Kartový štandard

Minimálne technické požiadavky

1. Účel dokumentu

Dokument opisuje Minimálne technické požiadavky, ktoré musia spĺňať Akceptačné zariadenia tarifno-informačného systému Dopravcu pre akceptáciu elektronických cestovných lístkov na Dopravných kartách.

2. Skratky

APDU – Application Protocol Data Unit (komunikačný protokol)

BČK – Bezkontaktná Čipová Karta

EP – Elektronická Peňaženka

PCL – Predplatný Cestovný Lístok

SAM – Secure Access Module (bezpečnostný hardvérový modul)

SNR – Serial Number (výrobné číslo karty)

3. Pojmy

Akceptačné zariadenie – zariadenie, ktoré umožňuje čítanie a zápis dát na BČK. Bezpečnostné požiadavky zariadenie zabezpečuje prostredníctvom SAM modulu.

SAM modul – bezpečnostný modul (secure cryptoprocessor), ktorý slúži ako bezpečné úložisko šifrovacích kľúčov.

4. Požiadavky na hardvér

Akceptačné zariadenie musí spĺňať nasledovné hardvérové požiadavky:

4.1. Súčasťou zariadenia musí byť dostatočne výkonný procesor, ktorý umožní v akceptačnom zariadení použiť štandardný operačný systém vhodný pre Akceptačné zariadenia v aktuálnej verzii.

4.2. Súčasťou zariadenia musí byť dostatočne veľká pamäť pre uloženie zoznamu zablokovaných kariet (black list) a zoznamu produktov predaných cez internet (green list).

4.3. Súčasťou zariadenia musí byť čítačka bezkontaktných kariet, ktorá spĺňa požiadavky normy ISO/IEC 14443 so SAM slotom, ktorý spĺňa požiadavky normy ISO/IEC 7816:

a) akceptačné zariadenie umiestnené vo vozidle, v predpredaji alebo v automate – min 2 sloty pre SAM modul, form factor 2FF (Mini-SIM),

b) prenosné Akceptačné zariadenie (revízorská čítačka) – min 1 slot pre SAM modul, form factor 2FF (Mini-SIM) alebo 1 slot pre SAM modul vo forme secure microSD karty.

4.4. Súčasťou zariadenia musí byť 3G/4G modem pre prenos dát z/do Akceptačného zariadenia.

5. Požiadavky na systémový softvér

Akceptačné zariadenie musí spĺňať nasledovné požiadavky na systémový softvér:

5.1. Štandardný operačný systém (Linux, Android, Windows Embedded) vhodný do Akceptačných zariadení.

5.2. Ovládač pre čítačku BČK podľa normy ISO/IEC 14443.

5.3. Ovládač pre SAM modul podľa normy ISO/IEC 7816.

5.4. Ovládač pre 3G/4G modem.

6. Požiadavky na aplikačný softvér

Akceptačné zariadenie musí spĺňať nasledovné požiadavky na aplikačný softvér:

6.1. Všeobecné požiadavky

6.1.1. Možnosť vzdialenej aktualizácie aplikácie pre Akceptačné zariadenie.

6.1.2. Možnosť vzdialenej autorizácie SAM modulu.

6.1.3. Možnosť vzdialenej aktualizácie aplikácie a dát v SAM module.

6.1.4. Ak zariadenie obsahuje kombinovanú čítačku dopravných kariet a bankových kariet, možnosť definovať, ktorá čítačka má prednosť pri použití karty s dopravnou aj bankovou funkcionalitou.

6.2. Požiadavky na knižnicu pre prácu s BČK

6.2.1. Karta Mifare Classic – natívne príkazy karty Mifare Classic podľa špecifikácie výrobcu média.

6.2.2. Karta Mifare DESFire – natívne príkazy karty Mifare DESFire vrátane jej emulácie, zapuzdrené do formátu APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu média.

6.3. Požiadavky na knižnicu pre prácu so SAM modulom

6.3.1. Karta JavaCard (SAM modul) – natívne príkazy vo formáte APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu karty.

6.3.2. Secure microSD karta (SAM modul) – natívne príkazy vo formáte APDU správ podľa normy ISO/IEC 7816-4 a špecifikácie výrobcu karty.

6.4. Požiadavky na knižnicu pre 3G/4G komunikáciu s Akceptačným zariadením

6.4.1. Nahrávanie vstupných dát z Centrálneho systému do Akceptačného zariadenia – konfiguračný súbor, blokované karty, produkty predané cez internet (kartové udalosti).

6.4.2. Nahrávanie výstupných dát z Akceptačného zariadenia do Centrálneho systému – informácie o vykonaných kartových transakciách a kartových udalostiach, informácie o stave Akceptačného zariadenia.

6.4.3. Nahrávanie aktualizácií aplikačného softvéru – aktualizácia aplikácie pre Akceptačné zariadenie, aktualizácie SAM modulu.

6.4.4. Vzdialená autorizácia SAM modulu.

6.5. Požiadavky na knižnicu pre spracovanie vstupných dát

6.5.1. Práca so zoznamom zablokovaných kariet.

6.5.2. Práca so zoznamom produktov predaných cez internet (kartové udalosti).

6.6. Požiadavky na knižnicu pre generovanie výstupných dát

- Predajca,
- Číslo strojčeka,
- Číslo odpočtu,
- Číslo transakcie,
- Kód tarify,
- Zoznam a počet všetkých zón,
- Cena cestovného s DPH a bez DPH,
- Dátum a čas predaja,
- Spôsob predaja,
- Dátum začiatku platnosti,
- Dátum konca platnosti,
- Číslo nástupnej zastávky a číslo nástupnej zóny,
- Číslo výstupnej zastávky a číslo výstupnej zóny,
- Poradie PCL,
- Linka,
- Spoj,
- Tarifné kilometre,
- Časová platnosť,
- Typ platby,
- SNR karty,
- Emitent karty,
- Storno,
- Hodnota vkladu na EP,
- Počiatočný a konečný zostatok na BČK,
- Číslo operácie s EP,
- Emitent EP.

