MF3ICDx21_41_81

MIFARE DESFire EV1 contactless multi-application IC

Rev. 3.1 — 21 December 2010
145631

Product short data sheet
PUBLIC

1. General description

MIFARE DESFire EV1 (MF3ICD(H) 21/41/81), a Common Criteria (EAL4+) certified product, is ideal for service providers wanting to use secure multi-application smart cards in public transport schemes, access managment or closed-loop e-payment applications. It is 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, allowing fast data transmission.

The main characteristics of this device are denoted by its name “DESFire”: DES indicates the high level of security using a 3DES or AES hardware cryptographic engine for enciphering transmission data and Fire indicates 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 end users. 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.

2. Features and benefits

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 power provided by the PCD and 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
- True deterministic anticollision
- 7 bytes unique identifier (cascade level 2 according to ISO/IEC 14443-3 and option for random ID)
- Uses ISO/IEC 14443-4 protocol

2.2 ISO/IEC 7816 compatibility

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

2.3 Non-volatile memory

- 2 kB or 4 kB or 8 kB NV-Memory
- Data retention of 10 years
- Write endurance typcial 500 000 cycles

2.4 NV-memory organization

- Flexible file system
- Up to 28 applications simultaneously on one PICC
- Up to 32 files in each application (standard data file, back-up data file, value file, linear record file and cyclic record file)
- File size is determined during creation

2.5 Security

- Common Criteria Certification: EAL4+ (Hardware and Software)
- Unique 7 bytes serial number for each device
- Optional “RANDOM” ID for enhance security and privacy
- Mutual three pass authentication
- Mutual authentication according to ISO/IEC 7816-4

- 1 card master key and up to 14 keys per application
- 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
- Data encryption on RF-channel
- Authentication on application level
- Hardware exception sensors
- Self-securing file system
- Backward compatibility to MF3ICD40: 4 byte MAC, CRC 16

2.6 Special features

- Transaction oriented automatic anti-tear mechanism
- Configurable ATS information for card personalisation
- Backward compatibility mode to MF3ICD40
- Optional high input capacitance (70pF) for small form factor design (MF3ICDH 21/41/81)

3. Applications

- Advanced public transportation schema
- Highly secure access management
- Closed-loop e-payment scheme
- Event ticketing
- eGovernment applications

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 for MF3ICD21/41/81	T_{amb} = 22 °C; f_i = 13.56 MHz; 2.8 V RMS	[3]	14.96	17.0	19.04	pF
	input capacitance for MF3ICDH21/41/81			64	69	74	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/05	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format); see Ref. 4, 8K EEPROM, 17pF input capacitance	-
MF3ICD4101DUD/05	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format); see Ref. 4, 4K EEPROM, 17pF input capacitance	-
MF3ICD2101DUD/05	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format); see Ref. 4, 2K EEPROM, 17pF input capacitance	-
MF3ICDH8101DUD/05	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format); see Ref. 5, 8K EEPROM, 70pF input capacitance	-
MF3ICDH4101DUD/05	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format); see Ref. 5, 4K EEPROM, 70pF input capacitance	-
MF3ICDH2101DUD/05	FFC	8 inch wafer (sawn; 120 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format); see Ref. 5, 2K EEPROM, 70pF input capacitance	-
MF3MOD8101DA4/05	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape; see Ref. 6, 8K EEPROM, 17pF input capacitance	SOT500-2
MF3MOD4101DA4/05	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape; see Ref. 6, 4K EEPROM, 17pF input capacitance	SOT500-2
MF3MOD2101DA4/05	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape; see Ref. 6, 2K EEPROM, 17pF input capacitance	SOT500-2

Table 2. Ordering information *…continued*

Type number	Package		
	Name	Description	Version
MF3MODH8101DA4/05	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape; see Ref. 6, 8K EEPROM, 70pF input capacitance	SOT500-2
MF3MODH4101DA4/05	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape; see Ref. 6, 4K EEPROM, 70pF input capacitance	SOT500-2
MF3MODH2101DA4/05	PLLMC[1]	plastic leadless module carrier package; 35 mm wide tape; see Ref. 6, 2K EEPROM, 70pF input capacitance	SOT500-2

[1] This package is also known as MOA4.

