MF3ICD81, MF3ICD41, MF3ICD21

MIFARE DESFire EV1 contactless multi-application IC

Rev. 3 — 17 February 2009 Product short data sheet

1. General description

MIFARE DESFire EV1 is ideal for service providers wanting to use multi-application smart cards in transport schemes, e-government or identity applications. It fully complies with the requirements for fast and highly secure data transmission, flexible memory organization and interoperability with existing infrastructure.

MIFARE DESFire EV1 is based on open global standards for both air interface and cryptographic methods. It is compliant to all 4 levels of ISO/IEC 14443A and uses optional ISO/IEC 7816-4 commands.

Featuring an on-chip backup management system and the mutual three pass authentication, a MIFARE DESFire EV1 card can hold up to 28 different applications and 32 files per application. The size of each file is defined at the moment of its creation, making MIFARE DESFire EV1 a truly flexible and convenient product.

Additionally, an automatic anti-tear mechanism is available for all file types, which guarantees transaction oriented data integrity. With MIFARE DESFire EV1, data transfer rates up to 848 Kbit/s can be achieved, making fast data processing possible.

The chip's main characteristics are denoted by its name DESFire EV1 - DES indicates the high level of security MIFARE DESFire EV1 achieves using a 3DES hardware cryptographic engine for enciphering transmission data. Fire reflects its outstanding position as a fast, innovative, reliable and secure IC in the contactless proximity transaction market. Hence, MIFARE DESFire EV1 brings many benefits to endusers. Cardholders can experience convenient contactless ticketing while also having the possibility to use the same device for related applications such as payment at vending machines, access control or event ticketing. In other words, the MIFARE DESFire EV1 silicon solution offers enhanced consumer-friendly system design, in combination with security and reliability.

MIFARE DESFire EV1 delivers the perfect balance of speed, performance and cost efficiency. Its open concept allows future seamless integration of other ticketing media such as smart paper tickets, key fobs, and mobile ticketing based on Near Field Communication (NFC) technology. It is also fully compatible with the existing MIFARE reader hardware platform. MIFARE DESFire EV1 is your ticket to contactless systems worldwide.

founded by Philips

2. Features

2.1 Key features

- Fully ISO/IEC 14443 type A 1 to 4 compliant
- 8 KB EEPROM with fast programming
  (also 2 KB and 4 KB versions are available)
- Secure, high speed command set
- Flexible file structure
- Anti-collision
- Unique 7-byte serial number (ISO cascade level 2)
- Data integrity: CRC and bit counting on physical layer
- Open DES/3DES crypto algorithm in hardware
- Open AES128 crypto algorithm in hardware
- Based on NXP advanced 0.14 μm NV-technology
- Fast data transfer: 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s
- Functional backward compatibility to MF3ICD40
- Composite CC EAL 4+ certification

3. Applications

- Advanced public transportation
- High secure access control
- Event ticketing
- eGovernment
- Identity

4. Quick reference data

Table 1. Quick reference data [1][2]

Symbol	Parameter	Conditions	Min	Typ	Max	Unit
f_i	input frequency		-	13.56	-	MHz
C_i	input capacitance	T_{amb} = 22 °C, f_i = 13.56 MHz; 2,8 V_{RMS} [3]	14.96	17.0	19.04	pF
EEPROM characteristics:						
t_{ret}	retention time	T_{amb} = 22 °C	10	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 22 °C	200000	500000	-	cycle
$t_{cy(W)}$	write cycle time	T_{amb} = 22 °C	-	2.9	-	ms

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

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

[3] Measured with LCR meter

5. Ordering information

Table 2. Ordering information

Type number	Package		
	Name	Description	Version
MF3ICD8101DUD/04	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) (see also Ref. 4), 8K EEPROM	-
MF3ICD4101DUD/04	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) (see also Ref. 4), 4K EEPROM	-
MF3ICD2101DUD/04	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format) (see also Ref. 4), 2K EEPROM	-
MF3MOD8101DA4/04	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape (see Ref. 5), 8K EEPROM	SOT500-2
MF3MOD4101DA4/04	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape (see Ref. 5), 4K EEPROM	SOT500-2
MF3MOD2101DA4/04	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape (see Ref. 5), 2K EEPROM	SOT500-2

[1] This package is also known as MOA4.

