

# AN14218

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

Rev. 1.0 — 6 November 2024  
975310

Application note  
CONFIDENTIAL

### Document information

Information	Content
Keywords	MIFARE DUOX, MIFARE DESFire EV3, MIFARE, compatibility, comparison
Abstract	In this document the MIFARE DUOX product is compared to MIFARE DESFire EV3 and their compatibility is analyzed. Their differences on command and feature level are shown.



## 1 Introduction

MIFARE DUOX is a new addition to the MIFARE product family of NXP, carrying over parts of the functionality from MIFARE DESFire EV3, but adding a lot of new functionalities and innovations on top.

In this document the detailed comparison of the product functionalities from MIFARE DUOX versus MIFARE DESFire EV3 is presented and all different and newly added functionalities are outlined.

### 1.1 About the content of this document

This document addresses developers, project leaders and system integrators who have a general technical understanding or are already familiar with the MIFARE DESFire product family. Knowledge of the reader terminal infrastructure or complete service infrastructure is good to have.

**Note:** This document does not cover the general working principle of the MIFARE DUOX, but only gives a high-level functional overview and comparison to the MIFARE DESFire EV3 product. Read Ref [\[1\]](#) in order to get the full overview and description of MIFARE DUOX and the associated command set.

This application note is a supplementary document for implementations using the MIFARE DUOX. Should there be any confusion, please check the MIFARE DUOX data sheet Ref [\[1\]](#).

### 1.2 Structure of this document

This document describes the relevant information for being able to compare the products MIFARE DUOX and MIFARE DESFire EV3, starting with an Introduction.

In [Section 2.1](#), the key differences of the products will be outlined and supported commands are listed.

In the following [Section 3](#), all key management relevant infos are discussed.

[Section 4](#) highlights configuration settings of the IC.

Application management and application level functionality are discussed in [Section 5](#).

Functionality related to file management is compared in [Section 6](#).

The advanced and new features are finally discussed in [Section 7](#).

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

## 2 Key differences

This section highlights the most important differences between MIFARE DESFire EV3 and MIFARE DUOX. Starting with an overview of the feature differences and followed by the differences of available and supported commands.

### 2.1 Key and feature differences

Table 1. Key Differences between MIFARE DUOX and MIFARE DESFire EV3

Item	MIFARE DESFire EV3	MIFARE DUOX
ECC asymmetric cryptography and PKI support	Not Supported	New Feature
Transaction Signature feature	Not Supported	New Feature
Support for EV-Charging functionality as per VDE-DKE AR-E 2532-100	Not Supported	New Feature
D40 and EV1 secure messaging (using Authenticate, AuthenticateISO and AuthenticateAES commands)	Supported	Dropped
TDEA	Supported	Dropped
VCA	Supported	Dropped, except Proximity Check

### 2.2 Supported commands

Table 2. Supported Commands for MIFARE DUOX and MIFARE DESFire EV3

Command Name	Command Code	MIFARE DESFire EV3	MIFARE DUOX
Authenticate	0x0A	Yes	No
AuthenticateISO	0x1A	Yes	No
AuthenticateAES	0xAA	Yes	No
ISOGeneralAuthenticate	0x87	No	Yes, new command
ISOInternalAuthenticate	0x88	Yes, only symmetric	Yes
AuthenticateEV2First	0x71	Yes	Yes
AuthenticateEV2NonFirst	0x77	Yes	Yes
FreeMem	0x6E	Yes	Yes
Format	0xFC	Yes	Yes
SetConfiguration	0x5C	Yes	Yes but differences
GetVersion	0x60	Yes	Yes
GetCardUID	0x51	Yes	Yes
ChangeKey	0xC4	Yes	Yes
ChangeKeyEV2	0xC6	Yes	Yes
InitializeKeySet	0x56	Yes	Yes
FinalizeKeySet	0x57	Yes	Yes
RollKeySet	0x55	Yes	Yes

