# MF3E(H)x3_SDS

## MIFARE DUOX contactless smartcard IC

Rev. 1.0 — 12 November 2024 Product short data sheet
974510

# 1 General description

## 1.1 Introduction

MF3E(H)x3 is the latest addition to the MIFARE product family introducing new features and new crypto protocols by offering ECC asymmetric cryptography and PKI support, along with enhanced performance for best user experience. As first product in the MIFARE family supporting asymmetric cryptographic features, MIFARE DUOX opens up new use cases and allows simplified key management as well as simplified key distribution approaches, relying on PKI functionality.

MF3E(H)x3 supports both symmetric as well as asymmetric cryptography in form of AES128, AES256 or ECC cryptographic protocols. For asymmetric cryptogryphic support, the IC features keypair generation, signature generation and verification as well as PKI based X.509 certificate handling. The newly introduced asymmetric cryptographic protocols allow for a simplified key management and increased system security as the risk associated to secret key leakage from the reader terminal, that can be abused for credential cloning, is eliminated.

The MF3E(H)x3 is Common Criteria EAL6+ 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, but still relying on a high secure product, without compromises on security.

MF3E(H)x3 offers best flexibility when creating multi-application schemes on one smartcard IC. Features such as Delegated Application Management are supporting flexible business models. Smart City services could be utilized with only one smartcard by combining services such as access aplications (access to city attractions, corporate and governmental access), car or bike sharing, citizen services, car access applications and electric vehicle charging applications.

MF3E(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 installations for MIFARE infrastructure. Additionally, MF3E(H)x3 is compliant with NFC Forum Tag Type 4 and obtained the NFC Forum certification, as seen in Figure 1, allowing creation of NDEF formatted applications on the IC.

Depending on the chosen delivery and package type, MF3E(H)x3 features can be utilized via the NFC interface or via the newly introduced $I^2C$ interface (which is optionally available on selected product configurations).

Featuring an on-chip backup management system and the mutual authentication, a MF3E(H)x3 card can hold as many applications as the memory can accommodate. Each application can hold up to 32 files with various file configurations and different settings that can be applied. The size of each file is defined at the moment of its creation, making MF3E(H)x3 a truly flexible and convenient product. An automatic anti-tearing mechanism is available for all file types, guaranteeing transaction-oriented data integrity.

The main characteristics of this device are underpinned by the outstanding position of the MIFARE product portfolio as fast, innovative, reliable and secure smartcard ICs in the contactless proximity transaction market.

MF3E(H)x3 delivers the perfect balance of speed, performance and cost efficiency. Its open concept allows seamless future integration of other smartcard media such as smart paper tickets, banking convergence card, and MIFARE 2GO mobile ticketing service based on Near Field Communication (NFC) technology. MF3E(H)x3 is your entrance to secure contactless systems worldwide.


**Figure 1. NFC Forum certification for MF3E(H)x3**

# 2 Features and benefits

## 2.1 Feature overview

### 2.1.1 RF interface: ISO/IEC 14443 Type A

- Contactless interface compliant with ISO/IEC 14443-2/3/4 A
- Contactless transmission protocol using ISO/IEC 14443-4
- 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
- Very High Bit Rate (VHBR): 1.7 Mbit/s and 3.4 Mbit/s - PICC to PCD only
- Configurable FSCI to support up to 256 bytes frame size

### 2.1.2 Non-volatile memory

- 2 kB, 4 kB or 8 kB standard memory sizes are available
- 16 kB memory size is available for applications requesting a large user memory size
- Data retention of 25 years
- Write endurance of typical 1 000 000 cycles

### 2.1.3 NV-memory organization and multi-application support

- **Flexible application management on the IC**
  - Flexible file system offering the user free definition of application and file structures on the PICC
  - Amount of applications is not limited: applications can be created as long as there is free user memory available on the PICC
  - Shared application management allows to access files from any two applications during a single transaction if access rights are configured accordingly
- **Flexible and dynamic file management inside the applications**
  - Amount of files per application is set to 32: up to 32 files can be created in each application
  - Availability of 6 file types: Standard Data file, Backup Data file, Value file, Linear Record file, Cyclic Record file and Transaction MAC file
  - File size is determined during the file creation (exception for Transaction MAC file)
- **Delegated Application Management feature** allows smart management of multiple applications per smartcard shared by different entities
  - Memory can be re-used in delegated applications (via formatting the complete delegated application)
  - Factory loaded NXP's Delegated Application Management (DAM) keys for a remote application management service support

