AN12752

MIFARE DESFire EV3 feature and functionality comparison to other MIFARE DESFire products

Rev. 1.2 — 30 September 2020 Application note
575612 COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE DESFire EV3, MIFARE DESFire EV2, MIFARE DESFire EV1, MIFARE, compatibility, comparison
Abstract	In this document several MIFARE DESFire products, MIFARE DESFire EV1, EV2, EV3 are compared and their compatibility is analyzed. Their differences on command and feature level are shown.

Revision history

Revision history

Rev	Date	Description
1.2	20200930	DocStore document number of MIFARE DESFire EV3 data sheet corrected in Section 8
1.1	20200528	Renamed the descriptive title of the document and removed specific sections. Security status changed to Company Public.
1.0	20200225	Initial version of the document

1 Introduction

MIFARE DESFire EV3 is the successor of MIFARE DESFire EV2, [2].

Additionally, MIFARE DESFire EV3 is the latest member of the MIFARE DESFire family. The MIFARE DESFire family offers products which are based on a flexible, secure and scalable platform, offering continuous innovation and the important aspects security as well as privacy. Extending the MIFARE DESFire EV2 which is a very powerful, flexible and complex platform for dynamic multi-application use cases, the MIFARE DESFire EV3 offers even more advanced hardware and software implementation on a brand new IC.

MIFARE DESFire EV3 is covering all well-known commands and features from MIFARE DESFire EV2, plus adding some new features like Transaction Timer and Secure Dynamic Messaging on top [1].

In this document the detailed comparison of the products MIFARE DESFire EV3, MIFARE DESFire EV2 and EV1 is presented and all different 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.

Please note that this document does not cover the general working principle of the MIFARE DESFire EV3, but only gives a high-level functional overview and comparison to the MIFARE DESFire EV2 product. Read Ref [1] in order to get the full overview and description of MIFARE DESFire EV3 and the associated command set.

This application note is a supplementary document for implementations using the MIFARE DESFire EV3. Should there be any confusion, please check the MIFARE DESFire EV3 data sheet Ref [1].

1.2 Structure of this document

This document describes the relevant information for being able to compare the products MIFARE DESFire EV3, MIFARE DESFire EV1 / EV2, starting with an Introduction.

In chapter Section 2.1, the key differences of the products will be outlined and supported commands are listed.

In the following chapter Section 3, all key management relevant infos are discussed.

Chapter 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.

2 Key Differences

This section highlights the most important differences between MIFARE DESFire EV1, MIFARE DESFire EV2 and its successor MIFARE DESFire EV3. 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 DESFire EV2, MIFARE DESFire EV3

Item	MIFARE DESFire EV2	MIFARE DESFire EV3
Application deletion using the DAMMAC	Not Supported	New Feature See Section 4.4.2
Secure Dynamic Messaging and Mirroring	Not Supported	New Feature See Section 7.5
Transaction Timer	Not Supported	New Feature See Section 7.4

2.2 Supported commands

Table 2. Supported Commands for MIFARE DESFire EV1, MIFARE DESFire EV2 and MIFARE DESFire EV3

Command Name	Command Code	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3
Authenticate	0x0A	Yes	Yes	Yes
AuthenticateISO	0x1A	Yes	Yes	Yes
AuthenticateAES	0xAA	Yes	Yes	Yes
AuthenticateEV2First	0x71	No	Yes	Yes
AuthenticateEV2NonFirst	0x77	No	Yes	Yes
FreeMem	0x6E	Yes	Yes	Yes
Format	0xFC	Yes	Yes	Yes
SetConfiguration	0x5C	Yes	Yes	Yes but differences
GetVersion	0x60	Yes	Yes	Yes
GetCardUID	0x51	Yes	Yes	Yes but differences
ChangeKey	0xC4	Yes	Yes	Yes
ChangeKeyEV2	0xC6	No	Yes	Yes
InitializeKeySet	0x56	No	Yes	Yes
FinalizeKeySet	0x57	No	Yes	Yes
RollKeySet	0x55	No	Yes	Yes
GetKeySettings	0x45	Yes	Yes	Yes
ChangeKeySettings	0x54	Yes	Yes	Yes
GetKeyVersion	0x64	Yes	Yes	Yes

Table 2. Supported Commands for MIFARE DESFire EV1, MIFARE DESFire EV2 and MIFARE DESFire EV3*...continued*