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

Table 2. Supported Commands for MIFARE DUOX and MIFARE DESFire EV3...continued

Command Name	Command Code	MIFARE DESFire EV3	MIFARE DUOX
GetKeySettings	0x45	Yes	Yes
ChangeKeySettings	0x54	Yes	Yes
ManageKeyPair	0x46	No	Yes, new command
ManageCARootKey	0x48	No	Yes, new command
ExportKey	0x47	No	Yes, new command
GetKeyVersion	0x64	Yes	Yes
CreateApplication	0xCA	Yes	Yes
DeleteApplication	0xDA	Yes	Yes
CreateDelegatedApplication	0xC9	Yes	Yes
SelectApplication	0x5A	Yes	Yes
GetApplicationIDs	0x6A	Yes	Yes
GetDFNames	0x6D	Yes	Yes
GetDelegatedInfo	0x69	Yes	Yes
CreateStdDataFile	0xCD	Yes	Yes, with additions
CreateBackupDataFile	0xCB	Yes	Yes, with additions
CreateValueFile	0xCC	Yes	Yes
CreateLinearRecordFile	0xC1	Yes	Yes
CreateCyclicRecordFile	0xC0	Yes	Yes
CreateTransactionMACFile	0xCE	Yes	Yes
DeleteFile	0xDF	Yes	Yes
GetFileIDs	0x6F	Yes	Yes
GetISOFileIDs	0x61	Yes	Yes
GetFileSettings	0xF5	Yes	Yes
GetFileCounters	0xF6	Yes	Yes
ChangeFileSettings	0x5F	Yes	Yes
ReadData	0xBD / 0xAD	Yes	Yes
WriteData	0x3D / 0x8D	Yes	Yes, with additions
GetValue	0x6C	Yes	Yes
Credit	0x0C	Yes	Yes
Debit	0xDC	Yes	Yes
LimitedCredit	0x1C	Yes	Yes
ReadRecords	0xBB / 0xAB	Yes	Yes
WriteRecord	0x3B / 0x8B	Yes	Yes
UpdateRecord	0xDB / 0xBA	Yes	Yes
ClearRecordFile	0xEB	Yes	Yes
CommitTransaction	0xC7	Yes	Yes

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

Table 2. Supported Commands for MIFARE DUOX and MIFARE DESFire EV3...continued

Command Name	Command Code	MIFARE DESFire EV3	MIFARE DUOX
AbortTransaction	0xA7	Yes	Yes
CommitReaderID	0xC8	Yes	Yes
ISOSelectFile	0xA4	Yes	Yes
ISOReadBinary	0xB0	Yes	Yes
ISOUpdateBinary	0xD6	Yes	Yes
ISOReadRecord	0xB2	Yes	Yes
ISOAppendRecord	0xE2	Yes	Yes
ISOGetChallenge	0x84	Yes	Yes
ISOExternalAuthenticate	0x82	Yes	Yes
ISOSelectFile (VC)	0xA4	Yes	Yes
ISOExternalAuthenticate (VC)	0x82	Yes	Yes
PreparePC	0xF0	Yes	Yes
ProximityCheck	0xF2	Yes	Yes
VerifyPC	0xFD	Yes	Yes
Read_Sig	0x3C	Yes	Yes
VDE_ReadData	0x02	No	Yes, new command
VDE_WriteData	0x01	No	Yes, new command
VDE_ECDSASign	0x03	No	Yes, new command

**Note:** Some commands have changed, e.g. the file management commands for StdDataFiles and BackupDataFiles are also available at PICC level for certificate management.

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

### 3 Keys, key management and certificates

This chapter compares the differences in the available keys and key management scenarios between MIFARE DUOX and MIFARE DESFire EV3.

#### 3.1 PICC keys

Table 3. Symmetric PICC level Keys

Key	Key Number	MIFARE DESFire EV3	MIFARE DUOX	Comment
PICC Master Key	0x00	Supported	Supported	Same functionality
Originality Keys	0x01, 0x02, 0x03, 0x04	Supported	Supported	Same functionality Keys for the Originality Check feature, written into the IC during manufacturing, used by TagInfo App
DAM Keys	0x10, 0x11, 0x12	Supported	Supported	Same functionality Keys for the delegated application management
NXP DAM Keys	0x18, 0x19, 0x1A	Supported	Supported	Same functionality Keys for the delegated application management by NXP
VC configuration and PC key	0x20, 0x21	Supported	Supported	Same functionality Keys for the virtual card and proximity check features
VC ENC and MAC keys	0x22, 0x23	Supported	Not Supported	Removed, as VCA is not supported anymore
Application Default Key	-	Supported	Supported	Same functionality Default key value with which all application keys are initialized, once a new application is created on PICC level.