### 2.1.4 Security and Privacy

- Common Criteria certification: CC EAL6+ AVA_VAN.5 on Hardware and Software
- 7 bytes unique identifier (UID) for each device
- Optional 4 bytes random ID can be enabled, for enhanced security and privacy of the device
- Hardware exception sensors are in place
- Self-securing file system is implemented
- **Symmetric cryptography features**:
  - Mutual AES-based three-pass authentication
  - Flexible symmetric key management: One card master key and up to 14 application keys per application key set
  - Multiple key sets per application with fast key rolling mechanism (up to 16 key sets per application)
  - Hardware AES co-processor supporting AES 128-bit keys or AES 256-bit keys
- **Asymmetric cryptography features**:
  - Mutual and Reader-Unilateral ECC-based authentication
  - Card-Unilateral ECC-based authentication
  - Flexible certificate / asymmetric keypair management and certificate management:
    - Up to two CA Public Keys at PICC level
    - Up to five CA Public Keys per application
    - Up to five private keys per application
  - ECC key pair generation over NIST curve P-256 and brainpoolP256r1
  - Hardware ECC co-processor supporting ECC 256-bit keys
  - ECC based Originality Check feature ensures proof of genuine NXP products
- **Access Rights Management**:
  - Multiple key assignment for each file access rights (up to eight)
  - Unified access right management system allowing for mixed applications with symmetric- and asymmetric-based authentication access control
- **Secure Messaging**:
  - Secure channel with AES-based data encryption and data authenticity ensured by CMAC
  - Authentication can be executed on card and on application level
- **Security related features**:
  - Transaction MAC and Transaction Signature features are available for symmetric and asymmetric cases, ensuring generating secure checksum / secure signature per application and executed transaction
  - Transaction Timer feature is available to protect against Man-in-the-Middle attacks
  - Proximity Check feature is offered for protection against Relay Attacks
- **Originality Check feature ensuring authenticity of the product**:
  - Dynamic ECC based Originality Check to ensure proof of genuine NXP products
  - MIFARE DUOX is pre-provisioned with an Originality Check ECC-based key pair and related certificate, allowing the verification of the genuineness of the IC
  - Executed via a card-unilateral authentication through a challenge-response protocol

### 2.1.5 ISO/IEC 7816 compatibility

- Supports ISO/IEC 7816-4 file structure (selection by File ID or by DF name)
- Supports ISO/IEC 7816-4 APDU message structure
- Supports ISO/IEC 7816-4 APDU wrapper for MF3E(H)x3 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 ‘87’ for GENERAL AUTHENTICATE
- Supports ISO/IEC 7816-4 INS code ‘88’ for INTERNAL AUTHENTICATE

### 2.1.6 Special features

MF3E(H)x3 offers a wide variety of avaialble features that can be consumed and configured individually on the IC. The flexibiliy of feature-availability allows a customization of the product according to the needs and requirements of the customer.

- **Various configuration options on the IC via the SetConfiguration command**:
  - Configurable ATS and contacltess protocol parameter (ATQA, SAK) configuration: Offering flexible NFC parameter settings to fit the customer`s NFC reader infrastructure requirements
  - Secure Messaging related configuration: Offering selection of authentication and secure messaging related detail setting, including curve selection for asymmetric authentication protocol, optional asymmetric private key usage limitation, and authentication counter setting
  - Card and application level configuration: Offering specific settings to apply configurations for ISODFName, VCIID, Capability Data, Application Default Keys, etc
  - Communication channel configuration: Offering settings to define NFC, $I^2C$ and GPIO related detailed settings (if applicable to the product type / product configuration, and if required)
- **Inclusion of asymmetric cryptography to the product**:
  - Aditionally to the symmetric AES128 and AES256 functionality also ECC asymmetric cryptography is supported
  - Major functionality related to ECC is added to MF3E(H)x3 (e.g. ECC-based authentication, certificate management, asymmetric key management, PKI functionality etc)
- **Transaction Signature feature**:
  - Similar functionality offered as via the symmetric Transaction MAC feature which is consuming AES128 or AES256 symmetric crypto. Transaction Signature is based on asymmetric ECDSA signature which is calculated on top the executed transaction, allowing for reduced security requirements on the reader / back-end infrastructure storage, as only a public key is required for validation
- **Transaction Timer feature**:
  - Feature to prevent Man-in-the-Middle (MitM) attacks where the attacker delays the conclusion of a transaction by keeping the card powered after it left the legitimate reader device
- **Secure Unique NFC (SUN) enabled by Secure Dynamic Messaging (SDM)** to ensure confidential and integrity-protected data exchange without prior authentication. There are two flavors of the feature available on MF3E(H)x3:
  - Symmetric SDM MAC: data is protected by a MAC generated by a symmetric AES key
  - Asymmetric SDM SIG: data is protected by a ECDSA signature generated by the private key of an ECC key pair
  - SUN / SDM allows adding security to the data that´s read out from the chip, while still being able to access it with standard NDEF readers for NFC Forum Tag Type 4 formatted cards.
  - The typical use case is an NDEF holding a URI and some meta-data, where SDM allows this meta-data to be communicated confidentiality and integrity protected toward a backend server.