7. Požiadavky na BČK

7.1. Požiadavky na BČK

7.1.1. V súlade so špecifikáciou:
https://www.nxp.com/docs/en/data-sheet/MF3DHx3_SDS.pdf
(ktorá je zároveň prílohou tohto dokumentu).

7.1.2. Minimálna veľkosť pamäte 4 kB.

7.2. Výkonnostné požiadavky

Akceptačné zariadenie musí spĺňať nasledovné výkonnostné požiadavky na hardvér, systémový softvér a aplikačný softvér:

7.2.1. Celkový čas Testovacej transakcie s Mifare DESFire kartou musí byť menší ako 600 ms (mimo času, ktorý spotrebuje SAM modul).

8. Testovacia transakcia

Pre overenie funkčnosti HW čítačky a SW komponent akceptačného zariadenia je možné použiť nasledovnú testovaciu transakciu:

I. Vytvorenie spojenia v súlade s ISO/IEC 14443-4.

II. Výber aplikácie (Select).

III. Autentifikácia (Authenticate, prístupový kľúč v SAM module).

IV. Čítanie súboru (Read Backup Data File, 96 B, 3DES MAC).

V. Čítanie súboru (Read Value File, 3DES MAC).

VI. Zápis súboru (Write Backup Data File, 96 B, 3DES MAC).

VII. Zápis súboru (Write Value File, 3DES MAC).

VIII. Potvrdenie transakcie (Commit).

IX. Ukončenie spojenia v súlade s ISO/IEC 14443-4.

MF3D(H)x3

MIFARE DESFire EV3 contactless multi-application IC

Rev. 3.0 — 15 May 2020 Product short data sheet
612530 COMPANY PUBLIC

1 General description

1.1 Introduction

MF3D(H)x3 is the latest addition to the MIFARE DESFire product family introducing new feature along with enhanced performance for best user experience. The MF3D(H)x3 is Common Criteria EAL5+ security certified which is the same security certification level as demanded for smart card IC products used e.g. for banking cards or electronic passports. It fully complies with the requirements for fast and highly secure data transmission and flexible application management. This makes it the ideal product for service providers and service operators who want to offer an easy, convenient and secure access to a wide variety of different services.

MF3D(H)x3 offers best flexibility when creating multi-application schemes and feature such as MIsmartApp is supporting new business models. Using MF3D(H)x3 with NXP's AppXpplorer cloud service, Smart Cities services for example could be utilized with only one card by combining services such as public transport, car or bike sharing, access to city attractions with citizen services, closed-loop e-payment applications and local loyalty programs.

MF3D(H)x3 is based on global open standards for both air interface and cryptographic methods. It is compliant to all levels of ISO/IEC 14443A and supports optional ISO/IEC 7816-4 commands (APDU and file structure supported) and is fully interoperable with existing NFC reader for MIFARE infrastructure.

Featuring an on-chip backup management system and the mutual three-pass authentication, a MF3D(H)x3 card can hold as many applications as the memory can accommodate. Each application can hold up to 32 files with various data configurations. The size of each file is defined at the moment of its creation, making MF3D(H)x3 a truly flexible and convenient product. An automatic anti-tear mechanism is available for all file types, guaranteeing transaction-oriented data integrity.

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 confidentiality and integrity protection of the transmission data. Fire indicates its outstanding position as a Fast, Innovative, Reliable and sEcure IC in the contactless proximity transaction market.

MF3D(H)x3 delivers the perfect balance of speed, performance and cost efficiency. Its open concept allows seamless future integration of other ticketing media such as smart paper tickets, banking convergence card, and MIFARE 2GO mobile ticketing service based on Near Field Communication (NFC) technology. MF3D(H)x3 is your ticket to secure contactless systems worldwide.

1.2 Evolution of MIFARE DESFire products family

MIFARE DESFire has evolved over time, enhancing its security properties to protect against current and future security threats, and adding new features to better suit into new user requirements.

MIFARE DESFire EV3 is the fourth generation of the MIFARE DESFire products family succeeding MIFARE DESFire EV2. It is functionally backward compatible with all previous MIFARE DESFire generations, namely MIFARE DESFire EV2, MIFARE DESFire EV1 and MIFARE DESFire D40 (MF3ICD40).

Figure 1 shows the relationship between the latest three generations of MIFARE DESFire products. The latest generation encompasses the features from the older generation(s). Therefore, allowing existing users of the older products to adopt the latest product with minimum or no changes to their infrastructures.

MIFARE DESFire EV3 can be used as a MIFARE DESFire EV2 or a MIFARE DESFire EV1 in its default delivery configuration. Every new feature would require an activation and/or the use of new commands which is described in their respective sections in this document.