6. Block diagram

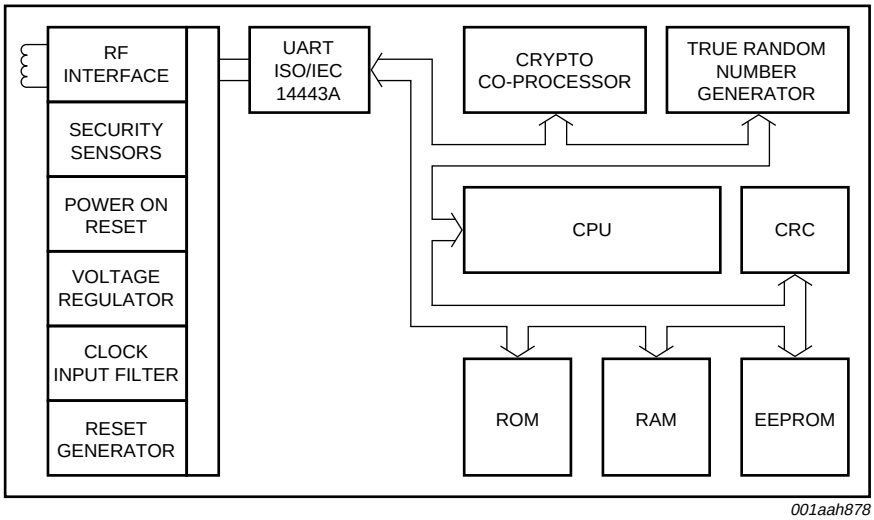

Fig 1. Block diagram of MF3ICD(H)81, MF3ICD(H)41, MF3ICD(H)21

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 MIFARE DESFire EV1 is connected to a coil consisting of a few turns embedded in a standard ISO/IEC smart card (see Ref. 8). A battery is not needed. When the card is positioned in the proximity of the PCD antenna, the high speed RF communication interface allows data to be transmitted up to 848 kbit/s.

8.2 Anti-collision

An intelligent anti-collision mechanism allows more than one MIFARE DESFire EV1 in the field to be handled simultaneously. The anti-collision algorithm selects each MIFARE DESFire EV1 individually and ensures that the execution of a transaction with a selected MIFARE DESFire EV1 is performed correctly without data corruption resulting from other MIFARE DESFire EV1s 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. 12) during the first anti-collision loop the cascade tag returns a value of 88h and also the first 3 bytes of the UID, UID0 to UID2 and BCC. The second anti-collision loop returns bytes UID3 to UID6 and BCC.

UID0 holds the manufacturer ID for NXP (04h) according to ISO/IEC 14443-3 and ISO/IEC 7816-6 AMD 1.

MIFARE DESFire EV1 also allows Random ID to be used. In this case MIFARE DESFire EV1 only uses a single anti-collision loop. The 3 byte random number is generated after RF reset of the MIFARE DESFire EV1.

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 MIFARE DESFire EV1. Each application provides up to 32 files. Every application is represented by its 3 bytes Application IDentifier (AID).

Five different file types are supported; see Section 8.5.

A guideline to assign MIFARE DESFire AIDs can be found in the application note *MIFARE Application Directory* (MAD); see Ref. 9.

Each file can be created either at MIFARE DESFire EV1 initialization (card production/card printing), at MIFARE DESFire EV1 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 being 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 commands are the same for MF3ICD(H)81, MF3ICD(H)41 and MF3ICD(H)21, the command details are available in Ref. 1. Only the memory size and input capacitance are different between the devices.

8.5 Available file types

The files within an application can be any of the following types:

- 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 MIFARE DESFire EV1 keys contribute to gain an effective anti-cloning mechanism and increase the security of the original key; see Ref. 7.

Prior to data transmission a mutual three pass authentication can be done between MIFARE DESFire EV1 and PCD depending on the configuration employing either 56-bit DES (single DES, DES), 112-bit 3DES (triple DES, 2K3DES), 168-bit 3DES (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 options of secure communication between MIFARE DESFire EV1 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 recommended secure handling of the product can be seen in Ref. 2 and in Ref. 11.

9. DESFire command set

A detailed description of all commands is provided 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	WUPA is implemented fully according to ISO/IEC 14443-3
ANTICOLLISION/SELECT Cascade Level 1	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	ANTICOLLISION and SELECT commands are implemented fully according to ISO/IEC 14443-3; the response is part 2 of the UID
HALT	brings MIFARE DESFire EV1 to the HALT state

9.2 ISO/IEC 14443-4

Table 5. ISO/IEC 14443-4

Command	Description
RATS	identifies the MIFARE DESFire EV1 type to the PCD
PPS	allows individual selection of the communication baud rate between PCD and MIFARE DESFire EV1; for DESFire it is possible to set different communication baud rates for each direction i.e. DESFire allows a non-symmetrical information interchange speed.
WTX	if the MIFARE DESFire EV1 needs more time than the defined FWT to respond to a PCD command it requests a Waiting Time eXtension (WTX)
DESELECT	allows MIFARE DESFire EV1 to be brought to the HALT state

9.3 MIFARE DESFire EV1 command set overview – security related commands

Table 6. Security related commands

Command	Description
Authenticate	MIFARE DESFire EV1 and the reader device show in an encrypted way that they possess the same secret which especially means the same key; this not only confirms that both entities are permitted to perform 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 MIFARE DESFire EV1 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 MIFARE DESFire EV1
Get Key Version	reads out the current key version of any key stored on the MIFARE DESFire EV1