- **NFC Forum Type 4 Tag certification of the IC**, allowing to store NDEF Tag Type 4 formatted messages on the IC, for an automated interaction when tapping the smartcard to an NFC enabled mobile device
- **Product versions** offering both the low input and high input capacitance versions (17 pF and 70 pF):
  - Allowing to optimally tune smartcard IC antennas for any kind of form factor size and design (standard ID-1 sized smartcards or smaller form factors like wristbands, key fobs, tokens, etc)
- **Compatibility to MIFARE DESFire products:**
  - MF3E(H)x3 is based on the same underlying file system concept as exisitng products in the MIFARE DESFire product family. The concept of applications and files that can be created on the PICC is backwards-compatible.
  - MF3E(H)x3 is functional compatible to the AES-128 cryptographic mechanisms of the MIFARE DESFire EV3 product. Support and compatibility for DES, 2K3DES and 3K3DES cryptographic mechanisms has been disabled on MF3E(H)x3.
  - Existing card layouts that are based on MIFARE DESFire EV3 utilizing AES-128 cryptography can be ported to MIFARE DUOX.
- **Compliancy to Automotive Industry regulations and requirements:**
  - Compliancy of MF3E(H)x3 to ISO / SAE 21434 cyber security regulations
  - Compliancy to the MISRA-C coding standard
  - Dedicated Automotive-like qualification on silicon level of MF3E(H)x3, which is based on a dedicated qualification flow including cold test
  - Support of an extended temperature range from -40 °C up to 105 °C operating condition on silicon level, which is the perfect fit for automotive environments
  - Fast ECC-based authentication for initial pairing between smartcard IC and vehicle
  - Proximity Check feature as key functionality to prevent Relay Attacks in the automotive segment
- **Compliancy to Electric Vehicle Charging (EV-Charging) Industry regulations and requirements**:
  - Utilizing PKI capability of MF3E(H)x3 for enabling interoperability between multiple CPOs and EMSPs
  - Seamless feasibility to use one smartcard in multiple EV-Charging networks (tremendous end user benefit)
  - Compliancy to the VDE-DKE regulation VDE-AR-E 2532-100 (support of required file structure and command support for electric vehicle charging applications)
    - Availability of the required command set to interact with EV-Charging stations as per the mentioned guideline
    - Provisioning of required card layout, application structure, configuration settings, asymmetric keypair and certificate during the NXP Trust Provisioning process (available in a dedicated product type with dedicated part number)

# 3 Target Applications

MF3E(H)x3 is the future proven secure contactless smartcard IC for applications demanding flexibility, dynamic key provisioning and high security.

The potential application areas and use case possibilities vary from a wide spectrum of available scenarios. Depending on client and customer requirements, MF3E(H)x3 can be positioned in countless different applications as the product' s features and configuration options give the broadest possibilities to tailor the product to the individual end customer requirements.

Ideal and examplary target application are

- Physical Access Management (corporate, governmental, high-security areas, etc)
  - Especially aiming at multi-site Access Management systems, MF3E(H)x3 is the perfect fit to realize versatile and enhanced access infrastructures.
  - Secure Car Access Management and Digital Car Key Management (secure access to vehicle and start of engine)
  - Electric Vehicle Charging (user authorization to start EV-charging session, EV-charging credential, EV-charging membership card, etc). For the EV-Charging vertical, a dedicated product configuration is available, which features pre-loaded data and keys inside the MIFARE DUOX user memory.
  - Car and Vehicle Sharing (car, scooter, electric vehicle sharing applications, etc)

# 4 Ordering information

MF3E(H)x3 is available in one major product versions which can be used for all use cases and verticals.

An additional, second trust-provisioned configuration is available, which is building on top of the major product version. This product version includes trust-provisioned (pre-loaded) EV-Charging specific data structure, keys and related certificates.

The product configuration information is part of the product version information which can be read-out from the IC with the GetVersion command, as defined in [1]. Retrieving all details of the product version is possible with the GetVersion command.

The MIFARE DUOX MF3E(H)x3 product is characterized through following aspects:

- Extended product qualification flow meeting automotive industry requirements
- Additional cold-test during product qualification
- Extended temperature range for operating conditions of IC: -40°C up to +105°C on silicon level

The product type list and ordering information is available in following subsections:

- MIFARE DUOX ordering information: Ordering information for MIFARE DUOX product
- MIFARE DUOX for EV-Charging ordering information: Ordering information for MIFARE DUOX EV-Charging ../01EV product

