MF3ICD41 Contactless multi-application IC

MIFARE DESFire short form specification

Rev. 02.00 — 25 October 2007
145420

Preliminary data sheet
CONFIDENTIAL

1. General description

NXP has developed the MIFARE DESFire (MF3ICD41) to be used with Proximity Coupling Devices (PCDs) according to ISO/IEC 14443 Type A. The transport protocol complies to part ISO/IEC 14443-4. The MF3ICD41 is primarily designed for secure contactless transport applications and related loyalty programs.

2. Features

2.1 RF Interface: ISO/IEC 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, 848 kbit/s
- High data integrity: 16/32 Bit CRC, parity, bit coding, bit counting; CMAC; MAC
- True deterministic anticollision
- 7 byte unique identifier (cascade level two according to ISO 14443-3)
- Uses ISO 14443-4 protocol

2.2 ISO/IEC 7816 compatibility (only software version 0.6 and higher)

- Supports 7816-3 APDU message Structure
- Supports 7816-4 INS code ‘A4’ SELECT
- Supports 7816-4 INS code ‘B0’ READ BINARY
- Supports 7816-4 INS code ‘D6’ UPDATE BINARY
- Supports 7816-4 INS code ‘B2’ for READ RECORDS
- Supports 7816-4 INS code ‘E2’ for APPEND RECORD
- Supports 7816-4 INS code ‘84’ for GET CHALLENGE
- Supports 7816-4 INS code ‘88’ for INTERNAL AUTHENTICATE
- Supports 7816-4 INS code ‘82’ for EXTERNAL AUTHENTICATE

2.3 Non - volatile memory

- 4 kbyte NV-Memory
- Data retention of 10 years
- Write endurance typical 500 000 cycles

2.4 NV-memory organisation

- Flexible file system
- Up to 28 applications simultaneously on one PICC
- Up to 32 files in each application

2.5 Security

- Unique 7 byte serial number for each device
- Mutual three pass authentication
- Mutual authentication according to ISO 7816-4
- Data encryption on RF-channel with replay attack protection:
- Hardware DES using 56/112/168 bit keys featuring key version, data authenticity by 8 byte CMAC
- Hardware AES using 128 bit keys featuring key version, data authenticity by 8 byte CMAC
- Authentication on application level
- Hardware exception sensors
- Self-securing file system
- Backward compatibility to MF3 IC D40: 4 byte MAC