6. Block diagram

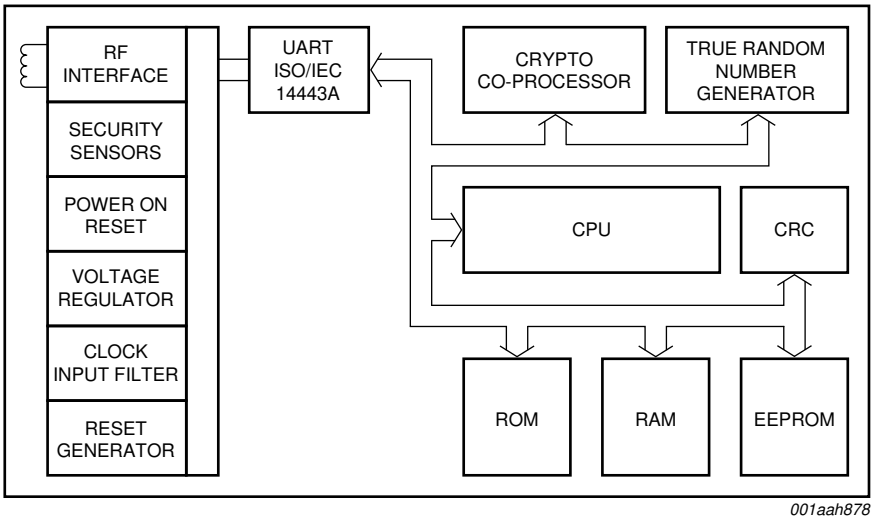

Fig 1. Block diagram of MF3ICD81, MF3ICD41, MF3ICD21

7. Limiting values

Table 3. Limiting values [1][2]

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

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

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

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

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

8. Functional description

8.1 Contactless energy and data transfer

In the MIFARE system, the MF3ICD81 is connected to a coil consisting of a few turns embedded in a standard ISO/IEC smart card (see Ref. 7). 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.

8.2 Anticollision

An intelligent anticollision mechanism allows handling more than one MF3ICD81 in the field simultaneously. The anticollision algorithm selects each MF3ICD81 individually and ensures that the execution of a transaction with a selected MF3ICD81 is performed correctly without data corruption resulting from other MF3ICD81s in the field.

8.3 UID/serial number

The unique 7 byte (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 ISO/IEC 14443-3 (see Ref. 11) during the first anticollision loop the cascade tag will be returned 88h and the first 3 bytes of the UID, UID0 to UID2 and BCC. The second anticollision loop will return bytes UID3 to UID6 and BCC.

SN0 holds the Manufacturer ID for NXP (04h) according to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD 1.

MF3ICD81 gives also the possibility to use Random ID. In this case MF3ICD81 only uses a single anti-collision loop. The 3 byte random number is generated after RF-reset of the MF3ICD81.

8.4 Memory organization

The 2/4/8 kB NV-memory is organized using a flexible file system. This file system allows a maximum of 28 different applications on one single MF3ICD81. 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, see Section 8.5.

A guideline to assign DESFire AIDs can be found in the application note “MIFARE Application Directory, MAD” (see Ref. 8).

Each file can be created either at MF3ICD81 initialization (card production/card printing), at MF3ICD81 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.

As the command are the same for all MF3ICD81, MF3ICD41, MF3ICD21, the details on the commands can be retrieved from Ref. 1. Only the memory size is different between the three products.

8.5 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

8.6 Security

The 7 byte UID is fixed 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 MF3ICD81 keys contribute to gain an effective anti-cloning mechanism and increase the security of the original key, see Ref. 6.

Prior to data transmission a mutual three pass authentication can be done between MF3ICD81 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 level of security of all further commands during the session is set. In addition the communication settings of the file/application result in the following option of secure communication between MF3ICD81 and PCD:

- Plain data transfer (only possible within the backwards compatible mode to MF3ICD40)
- Plain data transfer with cryptographic checksum (MAC):
  Authentication with Backwards compatible mode to MF3ICD40: 4 byte MAC
  All other Authentications based on DES/3DES/AES: 8 byte CMAC
- Encrypted data transfer (secured by CRC before encryption):
  Authentication with Backwards compatible mode to MF3ICD40: A 16 bit CRC is calculated over the stream and attached. The resulting stream is encrypted using the chosen cryptographic method.
  All other Authentications based DES/3DES/AES: A 32 bit CRC is calculated over the stream and attached. The resulting stream is encrypted using the chosen cryptographic method.

Find more information on the security concept of the product in Ref. 1. Be aware not all levels of security are recommended. The recommendation on the secure handling of the product can be seen in Ref. 2 as well as in Ref. 10.

9. DESFire command set

A detailed description of all commands can be found in Ref. 1.

9.1 ISO/IEC 14443-3

Table 4. 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.
HALT	The HALT command brings MF3ICD81 to the HALT-state.

9.2 ISO/IEC 14443-4

Table 5. ISO/IEC 14443-4

Command	Description
RATS	The response to the RATS command identifies the MF3ICD81 type to the PCD.
PPS	The PPS command allows an individual selection of the communication baud rate between PCD and MF3ICD81. 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 MF3ICD81 needs more time than the defined FWT to respond to a PCD command it will send a request for a waiting time extension.
DESELECT	Using DESELECT command MF3ICD81 can be brought to the HALT-state.

9.3 MF3ICD81 command set overview – security related commands

Table 6. Security related commands

Command	Description
Authenticate	In this procedure both, the MF3ICD81 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 MF3ICD81 and application level.
Set Configuration	Configures the card and pre personalizes 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 MF3ICD81.
Get Key Version	Reads out the current key version of any key stored on the MF3ICD81.