# 5 Block diagram

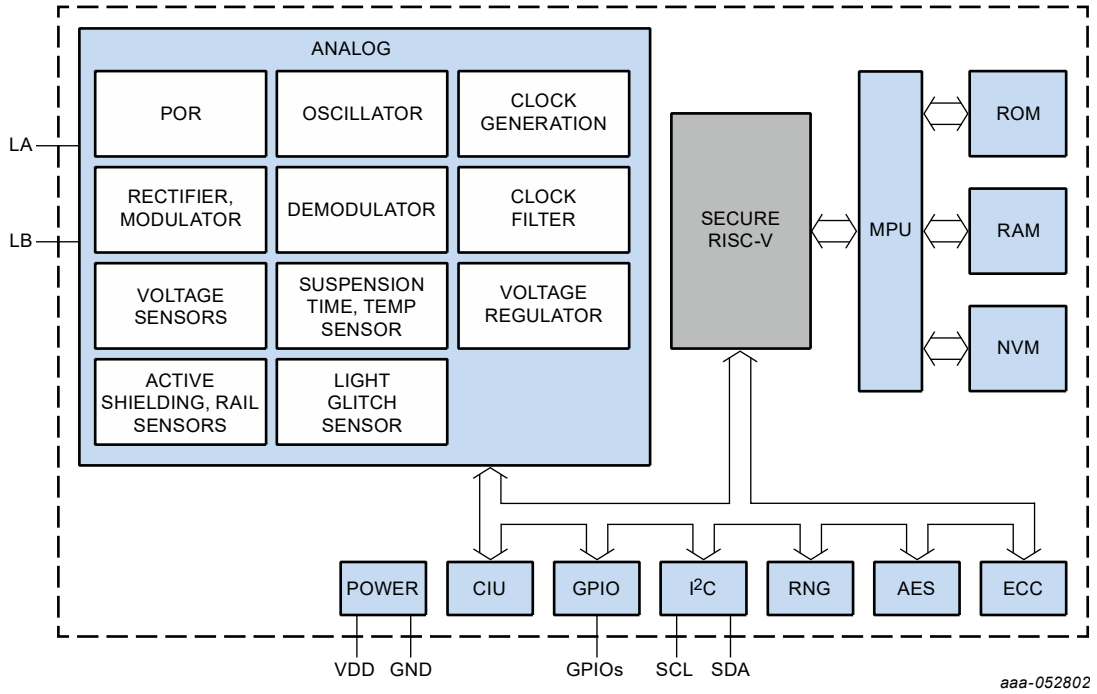



**Figure 2. MIFARE DUOX block diagram**

# 6 Functional description

MF3E(H)x3 is a contactless multi-application smart card IC compliant with ISOIEC 14443A (part 1-4) and provides an off-the-shelf platform for smart card application providers.

MF3E(H)x3 builds on the feature set of MIFARE DESFire EV3. This document describes the full functionality, that is, including MIFARE DESFire functionality.

The memory organization of MF3E(H)x3 is flexible and can be dynamically structured to fit into any application requirements, like it is already known from the MIFARE DESFire EV3 product.

Each application folder is a container of data files usable within a certain real-world application (for example, access management). There are five file types available for data storage and one file type for storing Transaction MAC.

Within the application folder, there is a set of keys, certificates, and configuration settings dedicated for the application. The application owner can freely organize the file structure and security settings within their application. An adjacent application will not have access to its files as long as they do not possess the correct security rights.

MF3E(H)x3 also supports the ISO/IEC 7816-4 file structure and APDUs.

MF3E(H)x3 supports confidential and integrity-protected communication. The EV2 secure messaging provides state-of-the-art crypto and security utilization.

Additionally, MF3E(H)x3 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.

Besides the application file structure support, which is already well known from the MIFARE DESFire EV3 product, the MF3E(H)x3 product offers many new and enhanced features.

The following list gives an overview of the main new features, compared to MIFARE DESFire EV3:

- ECC-based Mutual and Reader-Unilateral Authentication.
- ECC-based Card-Unilateral Authentication. This is also used for Originality Checking purposes. Additionally generic ECDSA support is offered.
- The access right management has been extended for the ECC-based authentications.
- Asymmetric key management for ECC keys.
- Other existing symmetric features have been extended with an ECC-based equivalent:
  - Transaction MAC with the Transaction Signature.
  - Secure Dynamic Messaging with an ECC-based signature.
- Symmetric crypto features have been extended with AES-256 support
  - AES-based symmetric authentication.
  - AES-based symmetric secure messaging (EV2 Secure Messaging).
  - Secure Dynamic Messaging.
  - The symmetric key management.
  - Transaction MAC.
  - Proximity Check.
- EV charging support. This is supporting the command set as defined by VDE-AR-E 2532-100.
- SetConfiguration command has been extended for the new features. GetConfiguration command is introduced to allow retrieval of the configurations.

The following features are not supported on MF3E(H)x3 compared to MIFARE DESFire EV3:

- D40 and EV1 authentication and secure messaging. This includes the ISO/IEC 7816-4 based authentication. From the latter, only ISOGetChallenge command is supported as a generic random source. This means that for symmetric authentication only EV2 authentication and secure messaging is supported. The EV2 secure messaging is also used as the secure channel after an ECC-based mutual or reader-unilateral authentication.
- The AES-based Originality Check and the Originality Check based on a static ECDS signature have been replaced by an ECC-based challenge-response protocol.
- The privacy preserving Virtual Card Selection method and related AuthVCMandatory and AuthPCMandatory configurations.
- MIFARE Classic support. The MIFARE Classic mapping as supported by MIFARE DESFire EV3 is not supported.
- At delivery the PICCMasterKey is configured as an AES128 key instead of a 2TDEA key.

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

# 7 MF3E(H)x3 command set

This section contains an overview of MF3E(H)x3 command codes. A detailed description of all commands is provided in [1].