Table 4. Asymmetric PICC level keys

Key	Key Number	MIFARE DESFire EV3	MIFARE DUOX	Comment
Priv.PICC	0x00	Not Supported	Supported	PICC functionality key pair. Pub.PICC is trusted via the Cert.PICC
Priv.Orig	0x01	Not Supported	Supported	Originality Check key pair. Pub.Orig is trusted via Cert.Orig

Table 5. PICC level certificates

Certificate	File Number	ISOFileID	MIFARE DESFire EV3	MIFARE DUOX	Comment
Cert.PICC	0x00	0xEF00	Not Supported	Supported	NXP PICC Certificate
Cert.Orig	0x01	0xEF01	Not Supported	Supported	Trust-provisioned file at the PICC level holding the Originality Check certificate

### 3.2 Application keys

The application key set concept is the same in MIFARE DUOX as it is already well-known from MIFARE DESFire EV3. Additionally to MIFARE DESFire EV3, customized certificates can be stored in StdDataFiles or BackupDataFiles, and up to 5 ECCPrivateKeys can be stored.

One application on MIFARE DUOX can have up to 16 keysets, with each keyset holding up to 14 symmetric keys. The number of keysets and keys per keyset can be defined during application creation. At a time, only one keyset is active. There is a process defined to role from one to the other keyset dynamically.

Multiple application keysets are available for standard applications, created with the CreateApplication command, and also available for delegated applications, created with the CreateDelegatedApplication command.

The default key value for applications keys is taken from the Application Default Key which is available on PICC level. This default key value is used for initializing all application keys with the same value, once a new application is created with the CreateApplication command.

When creating a new delegated application with the CreateDelegatedApplication command, the default key value for the applications keys is defined directly in the command, but not coming from the Application Default Key from PICC level.

Keyset rolling can be used inside an application on MIFARE DUOX and MIFARE DESFire EV3 in the same way. Keyset rolling is needed for switching from one currently used keyset, to another keyset in a very fast and secure way. This keyset rolling can be done securely in the field, if the keyset personalization process has been completed during the application personalization process.



## 4 Configuration and settings on PICC level

### 4.1 PICC level memory size

The complete user memory is available for application and file creation (including overhead). All PICC level keys and configuration data are located outside the user memory.

Table 6. Available user memory on different MIFARE DESFire versions

Product type	MIFARE DESFire EV3	MIFARE DUOX
2 kB	2560 bytes	2560 bytes
4 kB	5120 bytes	5120 bytes
8 kB	8192 bytes	8192 bytes
16 kB	16384 bytes	16384 bytes

### 4.2 Configuration settings on PICC level

MIFARE DUOX offers the SetConfiguration command for configuring features on PICC as well as on Application level. Most options of this command are the same as already known from MIFARE DESFire EV3, but some more functionality was added additionally.

Also, all VCA (Virtual card architecture) functionality was removed.

Table 7. SetConfiguration command options

Option	Bit Index and Meaning	MIFARE DESFire EV3	MIFARE DUOX	Description
0x00	Bit 6 - 4-byte NUID configuration	Supported	Not supported	4-byte NUID was supported for MIFARE Classic compatibility, not supported in MIFARE DUOX
	Bit 5 - Random ID configuration	Supported	Supported	Configuring the format of the Random ID (ISO compliant or legacy Random ID format).
	Bit 4 - Error code binding	Supported	Not supported	Same functionality
	Bit 3 - AuthVCMandatory	Supported	not supported	VCA was removed
	Bit 2 - PCMandatory	Supported	not supported	VCA was removed
	Bit 1 - Random ID enablement	Supported	Supported	Same functionality
	Bit 0 - Format disabling	Supported	Supported	Same functionality
0x01	Updating the PICCAppDefaultKey	Supported	Supported	Same functionality
0x02	Setting a user-defined ATS	Supported	Supported	Same functionality
0x03	Setting a user-defined SAK	Supported	Supported	Same functionality



## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

Table 7. SetConfiguration command options...continued

Option	Bit Index and Meaning	MIFARE DESFire EV3	MIFARE DUOX	Description
0x04	Secure Messaging configuration as on DESFire EV3	Supported	Not supported	D40 and EV1 secure messaging have been removed as whole
	Bit 22 - ISOSelect fast UID retrieval	Not supported	Supported	New feature
	Bit 21 - Enable free access over I <sup>2</sup> C	Not supported	Supported	New feature
	Bit 20 - Enable EV Charging unilateral authentication and related commands	Not supported	Supported	New feature
	Bit 19 - ISOSelect integrated ECC authentication	Not supported	Supported	New feature
	Bit 18 - EV2 secure messaging configuration for StdDataFiles	Not supported	Supported	New feature
	Bits 8-15 - Targeted Curve if bit 19 is enabled	Not supported	Supported	New feature
	Bit 0-7 - UID encryption key if bit 22 is set	Not supported	Supported	New feature
0x05	71...64 - VCTID Override	Supported	Supported	Same functionality
	55...48 - PDCap 1.2	Supported	Supported	Same functionality
	39...32 - PDCap 2.2	Supported	Supported	Same functionality
	15...8 - PDCap 2.5	Supported	Supported	Same functionality
	7...0 - PDCap 2.6	Supported	Supported	Same functionality
0x06	VCIID configuration	Supported	Supported	VCIID reconfiguration Changing the default ISO DF Name for MIFARE DESFire to a customized one.
0x0C	ATQA configuration	Supported	Supported	User ATQA Defining a customized ATQA value.
0x0F	NFC Management	Not supported	Supported	New feature - Management of the NFC interface including crypto protocol and specifications
0x10	I2C Management	Not supported	Supported	New feature - Management of the I2C interface including crypto protocol, address and specifications
0x11	GPIO Management	Not supported	Supported	New feature - Configuration of the GPIO pins: I/O configuration, access conditions power harvesting options and current configuration. Detailed parameters can be found in the datasheet.

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

Table 7. SetConfiguration command options...continued

Option	Bit Index and Meaning	MIFARE DESFire EV3	MIFARE DUOX	Description
0x15	Crypto API Management	Not supported	Supported	New feature - Defines the access conditions of the CryptoRequest command
0x16	Authentication Counter and Limit Configuration	Not supported	Supported	New feature - Enable and set AuthCtr for AuthenticateEV2 First
0x17	HALT and Wake-up Configuration	Not supported	Supported	New feature - Configure GPIO behaviour when in HALT state and under wakeup conditions
0xFF	Lock Configurations	Not supported	Supported	New feature - Lock configurations items to not be changeable again

### 4.3 Retrieving the Card UID

The GetCardUID command which is already well-known from MIFARE DESFire EV3 (see [1]) is existing in the same way also on MIFARE DUOX.

Additionally, MIFARE DUOX offers the option to retrieve the UID in encrypted format through the FCI returned to the ISOSelectFiles command. That way, an additional authentication with a static, non-diversified key is omitted.

### 4.4 Application management

#### 4.4.1 Application creation

On MIFARE DUOX, two ways for application creation are existing - the CreateApplication command for creating a standard application by the card owner, or CreateDelegatedApplication command for creating a delegated application by a third party application provider.

The two mentioned commands have the same purpose and functionality as they already had on MIFARE DESFire EV3. (see [1])

#### 4.4.2 Application deletion

The Application deletion functionality on MIFARE DUOX works the same as on MIFARE DESFire EV3. (see [1])

## 5 Application level functionality

### 5.1 Application configuration

On application level, MIFARE DUOX offers the same configuration options and settings as were already available on MIFARE DESFire EV3. (see [\[1\]](#))

### 5.2 File types and their configurability

MIFARE DUOX offers the six already well-known file types which were already available on MIFARE DESFire EV3 and previous product generations. (see [\[1\]](#))

The file access rights and, also the possibility of having multiple file access right sets per file, remain in the same already known way, except that file access rights can now also be granted via asymmetric authentications, in the same way as for symmetric authentication.

#### 5.2.1 File settings and options

There are no changes in the applicable file settings and options in MIFARE DUOX compared to MIFARE DESFire EV3. (see [\[1\]](#))

## 6 File level functionality

All file level commands which are intended to execute data manipulation, are already well-known from the older MIFARE DESFire versions. On MIFARE DUOX, the same commands can be utilized. (see [1])

For data exchange, MIFARE DUOX supports a frame size of up to 256 bytes. The default frame size equals 64 bytes, but can be extended or reduced by using the SetConfiguration command and modifying the relevant T0 byte inside the ATS.

The MIFARE DUOX also supports two different chaining modes: ISO/IEC 14443-4 chaining or native chaining (using 0xAF).

### 6.1 File access rights

As already well-known from MIFARE DESFire EV3 (see [1]), the file access rights management is implemented in the same way for MIFARE DUOX with a few additions necessary for the addition of asymmetric keys.

Every file can be associated with four basic access rights:

- Read
- Write
- ReadWrite
- ChangeConfiguration

These four access rights form one so called access condition set. Every file can be optionally equipped with up to eight access condition sets. Each set is containing three access conditions: one for each of Read, Write and ReadWrite. The first set is called the mandatory set as it needs to be always present for every file and is already defined during file creation. The ChangeConfiguration access right is only available in the first, mandatory access condition set as it can only be available once for each file.