Command Name	Command Code	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3
CreateApplication	0xCA	Yes	Yes	Yes but differences in KeySett3 parameter
DeleteApplication	0xDA	Yes	Yes	Yes but differences in how a delegated application can be deleted
CreateDelegatedApplication	0xC9	No	Yes	Yes but differences in KeySett3 parameter
SelectApplication	0x5A	Yes	Yes	Yes
GetApplicationIDs	0x6A	Yes	Yes	Yes
GetDFNames	0x6D	No	Yes	Yes
GetDelegatedInfo	0x69	No	Yes	Yes
CreateStdDataFile	0xCD	Yes	Yes	Yes but differences in FileOption
CreateBackupDataFile	0xCB	Yes	Yes	Yes but differences in FileOption
CreateValueFile	0xCC	Yes	Yes	Yes but differences in FileOption
CreateLinearRecordFile	0xC1	Yes	Yes	Yes
CreateCyclicRecordFile	0xC0	Yes	Yes	Yes
CreateTransactionMACFile	0xCE	No	Yes	Yes
DeleteFile	0xDF	Yes	Yes	Yes
GetFileIDs	0x6F	Yes	Yes	Yes
GetISOFileIDs	0x61	Yes	Yes	Yes
GetFileSettings	0xF5	Yes	Yes	Yes but differences in response for Standard, Backup and Value File
GetFileCounters	0xF6	Yes	No	Yes, new command
ChangeFileSettings	0x5F	Yes	Yes	Yes, but differences in FileOption and new additional parameters
ReadData	0xBD / 0xAD	Yes	Yes	Yes
WriteData	0x3D / 0x8D	Yes	Yes	Yes
GetValue	0x6C	Yes	Yes	Yes
Credit	0x0C	Yes	Yes	Yes
Debit	0xDC	Yes	Yes	Yes
LimitedCredit	0x1C	Yes	Yes	Yes
ReadRecords	0xBB / 0xAB	Yes	Yes	Yes
WriteRecord	0x3B / 0x8B	Yes	Yes	Yes

Table 2. Supported Commands for MIFARE DESFire EV1, MIFARE DESFire EV2 and MIFARE DESFire EV3*...continued*

Command Name	Command Code	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3
UpdateRecord	0xDB / 0xBA	Yes	Yes	Yes
ClearRecordFile	0xEB	Yes	Yes	Yes
CommitTransaction	0xC7	Yes	Yes	Yes
AbortTransaction	0xA7	Yes	Yes	Yes
CommitReaderID	0xC8	No	Yes	Yes
ISOSelectFile	0xA4	Yes	Yes	Yes
ISOReadBinary	0xB0	Yes	Yes	Yes
ISOUpdateBinary	0xD6	Yes	Yes	Yes
ISOReadRecord	0xB2	Yes	Yes	Yes
ISOAppendRecord	0xE2	Yes	Yes	Yes
ISOGetChallenge	0x84	Yes	Yes	Yes
ISOExternalAuthenticate	0x82	Yes	Yes	Yes
ISOInternalAuthenticate	0x88	Yes	Yes	Yes
ISOSelectFile (VC)	0xA4	No	Yes	Yes
ISOExternal Authenticate (VC)	0x82	No	Yes	Yes
PreparePC	0xF0	No	Yes	Yes but new response parameters depending on the Option byte
ProximityCheck	0xF2	No	Yes	Yes
VerifyPC	0xFD	No	Yes	Yes
Read_Sig	0x3C		Yes	Yes

3 Keys and key management

This chapter compares the differences in the available keys and key management scenarios between MIFARE DESFire EV2 and MIFARE DESFire EV3.

3.1 PICC keys

Table 3. PICC Keys

Key	Key Number	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3	Comment
PICC Master Key	0x00	Supported	Supported	Supported	Similar functionality
Originality Keys	0x01, 0x02, 0x03, 0x04	NOT Supported	Supported	Supported	Same functionality Keys for the Originality Check feature, written into the IC during manufacturing
DAM Keys	0x10, 0x11, 0x12	NOT Supported	Supported	Supported	Same functionality Keys for the delegated application management
NXP DAM Keys	0x18, 0x19, 0x1A	NOT Supported	NOT Supported	Supported	Keys for the delegated application management by NXP, through the AppXplorer with NXP as card issuer
VC and PC Keys	0x20, 0x21, 0x22, 0x23	NOT Supported	Supported	Supported	Same functionality Keys for the virtual card and proximity check features
Application Default Key	-	Supported	Supported	Supported	Same functionality Default key value with which all application keys are initialized, once a new application is created on PICC level.

3.2 Application keys

The application key set concept is the same in MIFARE DESFire EV3 as it is already well-known from MIFARE DESFire EV2.

One application on MIFARE DESFire EV3 can have up to 16 keysets, with each keyset holding up to 14 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. On MIFARE DESFire EV1 only one keyset is available, not multiple ones.

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 DESFire EV2 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.

Keyset rolling was not available on MIFARE DESFire EV1.

4 Configuration and settings on PICC level

4.1 PICC level memory size

The non-volatile flash-based memory, that is available for user data, is allocated in a page size of 256 bytes on MIFARE DESFire EV3. 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 4. Available User Memory on different MIFARE DESFire versions

Product type	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3	Comment
2 kB	2304 bytes	2560 bytes	2560 bytes	
4 kB	4864 bytes	5120 bytes	5120 bytes	
8 kB	7936 bytes	8192 bytes	8192 bytes	
16 kB	-	16384 bytes	Planned	
32 kB	-	32768 bytes	Planned	

4.2 Configuration settings on PICC level

MIFARE DESFire EV3 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 EV2, but some more functionality was added additionally.