## 7.1 Secure Messaging Commands

**Table 1. Secure messaging commands overview**

| Command | Description |
|---|---|
| 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. |
| ISOGeneralAuthenticate | Authentication for KeyType.ECC keys using the Station-to-Station protocol for authenticated key agreement. After this authentication, EV2 secure messaging is used. |
| ISOGeneralAuthenticateFinal | Authentication for KeyType.ECC keys using the Station-to-Station protocol for authenticated key agreement. After this authentication, EV2 secure messaging is used. The authentication consists of two parts Cmd.ISOSelectFile and Cmd.ISOGeneralAuthenticateFinal. It can only be initiated after a successfully executed Cmd.ISOSelectFile. |
| ISOInternalAuthenticate | Authentication for KeyType.ECC keys for performing the ECC-based card unilateral authentication protocol. This protocol can be applied for the Originality Check purpose. |

## 7.2 Memory and Configuration Management Commands

**Table 2. 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 | Updates the card or application configuration settings (e.g. Random ID configuration, ATS configuration, Secure Messaging configuration, Special feature enablement, etc). |
| GetConfiguration | Retrieves card or application configuration settings as defined with SetConfiguration. |
| GetVersion | Returns manufacturing related data of the PICC. |
| GetCardUID | Returns the UID of the PICC. |

## 7.3 Symmetric Key Management Commands

**Table 3. Symmetric Key Management commands overview**

| Command | Description |
|---|---|
| ChangeKey | Changes an AES128 or AES256 key stored on the PICC or application level. |
| ChangeKeyEV2 | Changes an AES128 or AES256 key stored on the PICC or application level. It additionally includes information about the application keyset where the key to be changed is located. |

**Table 3. Symmetric Key Management commands overview***...continued*

| Command | Description |
|---|---|
| InitializeKeySet | Depending on the currently selected application, the specified key set is initialized with a key type. |
| FinalizeKeySet | Within the currently selected application, the specified key set is finalized. |
| RollKeySet | Within the currently selected application, a key set rolling to the specified key set takes place. |
| GetKeySettings | Returns PICCKeySettings or AppKeySettings (configurations from PICC level or application level). In addition it returns the number of keys which are configured for the application, if applicable. |
| ChangeKeySettings | Changes the PICCKeySettings on PICC level or the AppKeySettings on application level. |
| GetKeyVersion | Reads out the current key version of any key stored on the PICC level or application level. |

## 7.4 Asymmetric Key Management Commands

**Table 4. Asymmetric Key Management commands overview**

| Command | Description |
|---|---|
| ManageKeyPair | Creates or updates a private key entry by generating a key pair or importing a private key. |
| ManageCARootKey | Creates or updates a public key entry for storing a KeyID.CARootKey. |
| ExportKey | Exports the public key value of a KeyID.CARootKey. |
| GetKeySettings | Returns PICCKeySettings or AppKeySettings (configurations from PICC level or application level). In addition it returns the number of keys which are configured for the application, if applicable. |

## 7.5 Application Management Commands

**Table 5. 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. The application is initialized according to the given settings. The application keys of the active key set are initialized with the Default Application Key. |
| SelectApplication | Selects one or two specific applications, or the PICC level, specified with the Application Identifiers (AIDs). |
| GetApplicationIDs | Returns the Application IDentifiers (AIDs) of all applications on a PICC. |
| GetDFNames | Returns the Application IDentifiers (AIDs) together with a File ID and DF name of all active applications with ISO/IEC 7816-4 support. |
| GetDelegatedInfo | Returns the DAMSlotVersion and QuotaLimit of a target Delegated Application Management (DAM) slot on the card. |

## 7.6 File Management Commands

**Table 6. 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. |
| 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 or Transaction Signature feature for the targeted application. |
| DeleteFile | Permanently deactivates a file within the file directory of the currently selected application. |
| GetFileIDs | Returns the File IDentifiers (File IDs) of all active files within the currently selected application. |
| GetISOFileIDs | Returns the ISO File IDentifiers (ISO File IDs) of all active files within the currently selected application. |
| GetFileSettings | Returns information on the properties and configuration settings of a specific file. |
| GetFileCounters | Returns information about the file related counters used for Secure Dynamic Messaging. |
| ChangeFileSettings | Changes the file configuration settings of the specific file (e.g. file access parameters, file options, feature configuration, etc). |

## 7.7 Data Management Commands

**Table 7. Data management commands overview**

| Command | Description |
|---|---|
| ReadData | Reads data from FileType.StandardData, FileType.BackupData or FileType. TransactionMAC files. |
| 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.Linear Record. |

**Table 7. Data management commands overview***...continued*

| Command | Description |
|---|---|
| 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.Cyclic Record file. |
| ClearRecordFile | Clears all records of a FileType.LinearRecord or FileType.CyclicRecord (reset to an empty file state). |

## 7.8 Transaction Management Commands

**Table 8. Transaction management commands overview**

| Command | Description |
|---|---|
| CommitTransaction | Validates all previous write accesses on FileType.BackupData, FileType.Value, File Type.LinearRecord and FileType.CyclicRecord files within the selected application(s).<br>If applicable, the FileType.TransactionMAC file is updated with the calculated Transaction MAC or Transaction Signature. |
| AbortTransaction | Invalidates all previous write accesses on FileType.BackupData, FileType.Value, File Type.LinearRecord and FileType.CyclicRecord files within the selected application(s).<br>If applicable, the TransactionMAC calculation is aborted. |
| CommitReaderID | Commits a ReaderID for the ongoing transaction. This will allow a backend to identify the attacking merchant / reader terminal, in case of fraud detected. |