3. Ordering information

See Delivery Type Addendum of Device

4. Block diagram

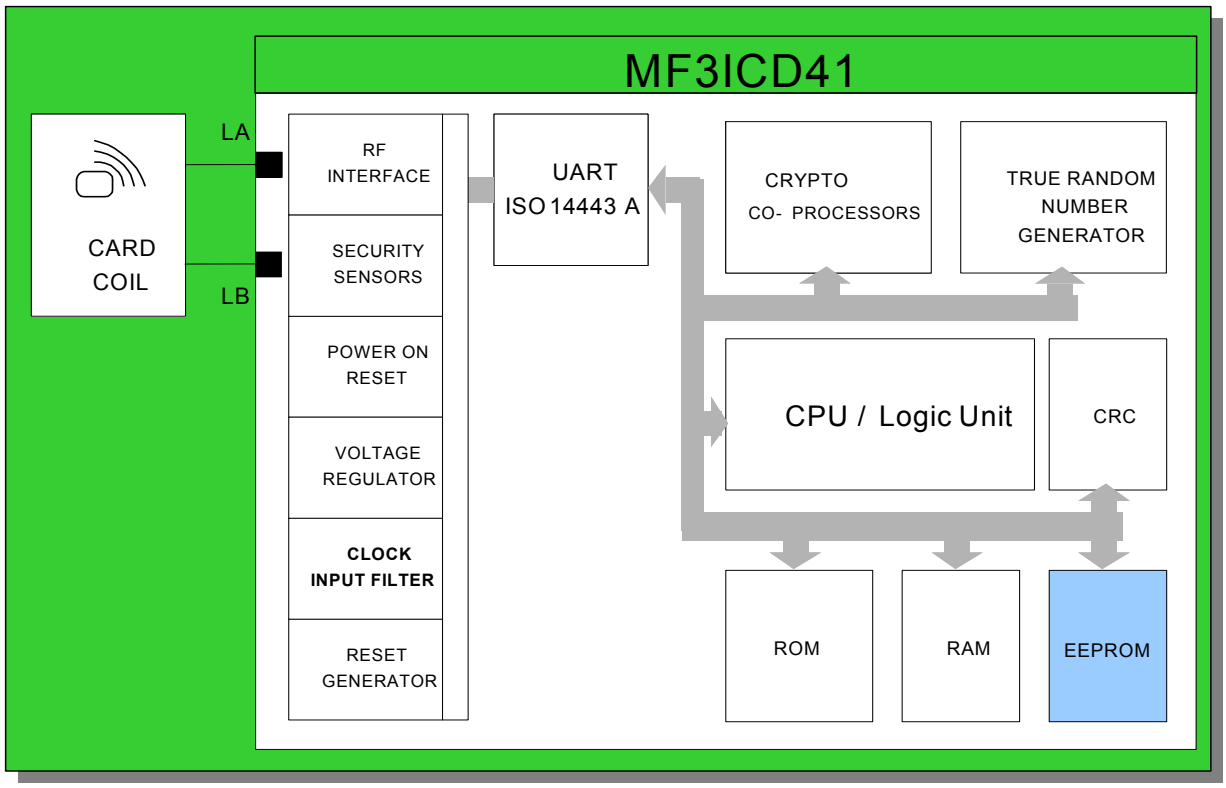

Fig 1. Block diagram

5. Pinning information

5.1 Pinning

See Delivery Type Addendum of Device

6. Functional description

6.1 Contactless energy and data transfer

In the MIFARE system, the MF3ICD41 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 848 kbit/s.

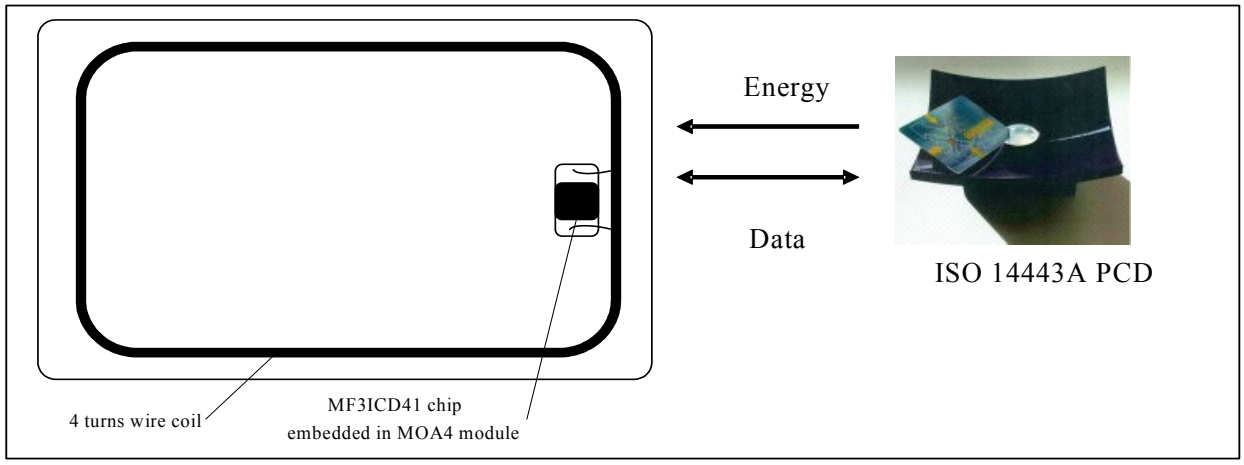

Fig 2. Contactless energy and data transfer

6.2 Delivery types

See Delivery Type Addendum of Device

6.3 Anticollision

An intelligent anticollision mechanism allows handling 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.

6.4 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 being programmed by the IC manufacturer at production time. According to ISO14443-3 during the first anticollision loop the cascade tag will be returned 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 NXP (04h) according to ISO14443-3 and ISO 7816-6 AMD 1.

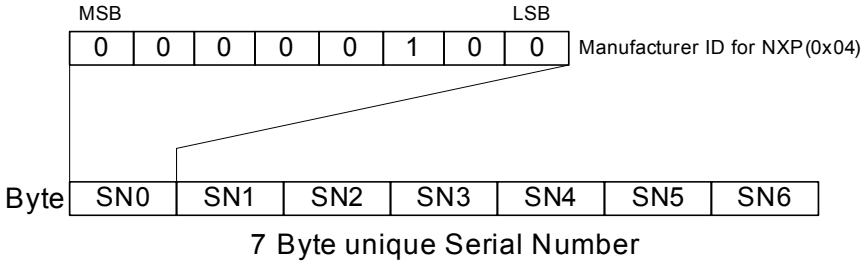

Fig 3. UID / Serial Number

6.5 Memory organisation

The 4 kbyte NV-memory is organized using a flexible file system. This file system allows a maximum of 28 different applications on one single PICC. Each application provides up to 32 files. Every application is represented by it's 3 bytes Application IDentifier, AID.

Five different file types are supported.

A guideline to assign DESFire AIDs can be found in the application note “MIFARE Application Directory, MAD”.

Each file can be created either at PICC initialisation (card production / card printing), at PICC personalization (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.

6.6 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

6.7 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.