#### File Access Rights for Secure Dynamic Messaging

For MIFARE DUOX the access rights and access conditions related to the SDM feature are existing in the same way as already known from MIFARE DESFire EV3, however they have been extended by one access right for the newly added SDMSIG

Once SDM is enabled for a Standard Data File, these additional four access rights can be defined:

- SDM Meta Read
- SDM File Read
- SDM File Read 2 (ECC)
- SDM Counter Retrieval

The SDM-related access rights can only be set if SDM was enabled for the Standard Data File during file creation, and if SDM is activated for the file. For all four mentioned access rights, an available application key number or the FREE (0xE) or NEVER (0xF) access right can be set. (0x0E is not an option for SDMFileRead and SDMFileRead2)

The purpose / functionality of the four mentioned access rights is the following:

- SDM Meta Read - Encryption of the PICCData (metadata) using the specified application key number
- SDM File Read - Encryption of the mirrored file data using the specified application key number
- SDM File Read 2 - Generation of the SDMSIG
- SDM Counter Retrieval - Possibility to retrieve the associated SDMReadCtr using the GetFileCounters command after an authentication with the specified application key number

## 7 Advanced and new features

All advanced and new features that are highlighted in this chapter are valid for the MIFARE DUOX product.

### 7.1 Virtual card

The virtual card feature and concept was removed on MIFARE DUOX except for the Proximity Check, that was previously part of the virtual card architecture. On MIFARE DUOX the Proximity Check is considered a standalone feature.

The functionality of the Proximity Check has not changed compared to MIFARE DESFire EV3.

### 7.2 Originality check

The originality check feature on MIFARE DUOX is fundamentally different from what was used before. As MIFARE DUOX has support for asymmetric ECC keys, a card-unilateral authentication with the Originality Check key pair (Priv.Orig, Pub.Orig) is used.

Always one batch of MIFARE DUOX (check batch number in GetVersion response) shares the same Originality Check key pair to reduce privacy implications.

### 7.3 Transaction timer

The Transaction Timer was introduced in MIFARE DESFire EV3 and is available on MIFARE DUOX in the same way.

### 7.4 Secure dynamic messaging

The Secure Dynamic Messaging (SDM) feature was introduced in MIFARE DESFire EV3 and is available on MIFARE DUOX in the same way.

### 7.5 Asymmetric authentication and certificate handling

One of the main new features of MIFARE DUOX is the asymmetric authentication and required key- and certificate handling functionality.

Table 8. Asymmetric crypto functionalities

Command	Comment
ManageKeyPair	Command used to manage, create or import an ECC key or key pair
ManageCARootKey	Command used to create or update a public key entry for storing a CARootKey
ExportKey	Exports the public key value of a CARootKey
ISOGeneralAuthenticate	Initiates an asymmetric mutual or reader-unilateral authentication.
ISOGeneralAuthenticateFinal	Second part of the ISOGeneralAuthenticate procedure. Can be used to finalize the Authentication initiated with ISOGeneralAuthenticate or ISOSelectFile
ISOInternalAuthenticate	Asymmetric card-unilateral authentication used for the Originality Check feature
CryptoRequest	Executes a ECC sign operation over various input options

## 7.6 EV charging according VDE-DKE

The EV Charging functionality, as required by VDE-AR-E 2532-100, is supported on MIFARE DUOX by either using existing commands or wrapping of existing functionality on the VDE-AR-E 2532-100 APDU structures.

Table 9. VDE-AR-E 2532-100 commands

VDE command	Command	Comment
SELECT	ISOSelectFile	Used for selecting the application, VDE defines a subset of ISOSelectFile.
ReadData	VDE_ReadData	Used for reading out the certificate and potentially additional card holder data.
ECDSASign	VDE_ECDSASign	Used for executing the unilateral card authentication.
WriteData	VDE_WriteData	Used for writing additional information to the additional file, e.g. during in the field enrolling.

The support of the above mentioned new commands (VDE\_ReadData, VDE\_ECDSASign and VDE\_WriteData) needs to be enabled using the SetConfiguration command with parameter 0x04 for a given application. In other applications, those commands are rejected.