## 7.9 Cryptographic Support Commands

**Table 9. Cryptographic Support commands overview**

| Command | Description |
|---|---|
| CryptoRequest | Executes a cryptographic operation. This is the generic API definition, including common error<br>codes. Specific operations are further defined by dedicated subcommands (Crypto Request_ECCSign, CryptoRequest_Echo). |
| CryptoRequest_ECCSign | Executes an ECC signature generation.<br>It supports signing a precomputed hash, or raw data, which means the hash operation is executed by MF3E(H)x3 on the fly. If the data is raw, the signature can be computed via a one-shot operation, or in the case of bigger input data, via an init-update-final mechanism. |
| CryptoRequest_Echo | Supports to return the provided command data. This allows to easily test the communication interface. |

## 7.10 ISO/IEC 7816-4 Standard Commands

**Table 10. 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. |

**Table 10. ISO/IEC 7816-4 support commands overview***...continued*

| Command | Description |
|---|---|
| ISOAppendRecord | Write a new record to FileType.LinearRecord and FileType.CyclicRecord files. |
| ISOGetChallenge | To initiate a ISO/IEC 7816-4 authentication |

## 7.11 Proximity Check Commands

**Table 11. 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. |

## 7.12 EV Charging Commands

**Table 12. EV Charging commands overview**

| Command | Description |
|---|---|
| VDE_ReadData | Reads data from FileType.StandardData with FileNo 0x00 or 0x01. |
| VDE_WriteData | Writes data to FileType.StandardData with FileNo 0x01, and eventually locks the file. |
| VDE_ECDSASign | Generates a ECDSA signature over a 32-byte challenge. |

## 7.13 Originality Check Commands

**Table 13. Originality Check commands overview**

| Command | Description |
|---|---|
| ISOInternalAuthenticate | For the asymmetric originality check procedure, the card-unilateral authentication via ISOInternalAuthenticate shall be used. |

# 8 Limiting values

## 8.1 Limiting Values applicable to MOA8

**Table 14. Limiting values for MOA8[1][2]**

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

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $I_{LA-LB,max}$ | maximum input current at LA/LB | - | - | 100 | mA |
| $V_{ESD}$ | electrostatic discharge voltage | [3] | - | 4 | kV |
| $P_{d,max}$ | maximum power dissipation | - | - | 80 | mW |
| $T_{stg}$ | storage temperature | | -55 | 125 | °C |
| $T_{amb}$ | ambient temperature for product in MOA8 delivery form | | -25 | 85 | °C |

[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

## 8.2 Limiting Values applicable to bumped FFC

**Table 15. Limiting values for bumped wafer on FFC[1][2]**

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

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $I_{LA-LB,max}$ | maximum input current at LA/LB | - | - | 100 | mA |
| $V_{ESD}$ | electrostatic discharge voltage | [3] | - | 4 | kV |
| $P_{d,max}$ | maximum power dissipation | - | - | 80 | mW |
| $T_{stg}$ | storage temperature | | -55 | 125 | °C |
| $T_{amb}$ | ambient temperature for product in bumped wafer on FFC delivery form | | -40 | 105 | °C |

[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.

# 9 Quick reference data

Characteristics described in this section are applicable to all product delivery types.

Further details can be retrieved from the full product datasheet, [1].

**Table 16. Electrical AC Characteristics of antenna pins LA, LB**

*$V_{CC}$ = 1 V to 1.98 V; $V_{SS}$ = 0 V; $T_{amb}$ = -40 °C to 105 °C, unless otherwise specified* [1]

| Symbol | Parameter | Conditions | Min | Typ[2] | Max | Unit |
|---|---|---|---|---|---|---|
| $f_{LALB}$ [3] | Operating frequency LA, LB | - | - | 13.56 | - | MHz |
| $C_{LALB}$ [3] | configured for antenna input with 17 pF capacitance. Test frequency = 13.56 MHz; $T_{amb}$ = 25 °C | $V_{LA,LB}$ = 2.1 V (rms)<br>$V_{LA,LB}$ = 0.3 V (rms) | - | 17.6 - 17.3 | - | pF |
| $C_{LALB}$ [3] | Configured for antenna input with 69 pF capacitance. Test frequency = 13.56 MHz; $T_{amb}$ = 25 °C | $V_{LA,LB}$ = 2.1 V (rms) | - | 68.1 | - | pF |
| $R_{LALB}$ [3][4][5][6] | Configured for antenna input with 17 pF capacitance. Test frequency = 13.56 MHz; $T_{amb}$ = 25 °C | $V_{LA,LB}$ = 2.1 V (rms)<br>$V_{LA,LB}$ = 0.3 V (rms) | - | 1.4 | - | kΩ |
| $R_{LALB}$ [3][4][5][6] | Configured for antenna input with 69 pF capacitance. Test frequency = 13.56 MHz; $T_{amb}$ = 25 °C | $V_{LA,LB}$ = 2.6 V (rms) | - | 1.3 | - | kΩ |