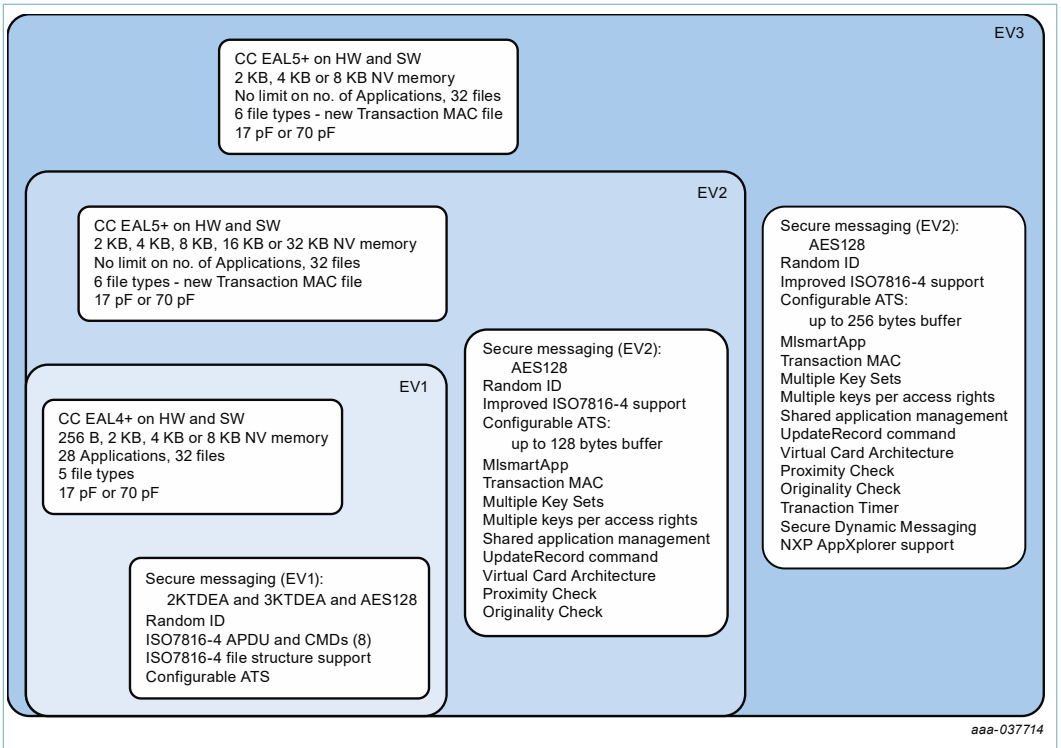


Figure 1. Evolution of MIFARE DESFire

2 Features and benefits

2.1 Feature overview

2.1.1 RF interface: ISO/IEC 14443 Type A

- Contactless interface compliant with ISO/IEC 14443-2/3 A
- Low Hmin enabling operating distance up to 100 mm (depending on power provided by the PCD and antenna geometry)
- Fast data transfer: 106 kbit/s, 212 kbit/s, 424 kbit/s, 848 kbit/s
- 7 bytes unique identifier (option for Random ID)
- Uses ISO/IEC 14443-4 transmission protocol
- Configurable FSCI to support up to 256 bytes frame size

2.1.2 Non-volatile memory

- 2 kB, 4 kB or 8 kB
- Data retention of 25 years
- Write endurance typical 1 000 000 cycles
- Fast programming cycles

2.1.3 NV-memory organization and multi-application support

- Flexible file system: user can freely define application structures on PICC
- As many applications as the memory size supports per PICC
- Up to 32 files in each application (6 file types available: Standard Data file, Back-up Data file, Value file, Linear Record file, Cyclic Record file and Transaction MAC file)
- File size is determined during creation (not for Transaction MAC file)
- *MIsmartApp* (Delegated Application Management)
- Memory reuse in DAM applications (Format Application)
- Factory loaded NXP's DAM keys for AppXplorer service support
- Accessing files from any two applications during a single transaction

2.1.4 Security and Privacy

- Common Criteria certification: EAL5+ (Hardware and Software)
- Unique 7 bytes serial number for each device
- Optional “RANDOM” ID for enhanced security and privacy
- Mutual three-pass authentication
- Mutual authentication according to ISO/IEC 7816-4
- Flexible key management: 1 card master key and up to 14 keys per application
- Multiple key assignment for each file access rights (up to 8)
- Multiple Key Sets per application with fast key rolling mechanism (up to 16 sets)
- Hardware DES using 56/112/168 bit keys featuring key version
- Hardware AES using 128-bit keys featuring key version
- Data authenticity by 8 byte CMAC
- MF3ICD40 compatible mode: 4 byte MAC, CRC 16

- Data encryption on RF-channel
- Authentication on application level
- Hardware exception sensors
- Self-securing file system
- Transaction MAC signed with secret key per application
- Virtual Card Architecture for enhanced card/application selection on multi-VC devices with privacy protection
- Proximity Check for protection against Relay Attacks
- Originality Check for proof of genuine NXP's product

2.1.5 ISO/IEC 7816 compatibility

- Supports ISO/IEC 7816-4 file structure (selection by File ID or DF name)
- Supports ISO/IEC 7816-4 APDU message structure
- Supports ISO/IEC 7816-4 APDU wrapper for MIFARE DESFire native commands
- 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

2.1.6 Special features

- Transaction-oriented automatic anti-tear mechanism with new transaction timer support
- Configurable ATS information for card personalization
- Backward compatibility mode to MIFARE DESFire EV2, EV1 and D40 (MF3ICD40)
- Secure Unique NFC (SUN) enabled by Secure Dynamic Messaging (SDM) which is mirrored as text into the NDEF message (compatible with NTAG DNA)
- NFC Forum Type 4 Tag certified (Certificate ID. 58652)
- Optional high input capacitance (70 pF) for small form factor designs (MF3DHx3)

2.2 Summary of key differences between MIFARE DESFire generations

Table 1 shows the key differences between the latest three product generations of the MIFARE DESFire family. For more detail on the new features, please refer to their respective sections in this document.