Remark: All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

9.4 MIFARE DESFire EV1 command set overview – MIFARE DESFire EV1 level commands

Table 7. Level commands

Command	Description
Create Application	creates new applications on the MIFARE DESFire EV1
Delete Application	permanently deactivates applications on the MIFARE DESFire EV1
Get Applications IDs	returns the Application IDentifiers of all applications on a MIFARE DESFire EV1
Free Memory	returns the free memory available on the card
GetDFNames	returns the DF names
Get KeySettings	gets information on the MIFARE DESFire EV1 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 MIFARE DESFire EV1
GetCardUID	returns the UID

Remark: All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

9.5 MIFARE DESFire EV1 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	gets 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 MIFARE DESFire EV1
Create BackupDataFile	creates files for the storage of plain unformatted user data within an existing application on the MIFARE DESFire EV1, 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 MIFARE DESFire EV1
Create LinearRecordFile	creates files for multiple storage of similar structural data, for example, loyalty programs within an existing application on the MIFARE DESFire EV1; 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 similar structural data, for example, logging transactions within an existing application on the MIFARE DESFire EV1; once the file is filled completely with data records, the MIFARE DESFire EV1 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 MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

9.6 MIFARE DESFire EV1 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

Table 9. Data manipulation commands *…continued*

Command	Description
Clear RecordFile	resets a Cyclic or Linear Record file to empty state
Commit Transaction	validates all previous write accesses on Backup Data files, Value files and Record files within one application
Abort Transaction	invalidates all previous write accesses on Backup Data files, Value files and Record files within one application

Remark: All command and data frames are exchanged between MIFARE DESFire EV1 and PCD by using block format as defined in ISO/IEC 14443-4.

9.7 MIFARE DESFire EV1 command set - ISO/IEC 7816 APDU commands

The MIFARE DESFire EV1 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

MIFARE DESFire EV1 supports the APDU message structure according to ISO/IEC 7816-4 for:

- an optional wrapping of the native MIFARE DESFire EV1 APDU format
- 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
CC	Common Criteria
CMAC	Cryptic Message Authentication Code
CRC	Cyclic Redundancy Check
DES	Digital Encryption Standard
DF	Dedicated File
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read-Only Memory
FWT	Frame Waiting Time
ID	IDentifier
INS	Instructions
LCR	inductance, Capacitance, Resistance
MAC	Message Authentication Code
MAD	MIFARE Application Directory
NV	Non-Volatile Memory
PCD	Proximity Coupling Device
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 EV1***, document number: 13403**[1].

[2] **Data sheet — *MF3ICD81 Guidance, Delivery and Operation Manual***, document number: 1469**.

[3] **Data sheet — *Specification addendum MF3ICD81***, document number: 1673**.

[4] **Data sheet — *MF3ICD8101 Sawn bumped 120 μm wafer addendum***, document number: 1318**.

[5] **Data sheet — *MF3ICDH8101 Sawn bumped 120 μm wafer addendum***, document number: 1970**.

[6] **Data sheet — *MF3MODx21_41_81 Contactless chip card module***, document number: 1439**.

[7] **Application note — *MIFARE DESFire - Implementation hints and examples***, document number: 0945**.

[8] **Application note — *Card Coil Design Notes for MIFARE DESFire EV1***, document number: 1713**.

[9] **Application note — *MIFARE Application Directory***, document number: 0018**.

[10] **Application note — *MIFARE ISO/IEC 14443 PICC Selection***, document number: 1308**.

[11] **Application note —** *End to end system security risk considerations for implementing contactless cards*, document number: 1550**.

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

1. ** ... BU-ID document version number

12. Revision history

Table 11. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF3ICDX21_41_81_SDS v3.1	20101221	Product short data sheet		MF3ICD21_41_81_SDS_2
Modifications:	• Data sheet title updated • Section 1 “General description”, Section 2 “Features and benefits”, Section 3 “Applications”, Section 11 “References”, Section 13 “Legal information”: updated • Section 5 “Ordering information”: type number MF3ICD801DUD/04 changed to MF3ICD8101DUD/05			
MF3ICD21_41_81_SDS_2	20090306	Product short data sheet	-	MF3ICD8101_SDS_N_1
Modifications:	• Section 5 “Ordering information”: type number MF3ICD8101DUD/01 changed to MF3ICD8101DUD/04 • Section 5 “Ordering information”: added root type numbers MF3ICD41 and MF3ICD21 • Section 1 “General description”, Section 2 “Features and benefits” and Section 3 “Applications”: updated • Section 11 “References”: added			
MF3ICD8101_SDS_N_1	20071213	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.

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.

13.3 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.

13.4 Licenses

ICs with DPA Countermeasures functionality	
LICENSED DPA™ COUNTERMEASURES	NXP ICs containing functionality implementing countermeasures to Differential Power Analysis and Simple Power Analysis are produced and sold under applicable license from Cryptography Research, Inc.

13.5 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: 21 December 2010
145631