[1] For the MOA8 delivery form, following values for $T_{amb}$ do apply: $T_{amb}$ = -25 °C to 85 °C
[2] Typical values are only referenced for information. They are subject to change without notice
[3] $C_{LALB}$ and $C_{LALB}$ values stated here assume a parallel RC equivalent circuit for the chip
[4] The value stated here was measured at estimated start of chip operation
[5] Measured with sine wave at $L_A$, $L_B$
[6] Parameter is valid in contacless ISO/IEC 14443 compliant operation only

**Table 17. Non-Volatile memory timing characteristics**

*$V_{CC}$ = 1 V to 1.98 V; $V_{SS}$ = 0 V; $T_{amb}$ = -40 °C to 105 °C, unless otherwise specified* [1]

| Symbol | Parameter | Conditions | Min | Typ[2] | Max | Unit |
|---|---|---|---|---|---|---|
| $t_{EEP}$ | FLASH erase + program time | - | - | - | 2.3 | ms |
| $t_{EEE}$ | FLASH erase time | - | - | - | 0.9 | ms |
| $t_{EEW}$ | FLASH program time | - | - | - | 1.4 | ms |
| $t_{EER}$ | FLASH data retention time | $T_{amb}$ = 55 °C | 25 | - | - | years |
| $N_{EEC}$ | FLASH endurance (maximum number of programming cycles applied to the whole memory block performed by NXP static and dynamic wear leveling algorithm) | | $20 \times 10^6$ | $100 \times 10^6$ | - | cycles |

[1] For the MOA8 delivery form, following values for $T_{amb}$ do apply: $T_{amb}$ = -25 °C to 85 °C
[2] Typical values are only referenced for information. They are subject to change without notice

# 10 Package outline

MF3E(H)x3 is delivered in two main form factors, the sawn 75 µm wafer on FFC and the contactless smartcard module package MOA8.

### Sawn wafer on FFC delivery

MF3E(H)x3 is offered in form of a 12-inch wafer delivery (sawn wafer, 75 µm thickness, on film frame carrier; electronic fail die marking according to SECSII format). With this delivery type, four pins are available for the contactless smartcard or contactless tag manufacturing.

A detailed description of the delivery type including pad coordinates is available inside the “Wafer and Delivery Specification”, [2] .