Table 1. Key differences between MIFARE DESFire generations

Features	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3
Cryptography scheme(s)	*Single DES, 2KTDEA, 3KTDEA, AES128*	*Single DES, 2KTDEA, 3KTDEA, AES128*	*Single DES, 2KTDEA, 3KTDEA, AES128*
Secure messaging(s)	*D40 Native, EV1*	*D40 Native, EV1, EV2 (see product data sheet)*	*D40 Native, EV1, EV2 (see* product data sheet
No. of applications	*28*	*No limit*	*No limit*
No. of files per application	*32*	*32*	*32*
Max. no. of files with backup	*32*	*32*	*32*
ISO/IEC7816-4 commands	*8*	*8 (refined)*	*8 (refined)*
Random ID	*Yes*	*Yes*	*Yes*
Configurable ATS	*Yes, Historical bytes only*	*Yes, all parameters*	*Yes, all parameters*
Max. communication buffer	*64 bytes*	*up to 128 bytes*	*Up to 256 bytes*
Chaining during data transfer	*Native (AFh)*	*Native (AFh) or ISO/ IEC14443-4*	*Native (AFh) or ISO/ IEC14443-4*
Multiple Key Sets with rolling	*No*	Yes	Yes
MIsmartApp (Delegated Application Management)	*No*	Yes	Yes
NXP AppXplorer supports	*No*	*Yes, self configuration*	Yes, preloaded DAM keys
Shared Application Management	*No*	Yes	Yes
Multiple keys per access right	*No*	Yes	Yes
UpdateRecord command	*No*	Yes	Yes
Transaction MAC	*No*	Yes	Yes
Transaction Timer	*No*	*No*	Yes
Secure Dynamic Messaging	*No*	*No*	Yes
Virtual Card Architecture	*No*	Yes	Yes
Proximity Check	*No*	Yes	Yes
Originality Check	*No*	Yes	Yes

3 Applications

- Secure public transport ticketing
- Multi-application smart city and mobility card
- Secure access management
- Micro-payment and Loyalty
- Student ID
- Road tolling and parking
- Hospitality
- Event ticketing

4 Quick reference data

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

Symbol	Parameter	Conditions		Min	Typ	Max	Unit
f_i	input frequency			-	13.56	-	MHz
C_i	input capacitance	MF3Dx3	[3][4]	-	17.0	-	pF
		MF3DHx3	[3][4]	-	66.5	-	pF
NV memory characteristics							
t_{ret}	retention time	T_{amb} = 25 °C		25	-	-	year
$N_{endu(W)}$	write endurance	T_{amb} = 25 °C		200 000	1 000 000	-	cycle

[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.
[4] T_{amb} = 25 °C; f_i = 13.56 MHz; 2.1 V RMS

5 Ordering information

Table 3. Ordering information

Type number	Package	Description	Version
MF3D2301DUD/00	FFC	12 inch wafer (sawn; 120 µm thickness)[1][2]; 2 KB, 17 pF input capacitance	-
MF3D4301DUD/00	FFC	12 inch wafer (sawn; 120 µm thickness)[1][2]; 4 KB, 17 pF input capacitance	-
MF3D8301DUD/00	FFC	12 inch wafer (sawn; 120 µm thickness)[1][2]; 8 KB, 17 pF input capacitance	-
MF3DH2301DUD/00	FFC	12 inch wafer (sawn; 120 µm thickness)[1][2]; 2 KB, 70 pF input capacitance	-
MF3DH4301DUD/00	FFC	12 inch wafer (sawn; 120 µm thickness)[1][2]; 4 KB, 70 pF input capacitance	-
MF3DH8301DUD/00	FFC	12 inch wafer (sawn; 120 µm thickness)[1][2]; 8 KB, 70 pF input capacitance	-
MF3D2300DA4/00	MOA4	plastic leadless module carrier package[3]; 2 KB, 17 pF input capacitance	SOT500-2
MF3D4300DA4/00	MOA4	plastic leadless module carrier package[3]; 4 KB, 17 pF input capacitance	SOT500-2
MF3D8300DA4/00	MOA4	plastic leadless module carrier package[3]; 8 KB, 17 pF input capacitance	SOT500-2
MF3DH2300DA4/00	MOA4	plastic leadless module carrier package[3]; 2 KB, 70 pF input capacitance	SOT500-2
MF3DH4300DA4/00	MOA4	plastic leadless module carrier package[3]; 4 KB, 70 pF input capacitance	SOT500-2
MF3DH8300DA4/00	MOA4	plastic leadless module carrier package[3]; 8 KB, 70 pF input capacitance	SOT500-2
MF3D2300DA8/00	MOA8	plastic leadless module carrier package[4]; 2 KB, 17 pF input capacitance	SOT500-4
MF3D4300DA8/00	MOA8	plastic leadless module carrier package[4]; 4 KB, 17 pF input capacitance	SOT500-4
MF3D8300DA8/00	MOA8	plastic leadless module carrier package[4]; 8 KB, 17 pF input capacitance	SOT500-4
MF3DH2300DA8/00	MOA8	plastic leadless module carrier package[4]; 2 KB, 70 pF input capacitance	SOT500-4
MF3DH4300DA8/00	MOA8	plastic leadless module carrier package[4]; 4 KB, 70 pF input capacitance	SOT500-4
MF3DH8300DA8/00	MOA8	plastic leadless module carrier package[4]; 8 KB, 70 pF input capacitance	SOT500-4

[1] Delivered on film frame carrier with electronic fail die marking according to SECSII format.
[2] See [2]
[3] See Figure 4
[4] See Figure 5