Remark: For new authentications other than 0x0A, the init vector for the calculation of the MAC is only reset to '0x00' after the authentication. So the init vector shall be remembered during the whole transaction until a new authentication is calculated.

6.8 3 pass authentication

Prior to data transmission a mutual three pass authentication can be done between PICC and PCD depending on the configuration employing either 56 bit DES (single DES, DES), 112 bit DES (triple DES, 3DES), 168 bit DES (3 key triple DES, 3K3DES) or AES. During the authentication the security level of all further commands during the session is set.

Three pass authentication proves that both parties (PCD and PICC) are owner of a common secret (DES/3DES/3K3DES/AES key). The result of a successful authentication is a trusted link between both parties. The authentication command also yields a session key that you can use to protect the data transmission channel.

7. DESFire command set

7.1 ISO/IEC 14443-3:

Table 1. ISO/IEC 14443-3

Command	Description
REQA	REQA and ATQA are implemented fully according to ISO/IEC 14443-3.
WUPA	WAKE-UP is implemented fully according to ISO/IEC 14443-3.
ANTICOLLISION / SELECT Cascade Level 1	The ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3.The response is part 1 of the UID.
ANTICOLLISION / SELECT Cascade Level 2	The ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3.The response is part 2 of the UID.

7.2 ISO/IEC 14443-4:

Table 2. ISO/IEC 14443-4:

Command	Description
RATS	The response to the RATS command identifies the PICC type to the PCD.
PPS	The PPS command allows an individual selection of 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.

7.3 MF3ICD41 command set overview – security related commands:

Table 3. 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 possess 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 generated.
Change KeySettings	Changes the master key settings on PICC and application level.
Set Configuration	Configures the card and pre personalises the card with a key, defines if the UID or the random ID is sent back during communication setup and configures the ATS string.
Change Key	Changes any key stored on the PICC.
Get KeyVersion	Reads out the current key version of any key stored on the PICC.

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

7.4 MF3ICD41 command set overview – PICC level commands:

Table 4. PICC level commands

Command	Description
Create Application	Creates new applications on the PICC.
Delete Application	Permanently deactivates applications on the PICC.
Get Applications IDs	Returns the Application IDentifiers of all applications on a PICC.
Free Memory	Returns the free memory available on the card
GetDFNames	Returns the DF names
Get KeySettings	Gets information on the PICC and application master key settings. In addition it returns the maximum number of keys which are configured for the selected application.
Select Application	Selects one specific application for further access.
FormatPICC	Releases the PICC user memory.
Get Version	Returns manufacturing related data of the PICC.
GetCardUID	Returns the UID.

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

7.5 MF3ICD41 command set overview – application level commands:

Table 5. 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 32 bit 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.

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

7.6 MF3ICD41 command set overview – data manipulation commands:

Table 6. 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	Invalidates all previous write access' on Backup Data Files, Value Files and Record Files within one application.

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

7.7 MF3ICD41 command set- ISO 7816 APDU commands:

The MF3ICD41 provides the following command set according to ISO 7816-4 clause 6:

- INS code 'A4' Select
- INS code 'B0' Read Binary
- INS code 'D6' Update Binary
- INS code 'B2' Read Records
- INS code 'E2' Append Record
- INS code '84' Get Challenge
- INS code '88' Internal Authenticate
- INS code '82' External Authenticate

7.7.1 ISO 7816-4 APDU message structure:

DESFire supports the APDU message structure according to ISO 7816-4 for

- an optional wrapping of the native DESFire APDU format
- for the additionally implemented 7816-4 commands, as described later on.

8. Limiting values

See Delivery Type Addendum of Device

9. Recommended operating conditions

See Delivery Type Addendum of Device

10. Characteristics

See Delivery Type Addendum of Device

11. Support information

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

12. Package outline

See Delivery Type Addendum of Device

13. Revision history

Table 7. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
145420	25 October 2007	Prelimary data sheet		
	• Initial version			

14. Legal information

14.1 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.

14.2 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.

14.3 Disclaimers

General — 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.

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 medical, military, aircraft, space or life support equipment, nor in applications where failure or malfunction of a 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.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) may cause permanent damage to the device. Limiting values are stress ratings only and operation of the device at these or any other conditions above those given in the Characteristics sections of this document is not implied. Exposure to limiting values for extended periods may affect device reliability.

Terms and conditions of 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, including those pertaining to warranty, intellectual property rights infringement and limitation of liability, unless explicitly otherwise agreed to in writing by NXP Semiconductors. In case of any inconsistency or conflict between information in this document and such terms and conditions, the latter will prevail.

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.

14.4 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.

DESFire — is a trademark of NXP B.V.

15. Contact information

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

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

16. Tables

17. Figures

18. 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: 25 October 2007
Document identifier: 145420