Remark: All command and data frames are exchanged between MF3ICD81 and PCD by using block format as defined in ISO/IEC 14443-4.

9.4 MF3ICD81 command set overview – MF3ICD81 level commands

Table 7. MF3ICD81 level commands

Command	Description
Create Application	Creates new applications on the MF3ICD81.
Delete Application	Permanently deactivates applications on the MF3ICD81.
Get Applications IDs	Returns the Application IDentifiers of all applications on a MF3ICD81.
Free Memory	Returns the free memory available on the card
GetDFNames	Returns the DF names
Get KeySettings	Gets information on the MF3ICD81 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.
FormatMF3ICD81	Releases the MF3ICD81 user memory.
Get Version	Returns manufacturing related data of the MF3ICD81.
GetCardUID	Returns the UID.

Remark: All command and data frames are exchanged between MF3ICD81 and PCD by using block format as defined in ISO/IEC 14443-4.

9.5 MF3ICD81 command set overview – application level commands

Table 8. 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 MF3ICD81.
Create BackupDataFile	Creates files for the storage of plain unformatted user data within an existing application on the MF3ICD81, 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 MF3ICD81.
Create LinearRecordFile	Creates files for multiple storage of structural similar data, for example for loyalty programs, within an existing application on the MF3ICD81. 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 MF3ICD81. Once the file is filled completely with data records, the MF3ICD81 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 and data frames are exchanged between MF3ICD81 and PCD by using block format as defined in ISO/IEC 14443-4.

9.6 MF3ICD81 command set overview – data manipulation commands

Table 9. 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 and data frames are exchanged between MF3ICD81 and PCD by using block format as defined in ISO/IEC 14443-4.

9.7 MF3ICD81 command set - ISO/IEC 7816 APDU commands

The MF3ICD81 provides the following commands according to ISO/IEC 7816-4:

- 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

9.7.1 ISO/IEC 7816-4 APDU message structure

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

- an optional wrapping of the native DESFire APDU format
- for the additionally implemented ISO/IEC 7816-4 commands

Find more information on the ISO/IEC 7816-4 commands in Ref. 1.

10. Abbreviations

Table 10. Abbreviations

Acronym	Description
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
ATS	Answer to Select
CMAC	Cryptic Message Authentication Code
CRC	Cyclic Redundancy Check
DES	Digital Encryption Standard
DF	Dedicated File
EEPROM	Electrically Erasable Programmable Read-Only Memory
FWT	Frame Waiting Time
INS	Instructions
MAC	Message Authentication Code
MAD	MIFARE Application Directory
NV	Non Volatile Memory
PCD	Proximity Coupling Device
MF3ICD81	Proximity Integrated Circuit Card
PPS	Protocol Parameter Selection
RATS	Request Answer To Select
REQA	Request Answer
RF	Radio Frequency
UID	Unique Identifier
WTX	Waiting Time Extension
WUPA	Wake Up Protocol A

11. References

[1] **Data sheet —** MF3ICD81 MIFARE DESFire Functional Specification, BL-ID Doc. No. 1340345

[2] **Data sheet —** MF3ICD81 Guidance, Delivery and Operation Manual, BL-ID Doc No. 146934

[3] **Data sheet —** Specification addendum MF3ICD81, BL-ID Doc. No. 167310

[4] **Data sheet —** MF3ICD8101 Sawn bumped 120µm wafer addendum, BL-ID Doc. No. 131831

[5] **Data sheet —** MF3MOD81 Contactless chip card module, BL-ID Doc. No. 143931

[6] **Application note —** MIFARE DESFire - Implementation hints and examples, BL-ID Doc. No. 094532

[7] **Application note —** MIFARE (Card) Coil Design Guide Product Specification, BL-ID Doc. No. 011732

[8] **Application note —** MIFARE Application Directory, BL-ID Doc. No. 001830

[9] **Application note —** MIFARE ISO/IEC 14443 MF3ICD81 Selection, BL-ID Doc. No. 130810

[10] **Application note —** End to end system security risk considerations for implementing contactless cards, BL-ID Doc. No. 155010

[11] **ISO/IEC Standard —** ISO/IEC 14443 Identification cards - Contactless integrated circuit cards - Proximity cards

12. Revision history

Table 11. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF3ICD81_MF3ICD41_ MF3ICD21_SDS_N_3	20090128	Product short data sheet	-	MF3ICD8101_SDS_N_1
Modifications:	• Specification status changed into “product” • Basic type number of MF3ICD81 changed • Type numbers MF3ICD41 and MF3ICD21 added • Section 1 “General description”, Section 2 “Features” and Section 3 “Applications”: updated • Section 11 “References”: added section			
MF3ICD8101_SDS_N_1	20071211	Objective short data sheet	-	-

13. Legal information

13.1 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.

13.2 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.

13.3 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 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.

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.

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.

13.4 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.

14. Contact information

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

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

15. Tables

16. Figures

17. 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: 17 February 2009
Document identifier: MF3ICD81_MF3ICD41_MF3ICD21_SDS_N_3