6 Block diagram

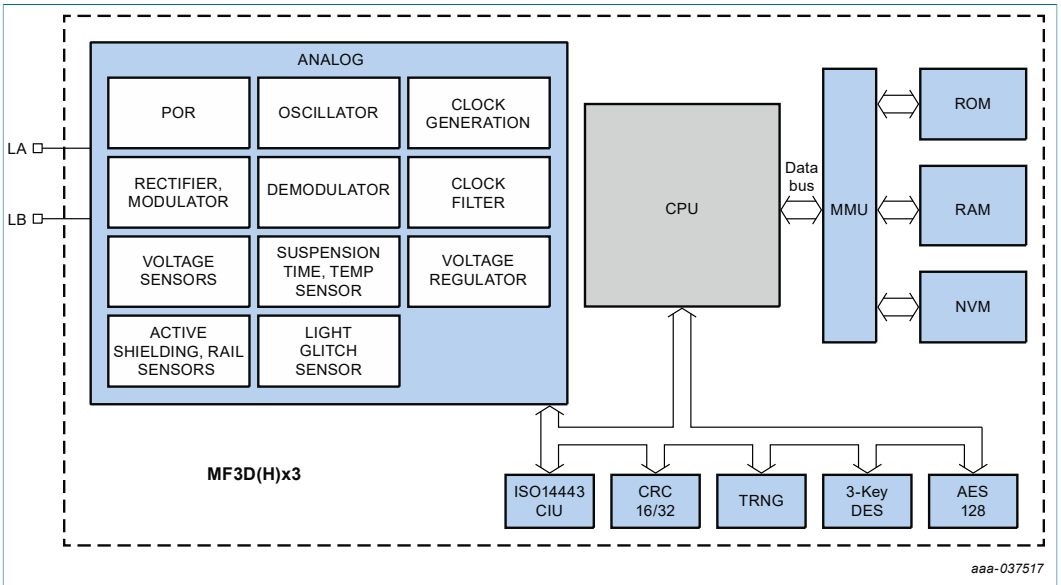


Figure 2. MIFARE DESFire EV3 IC block diagram

7 Functional description

7.1 Introduction

MIFARE DESFire EV3 is a contactless multi-application smart card IC compliant with ISOIEC 14443A (part 1-4). The MIFARE DESFire EV3 operating system provides an off-the-shelf development platform for smart card application providers.

The memory organization of MIFARE DESFire EV3 is flexible and can be dynamically structured to fit into any application requirements. The application and file structure is shown in Figure 3. Each application folder is a container of data files usable within a certain real world application (e.g. Transport ticketing). There are 5 file types available for data storage and 1 file type for storing Transaction MAC as detailed in Section 7.6.

Within the application folder, there is a set of keys and configuration settings dedicated for the application. The application owner can freely organize the file structure and security setting within his application. An adjacent application will not have access to its files as long as they do not possess the correct security rights. MIFARE DESFire EV3 also supports the ISO/IEC 7816-4 file structure and APDU.

At the PICC level, there is another set of keys and security settings for the PICC owner. The PICC owner will have the right to create or delete any application, but he will not have access to the application's files, unless he knows the application keys too.

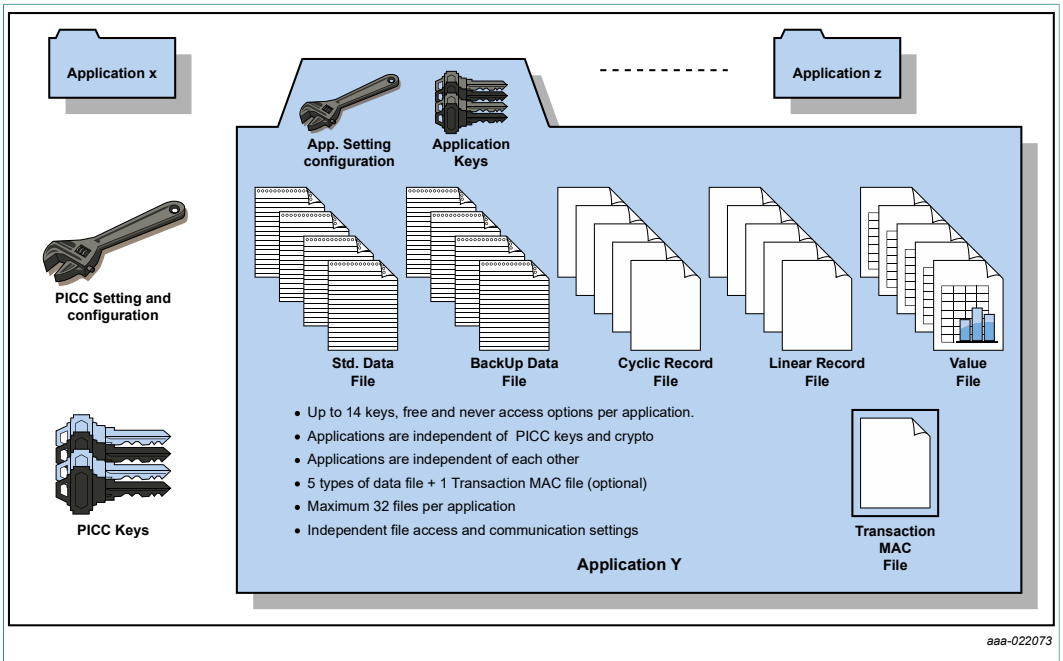


Figure 3. MIFARE DESFire EV3 product-based application and file structure

MIFARE DESFire EV3 supports confidential and integrity protected communication (see Section 7.7). Each MIFARE DESFire EV3 application can have its own cryptographic settings (i.e. 2TDEA, 3TDEA or AES) and secure messaging for communication. The D40 and EV1 secure messaging are included in the product for backward compatible support of existing installations. For new projects, the EV3 secure messaging is recommended.

MIFARE DESFire EV3 offers a transaction-oriented backup mechanism to prevent inconsistent updating of data storage across multiple files during a tearing situation. When transaction tearing occurs, either all data fields are updated or none is altered. MIFARE DESFire EV3 offers a new Transaction Timer feature which will prevent a Man-in-the-Middle (MitM) attack where the attacker delays the conclusion of a transaction by keeping the card powered after it left the legitimate reader device.

Besides the application file structure support, MIFARE DESFire EV3 offers many optional features such as following:

- Delegated Application Management (*MIsmartApp*) for giving rights to third-party application creation and management.
- Multiple key set within an application with key rolling mechanism and key migration supported.
- Shared files between two applications, supporting a single transaction over two applications at the same time.
- Multiple keys for each access right of files.
- Transaction MAC on application level, MACing the transacted data with a secret key on the card and served as a proof of transaction to the backend system.
- Secure Dynamic Messaging (SDM) which is mirror as text into the NDEF message
- Virtual Card Architecture providing a privacy protecting mechanism during card selection.
- Proximity Check to prevent against relay attacks.
- Originality Check for verification of genuine MIFARE DESFire EV3 product from NXP or its licensees.

