writes data to a record in a Cyclic or Linear Record File.
Read Records	Reads out a set of complete records from a Cyclic or Linear Record File.
Clear RecordFile	Resets a Cyclic or Linear Record File to empty state.
Commit Transaction	Validates all previous write access' on Backup Data Files, Value Files and Record Files within one application.
Abort Transaction	**In**validates all previous write access' on Backup Data Files, Value Files and Record Files within one application.

Note: All command & data frames are exchanged between PICC and PCD by using block format as defined in ISO 14443-4.

4 DEFINITIONS

Data sheet status	
Objective specification	This data sheet contains target or goal specifications for product development.
Preliminary specification	This data sheet contains preliminary data; supplementary data may be published later.
Product specification	This data sheet contains final product specifications.
Limiting values	
Limiting values given are in accordance with the Absolute Maximum Rating System (IEC 134). Stress above one or more of the limiting values may cause permanent damage to the device. These are stress ratings only and operation of the device at these or at any other conditions above those given in the Characteristics section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.	
Application information	
Where application information is given, it is advisory and does not form part of the specification.	

5 LIFE SUPPORT APPLICATIONS

These products are not designed for use in life support appliances, devices, or systems where malfunction of these products can reasonably be expected to result in personal injury. Philips customers using or selling these products for use in such applications do so on their own risk and agree to fully indemnify Philips for any damages resulting from such improper use or sale.

6 REVISION HISTORY

Table 1 Short Form Specification MF3 IC D40 Revision History

REVISION	DATE	CPCN	PAGE	DESCRIPTION
2.04	Sept 2003			Re-wording of command Descriptions
1.04	January 2003			General Update and Re-wording
1.01	July 2002			First official version.

Philips Semiconductors - a worldwide company

Contact Information

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

 SCA74

Let's make things better.

Philips Semiconductors

PHILIPS