## 7.7 GPIO and I<sup>2</sup>C

MIFARE DUOX offers two configurable GPIO pins that can be used for various purposes:

- I<sup>2</sup>C-follower Interface for wired communication coming from a peripheral host
- NFC power harvesting
- Authentication notification
- NFC field detection
- General purpose I/O

All GPIO related functionality can be configured via the SetConfiguration commands targeting the newly added parameters 0x10 (I2C) and 0x11 (GPIO). Additional to this, two new commands have been added:

Table 10. GPIO commands

Command	Comment
Manage GPIO	Used to configure the GPIO functionality at runtime, initiate the NFC Pause, or start power harvesting
ReadGPIO	Returns the status of GPIO1 and GPIO2

### NFC Pause:

The NFC Pause is used to transfer the control from an NFC host to an I<sup>2</sup>C host. The NFC Pause can be enabled via the ManageGPIO command, as well as implicitly via the ISOReadBinary or ReadData commands. The latter one allows to mirror data acquired over the I<sup>2</sup>C interface (e.g. a sensor input) at runtime into a file, which is then returned back over the NFC interface as response to the ReadData or ISOReadBinary command.



## 8 References

- [1] Product data sheet - MIFARE DESFire EV3 contactless multi-application IC, document number DS4870xx, available in <https://www.nxp.com/mynxp/secure-files>



9 Revision history

Table 11. Revision history

Document ID	Release date	Description
AN14218 v.1.0	06 November 2024	• initial version

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

## Legal information

## 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.

## 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.

**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.

**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](mailto: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 DUOX feature and functionality comparison to other MIFARE DESFire products

MIFARE — is a trademark of NXP B.V.

Provided under NDA only  
 COMPANY CONFIDENTIAL - Personal copy for:  
 Sergii Salata  
 Quantag IT Solutions GmbH  
 Do not copy, share or reproduce  
 3f8f002a-b609-4502-8bcd-78d68fdfa6df

## MIFARE DUOX feature and functionality comparison to other MIFARE DESFire products

## Tables

Tab. 1.	Key Differences between MIFARE DUOX and MIFARE DESFire EV3 .....	3	Tab. 6.	Available user memory on different MIFARE DESFire versions .....	8
Tab. 2.	Supported Commands for MIFARE DUOX and MIFARE DESFire EV3 .....	3	Tab. 7.	SetConfiguration command options .....	8
Tab. 3.	Symmetric PICC level Keys .....	6	Tab. 8.	Asymmetric crypto functionalities .....	13
Tab. 4.	Asymmetric PICC level keys .....	6	Tab. 9.	VDE-AR-E 2532-100 commands .....	14
Tab. 5.	PICC level certificates .....	6	Tab. 10.	GPIO commands .....	14
			Tab. 11.	Revision history .....	16

## Contents

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
1.1	About the content of this document .....	2
1.2	Structure of this document .....	2
<b>2</b>	<b>Key differences .....</b>	<b>3</b>
2.1	Key and feature differences .....	3
2.2	Supported commands .....	3
<b>3</b>	<b>Keys, key management and certificates .....</b>	<b>6</b>
3.1	PICC keys .....	6
3.2	Application keys .....	7
<b>4</b>	<b>Configuration and settings on PICC level .....</b>	<b>8</b>
4.1	PICC level memory size .....	8
4.2	Configuration settings on PICC level .....	8
4.3	Retrieving the Card UID .....	10
4.4	Application management .....	10
4.4.1	Application creation .....	10
4.4.2	Application deletion .....	10
<b>5</b>	<b>Application level functionality .....</b>	<b>11</b>
5.1	Application configuration .....	11
5.2	File types and their configurability .....	11
5.2.1	File settings and options .....	11
<b>6</b>	<b>File level functionality .....</b>	<b>12</b>
6.1	File access rights .....	12
<b>7</b>	<b>Advanced and new features .....</b>	<b>13</b>
7.1	Virtual card .....	13
7.2	Originality check .....	13
7.3	Transaction timer .....	13
7.4	Secure dynamic messaging .....	13
7.5	Asymmetric authentication and certificate handling .....	13
7.6	EV charging according VDE-DKE .....	14
7.7	GPIO and I2C .....	14
<b>8</b>	<b>References .....</b>	<b>15</b>
<b>9</b>	<b>Revision history .....</b>	<b>16</b>
	<b>Legal information .....</b>	<b>17</b>

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

© 2024 NXP B.V.

All rights reserved.

For more information, please visit: <https://www.nxp.com>

Date of release: 6 November 2024  
Document identifier: AN14217  
Document number: 975310