The following chapters provide basic description of some functionality on MIFARE DESFire EV3. For a more detailed description of each functionality on MIFARE DESFire EV3, see [1].

7.2 Contactless energy and data transfer

In the MIFARE product-based system, the MIFARE DESFire EV3 is connected to a coil consisting of a few turns embedded in a standard ISO/IEC smart card. 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.

7.3 Anti-collision

An intelligent anti-collision mechanism allows more than one MIFARE DESFire EV3 in the field to be handled simultaneously. The anti-collision algorithm selects each MIFARE DESFire EV3 individually and ensures that the execution of a transaction with a selected MIFARE DESFire EV3 is performed correctly without data corruption resulting from other MIFARE DESFire EV3s in the field.

7.4 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 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 EV3 also allows Random ID to be used. In this case, MIFARE DESFire EV3 only uses a single anti-collision loop. The 3 byte random number is generated after RF reset of the MIFARE DESFire EV3.

7.5 Memory organization

The NV memory is organized using a flexible file system. This file system allows multiple numbers of different applications on one MIFARE DESFire EV3. Each application can have multiple files. Every application is represented by its 3 bytes Application IDentifier (AID) and an optional ISO DF Name.

5 different data file types and 1 Transaction MAC file type are supported; see Section 8.6.

A guideline to assign DESFire AIDs can be found in the application note *MIFARE Application Directory* (MAD); see [3].

Each file can be created either at MIFARE DESFire EV3 initialization (card production/card printing), at MIFARE DESFire EV3 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.

7.6 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
- Transaction MAC file

7.7 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 EV3 keys contribute to gain an effective anti-cloning mechanism and increase the security of the original key.

Prior to data transmission a mutual three-pass authentication can be done between MIFARE DESFire EV3 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 options of secure communication between MIFARE DESFire EV3 and PCD:

- Plain data transfer (only possible within the backwards-compatible mode to MF3ICD40 and EV2 secure messaging)
- 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. A cryptographic checksum (CMAC) will also be attached when using EV2 secure messaging.

Find more information on the security concept of the product in [1]. Be aware not all levels of security are recommended. For new design, the EV2 secure messaging is recommended.

8 DESFire command set

This section contains an overview of MF3D(H)x3 command code. A detailed description of all commands is provided in [1].

8.1 Secure Messaging Commands

Table 4. Secure messaging commands overview

Command	Description
Authenticate	Authentication as it was already supported by D40. Only for KeyType.2TDEA keys. Note that the PICC only performs encryption operations. After this authentication, the D40 backwards compatible secure messaging is used.
AuthenticateISO	Authentication as already supported by DESFire EV1. Only for KeyType.2TDEA or KeyType.3TDEA keys. After this authentication, EV1 backwards compatible secure messaging is used.
AuthenticateAES	Authentication as already supported by DESFire EV1. Only for KeyType.AES keys. After this authentication, EV1 backwards compatible secure messaging is used.
AuthenticateEV2First	Authentication for KeyType.AES keys. After this authentication, EV2 secure messaging is used. This authentication is intended to be the first in a transaction.
AuthenticateEV2NonFirst	Authentication for KeyType.AES keys. After this authentication, EV2 secure messaging is used. This authentication is intended for any subsequent authentication after Cmd.AuthenticateEV2First in a transaction.

8.2 Memory and Configuration Management Commands

Table 5. Memory and configuration management commands overview

Command	Description
FreeMem	Returns the free memory available on the card
Format	At PICC level, all applications and files are deleted. At application level (only for delegated applications), all files are deleted. The deleted memory is released and can be reused.
SetConfiguration	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.
GetVersion	Returns manufacturing related data of the PICC.
GetCardUID	Returns the UID.

8.3 Key Management Commands

Table 6. Key management commands overview

Command	Description
ChangeKey	Changes any key stored on the PICC.
ChangeKeyEV2	Depending on the currently selected AID, this command updates a key of the PICC or of one specified application keyset.

Command	Description
InitializeKeySet	Depending on the currently selected application, initialize the key set with specific index.
FinalizeKeySet	Within the currently selected application, finalize the key set with specified number
RollKeySet	Within the currently selected application, roll to the key set with specified number
GetKeySettings	Gets information on the PICC and application master key settings.
ChangeKeySettings	Changes the master key settings on PICC and application level.
GetKeyVersion	Reads out the current key version of any key stored on the PICC.

8.4 Application Management Commands

Table 7. Application management commands overview

Command	Description
CreateApplication	Creates new applications on the PICC. The application is initialized according to the given settings. The application keys of the active key set are initialized with the Default Application Key.
DeleteApplication	Permanently deactivates applications on the PICC.
CreateDelegatedApplication	Creates delegated applications on the PICC with limited memory consumption.
SelectApplication	Selects one specific application for further access.
GetApplicationIDs	Returns the Application IDentifiers of all applications on a PICC.
GetDFNames	Returns the DF names
GetDelegatedInfo	Returns the *DAMSlotVersion* and *QuotaLimit* of a target DAM slot on the card.

8.5 File Management Commands

Table 8. File management commands overview

Command	Description
CreateStdDataFile	Creates files for the storage of plain unformatted user data within an existing application on the PICC.
CreateBackupDataFile	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.
CreateValueFile	Creates files for the storage and manipulation of 32bit signed integer values within an existing application on the PICC.
CreateLinearRecordFile	Creates files for multiple storages 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.

Command	Description
CreateCyclicRecordFile	Creates files for multiple storages 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.
CreateTransactionMACFile	Creates a Transaction MAC File and enables the Transaction MAC feature for the targeted application.
DeleteFile	Permanently deactivates a file within the file directory of the currently selected application.
GetFileIDs	Returns the File IDentifiers of all active files within the currently selected application.
GetISOFileIDs	Get back the ISO File ID.
GetFileSettings	Get information on the properties of a specific file.
ChangeFileSettings	Changes the access parameters of an existing file.