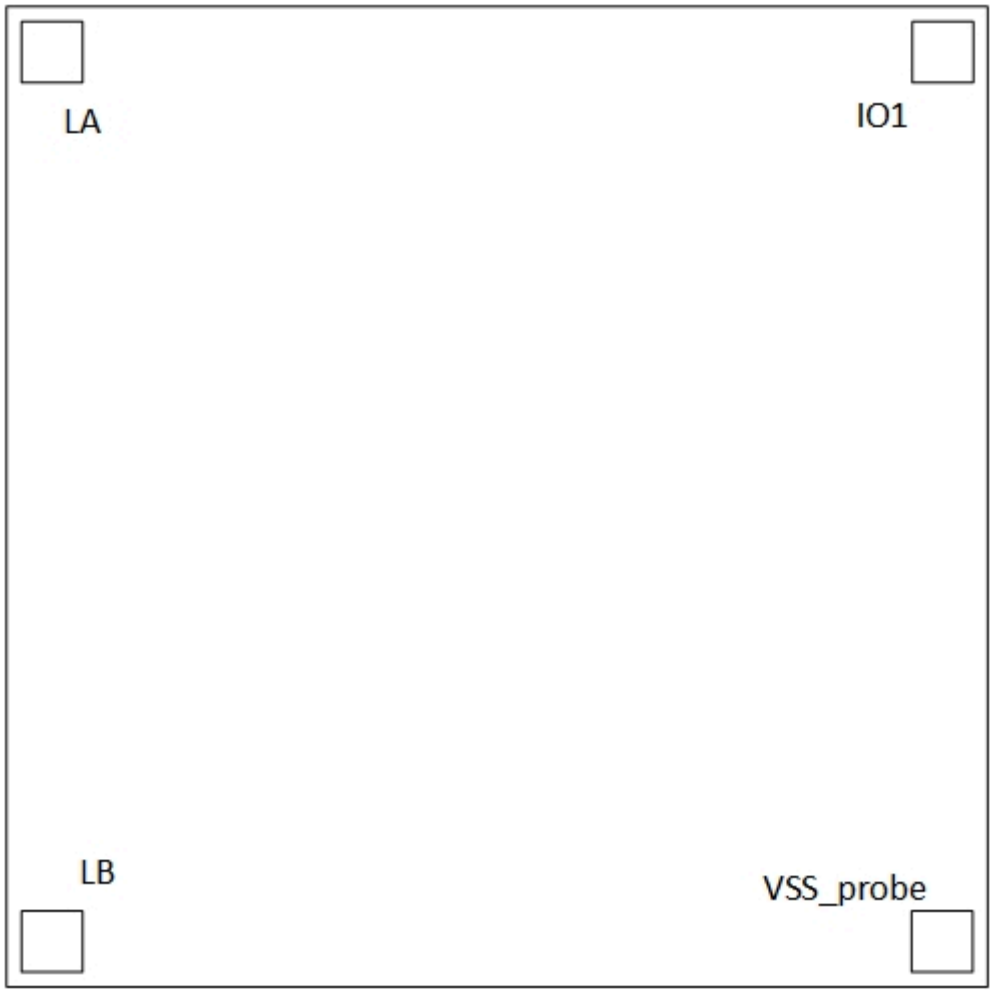


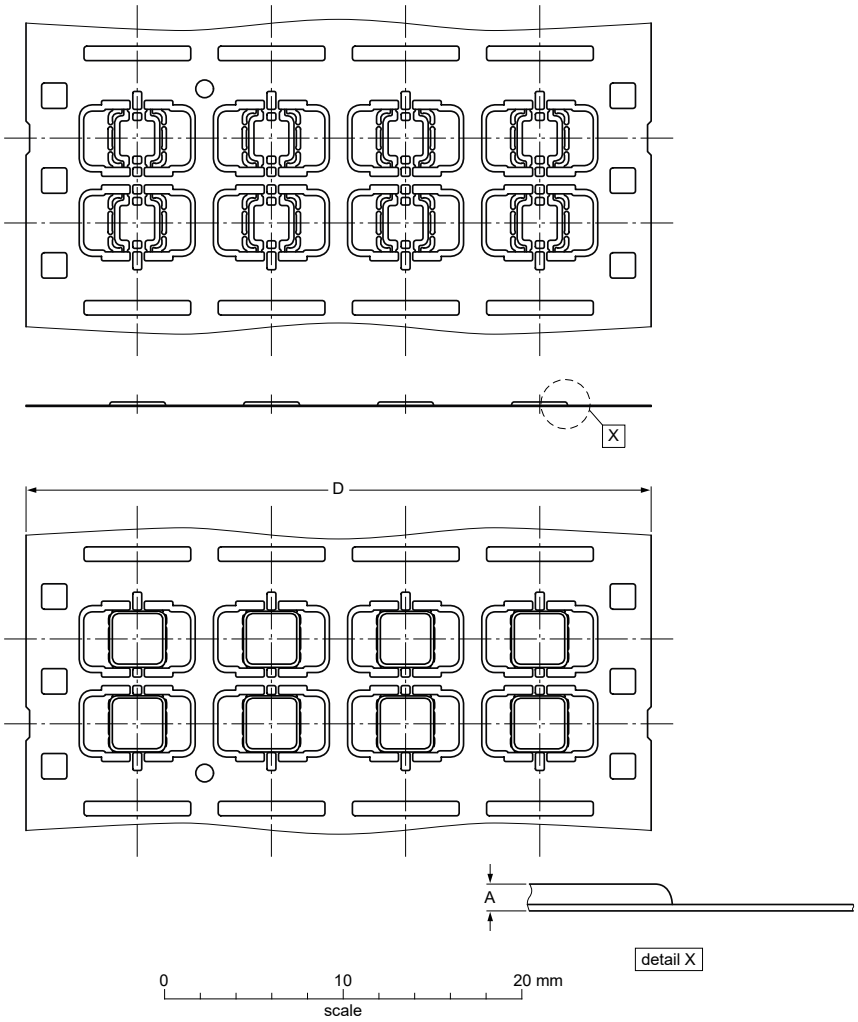

**Figure 3. MF3E(H)x3 package outline for bumped sawn wafer on FFC delivery**

## MOA8 delivery

MF3E(H)x3 is offered in form of MOA8 contacless smartcard IC modules.

**Table 18. MF3E(H)x3 package outline for MOA8 delivery**

**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 4. Package outline SOT500-4 (MOA8)**

# 11 Abbreviations

**Table 19. 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 |
| ECC | Elliptic Curve Cryptography |
| ECDH | Elliptic Curve Diffie Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| 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 *MF3E(H)x3 MIFARE DUOX Product data sheet*, document number: DS9744**[1].
[2] Data sheet Addendum *MF3E(H)x3 Wafer specification*, document number: AD9747**.

1 ** ... NXP document version number

# 13 Revision history

**Table 20. Revision history**

| Document ID | Release date | Description |
|---|---|---|
| MF3E(H)x3_SDS v. 1.0 | 12 November 2024 | • Initial version |

# Legal information

## 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 https://www.nxp.com.

## Definitions

**Draft** — A draft status on a document indicates that 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 in a draft version of a document 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.

## 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 https://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.

**Suitability for use in non-automotive qualified products** — Unless this document 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.

**HTML publications** — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

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

**Security** — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

**NXP B.V.** — NXP B.V. is not an operating company and it does not distribute or sell products.

## Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

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

**DESFire** — is a trademark of NXP B.V.

**MIFARE** — is a trademark of NXP B.V.

# Tables

# Figures

# Contents