8.6 Data Management Commands

Table 9. Data management commands overview

Command	Description
ReadData	Reads data from FileType.StandardData or FileType.BackupData.
WriteData	Writes data to FileType.StandardData or FileType.BackupData
GetValue	Reads the currently stored value from FileType.Value.
Credit	Increases a value stored in a FileType.Value.
Debit	Decreases a value stored in a FileType.Value.
LimitedCredit	Allows a limited increase of a value stored in a FileType.Value without having full Credit permissions to the file.
ReadRecords	Reads out a set of complete records from a FileType.CyclicRecord or FileType.LinearRecord.
WriteRecord	Writes data to a record in a FileType.CyclicRecord or FileType.LinearRecord.
UpdateRecord	Updates data of an existing record in a FileType.LinearRecord or FileType.CyclicRecord file.
ClearRecordFile	Resets a FileType.LinearRecord or FileType.CyclicRecord to empty state.

8.7 Transaction Management Commands

Table 10. Transaction management commands overview

Command	Description
CommitTransaction	Validates all previous write access' on FileType.BackupData, FileType.Value, FileType.LinearRecord and FileType.CyclicRecord within one application.
AbortTransaction	Invalidates all previous write access' on FileType.BackupData, FileType.Value, FileType.LinearRecord and FileType.CyclicRecord within one application.

Command	Description
CommitReaderID	Commits a ReaderID for the ongoing transaction. This will allow a backend to identify the attacking merchant in case of fraud detected.

8.8 ISO/IEC 7816-4 Standard Commands

Table 11. ISO/IEC 7816-4 support commands overview

Command	Description
ISOSelectFile	Selects either the PICC level, a DESFire application or a DESFire file within an application.
ISOReadBinary	Read data from FileType.StandardData and FileType.BackupData files.
ISOUpdateBinary	Write data to FileType.StandardData and FileType.BackupData files.
ISOReadRecord	Read data from FileType.LinearRecord and FileType.CyclicRecord files.
ISOAppendRecord	Write a new record to FileType.LinearRecord and FileType.CyclicRecord files.
ISOGetChallenge	To initiate a ISO/IEC 7816-4 authentication
ISOExternalAutheticate	Authenticate the PCD during a ISO/IEC 7816-4 authentication
ISOInternalAuthenticate	Authenticate the PICC during a ISO/IEC 7816-4 authentication

8.9 Virtual Card Commands

Table 12. Virtual Card commands overview

Command	Description
ISOSelect	Select VC with the given IID.
ISOExternalAuthenticate	Authenticate PCD before accessing the VC.

8.10 Proximity Check Commands

Table 13. Proximity Check commands overview

Command	Description
PreparePC	Prepare for the Proximity Check
ProximityCheck	Perform the precise measurement for the Proximity Check
VerifyPC	Verify the Proximity Check

8.11 Originality Check Commands

Table 14. Originality Check commands overview

Command	Description
Read_Sig	Retrieve the ECC originality check signature

9 Limiting values

Table 15. Limiting values [1][2]

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

Symbol	Parameter	Conditions	Min	Max	Unit
$P_{d,max}$	maximum power dissipation		-	240	mW
$I_{LA-LB,max}$	maximum input current at LA/LB		-	86	mA
T_{stg}	storage temperature		-55	125	°C
T_{amb}	ambient temperature		-25	85	°C
V_{ESD}	electrostatic discharge voltage	[3]	-	4	kV

[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] ANSI/ESDA/JEDEC JS-001; Human body model: C = 100 pF, R = 1.5 kΩ

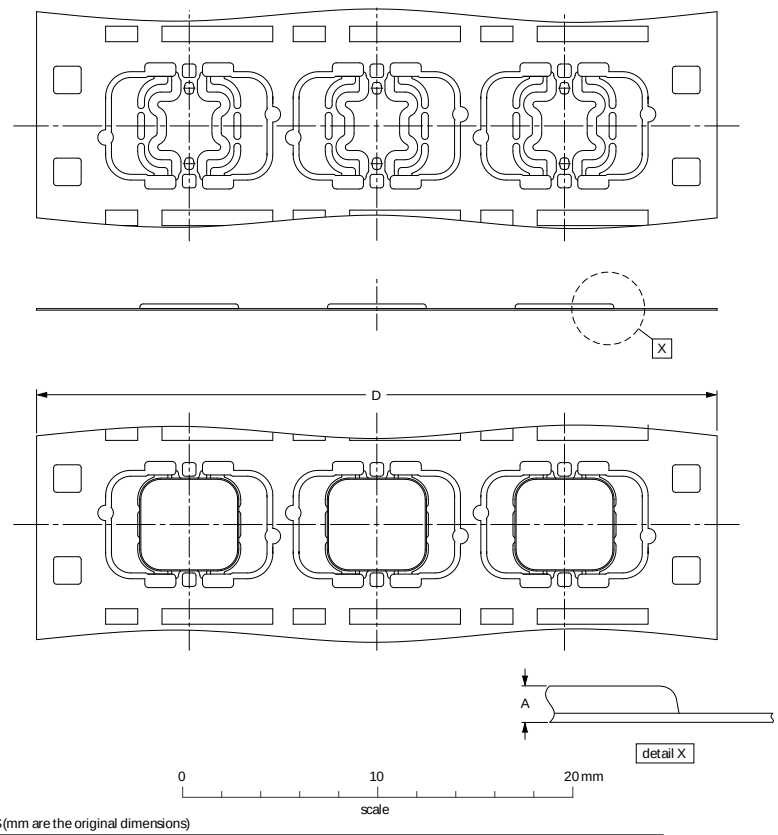
CAUTION

This device is sensitive to ElectroStatic Discharge (ESD). Observe precautions for handling electrostatic sensitive devices.

Such precautions are described in the *ANSI/ESD S20.20, IEC/ST 61340-5, JESD625-A* or equivalent standards.

10 Package outline

PLLMC: plastic leadless module carrier package; 35 mm wide tape SOT500-2



DIMENSIONS (mm are the original dimensions)

UNIT	A(1) max.	D	
mm	0.33	35.05 34.95	For unspecified dimensions see PLLMC-drawing given in the subpackage code.

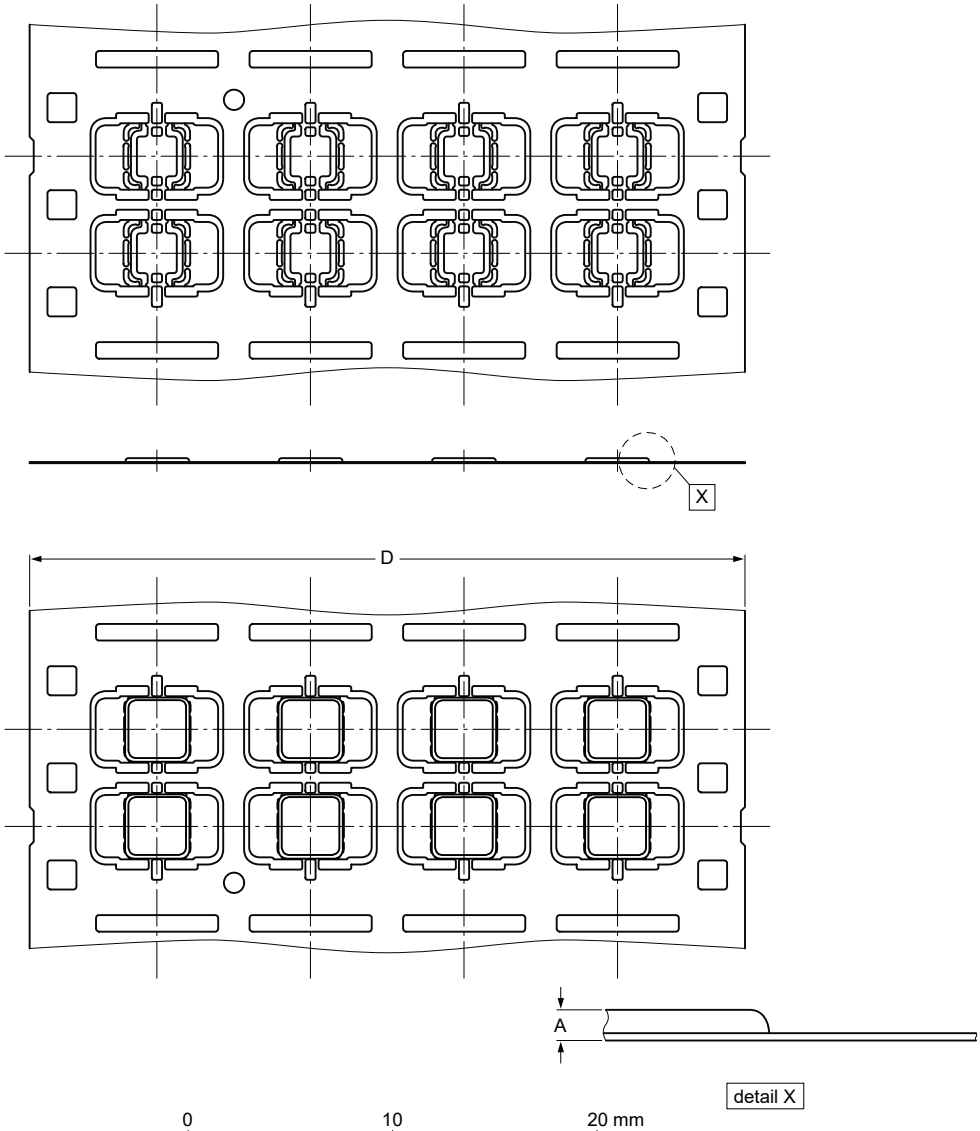
Note

1. Total package thickness, exclusive punching burr.

OUTLINE VERSION	REFERENCES				EUROPEAN PROJECTION	ISSUE DATE
	IEC	JEDEC	JEITA			
SOT500-2	---	---	---			03-09-17 06-05-22

Figure 4. Package outline SOT500-2 (MOA4)

PLLMC: plastic leadless module carrier package; 35 mm wide tape **SOT500-4**



Dimensions

Unit		A(1)	D
mm	max	0.26	35.05
	nom		35.00
	min		34.95

For unspecified dimensions see PLLMC-drawing given in the subpackage code.

Note
1. Total package thickness, exclusive punching burr.

sot500-4_po

Outline version	References				European projection	Issue date
	IEC	JEDEC	JEITA			
SOT500-4	- - -	- - -	- - -			11-02-18

Figure 5. Package outline SOT500-4 (MOA8)

11 Abbreviations

Table 16. 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

12 References

[1] Data sheet *MF3D(H)x3 MIFARE DESFire EV3 Product data sheet*, document number: 4870**[1].

[2] Data sheet *MF3D(H)x3 Wafer specification*, document number: 5808**.

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

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

13 Revision history

Table 17. Revision history

Document ID	Release date	Data sheet status	Change notice	Supersedes
MF3Dx3_MF3DHx3_ SDS v. 3.0	20200515	Product short data sheet	-	-

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.

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.

14.3 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. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. 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 and its suppliers accept 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.

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.

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 competent authorities.

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.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

14.4 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.

Purchase of NXP ICs with NFC technology

Purchase of an NXP Semiconductors IC that complies with one of the Near Field Communication (NFC) standards ISO/IEC 18092 and ISO/IEC 21481 does not convey an implied license under any patent right infringed by implementation of any of those standards. Purchase of NXP Semiconductors IC does not include a license to any NXP patent (or other IP right) covering combinations of those products with other products, whether hardware or software.

14.5 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.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

Figures

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: 15 May 2020
Document identifier: MF3D_H_x3_MIFARE_DESFire_EV3_SDS
Document number: 612530