Table 5. SetConfiguration command options

Option	Bit Index and Meaning	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3	Description
0x00	Bit 6 - 4-byte NUID configuration	Not supported	Not supported	Supported	Setting a 4-byte NUID for the PICC.
	Bit 5 - Random ID configuration	Not supported	Not supported	Supported	Configuring the format of the Random ID (ISO compliant or legacy Random ID format).
	Bit 4 - Error code binding	Not supported	Not supported	Supported	
	Bit 3 - AuthVCMandatory	Not supported	Supported	Supported	Same functionality
	Bit 2 - PCMandatory	Not supported	Supported	Supported	Same functionality
	Bit 1 - Random ID enablement	Supported	Supported	Supported	Same functionality
	Bit 0 - Format disabling	Supported	Supported	Supported	Same functionality
0x01	Updating the PICCAppDefaultKey	Supported	Supported	Supported	Same functionality

Table 5. SetConfiguration command options*...continued*

Option	Bit Index and Meaning	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3	Description
0x02	Setting a user-defined ATS	Supported	Supported	Supported	Same functionality
0x03	Setting a user-defined SAK	Not supported	Supported	Supported	Same functionality
0x04	Secure Messaging configuration	Not supported	Supported	Supported	Same functionality
0x05	71...64 - VCTID Override	Not supported	Not supported	Supported	VC Type Identifier Override
	55...48 - PDCap 1.2	Not supported	Supported	Supported	Same functionality
	39...32 - PDCap 2.2	Not supported	Not supported	Supported	Chip manufacturer defined PDCap2.2: TransactionTimer enablement and configuration (to limit the time of one transaction).
	15...8 - PDCap 2.5	Not supported	Supported	Supported	Same functionality
	7...0 - PDCap 2.6	Not supported	Supported	Supported	Same functionality
0x06	VCIID configuration	Not supported	Supported	Supported	VCIID reconfiguration Changing the default ISO DF Name for MIFARE DESFire to a customized one.
0x0C	ATQA configuration	Not supported	Not Supported	Supported	User ATQA Defining a customized ATQA value.

4.3 Retrieving the Card UID

The GetCardUID command which is already well-known from MIFARE DESFire EV1 and EV2 is existing in the same way also on MIFARE DESFire EV3.

4.4 Application management

4.4.1 Application creation

On MIFARE DESFire EV3, 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 EV2. But on MIFARE DESFire EV3 some minor functional add-ons were included in the command parameters.

One parameter of the commands, which was extended is the parameter *KeySett3*:

Table 6. KeySett3 parameter of CreateApplication and CreateDelegatedApplication command

Parameter	Bit Index and Meaning	MIFARE DESFire EV2	MIFARE DESFire EV3	Description
KeySett3	4 - Application deletion with Application MasterKey	NOT supported	Supported	Application deletion with the Application MasterKey can be always enabled, independent of the PICCKeySettings.
	2 - Application-specific capability data	Supported	Supported	Enabling / disabling capability data.
	1 - Application-specific VC keys	Supported	Supported	Enabling / disabling VC keys.
	0 - Application keysets	Supported	Supported	Enabling / disabling multiple application keysets.

On MIFARE DESFire EV1 in contrast, only the CreateApplication command was available.

4.4.2 Application deletion

The application deletion functionality on MIFARE DESFire EV3 was extended, with one more possible way of deletion. Option 1 and 2 were already well-known and Option 3 was added for an easier deletion of delegated applications:

1. On PICC Level: Application deletion after authentication with PICCMasterKey
2. On Application Level: Application deletion (standard and delegated application) after authentication with ApplicationMasterKey
3. On PICC Level: Delegated application deletion after authentication with PICCDAMAuthKey

5 Application level functionality

5.1 Application configuration

On application level, MIFARE DESFire EV3 offers the same configuration options and settings as were already available on MIFARE DESFire EV2. Some new options have been added additionally, which can be seen in the options of the SetConfiguration command, in Section 4.

5.2 File types and their configurability

MIFARE DESFire EV3 offers the six already well-known file types which were already available on MIFARE DESFire EV2.

The file access rights and, also the possibility of having multiple file access right sets per file, remain in the same already known way.

As new available feature, one of the available file types support the so-called *Secure Dynamic Messaging and Mirroring* on MIFARE DESFire EV3:

- Standard Data File

For enabling the mentioned feature, the FileOption parameter of the file creation command needs to be set accordingly:

Table 7. FileOption parameter of CreateStandardDataFile command

Parameter	Bit Index and Meaning	MIFARE DESFire EV1	MIFARE DESFire EV2	MIFARE DESFire EV3	Description
FileOption	7 - Additional Access Rights	NOT Supported	Supported	Supported	Enabling additional access right sets for this file.
	6 - Secure Dynamic Messaging & Mirroring	NOT Supported	NOT Supported	Supported for • Standard Data File	Enabling the SDM functionality.
	1...0 - Communication Mode	Supported	Supported	Supported	Set the communication mode for this file (Plain, MACed, Fully Encrypted).

5.2.1 File settings and options

The file settings are chosen during the creation of the file, as outlined in Section 5.2.

For again retrieving the file settings from the IC, the **GetFileSettings** command is available.

The GetFileSettings command returns the already known settings in the same way as it was already done for MIFARE DESFire EV2 for these file types:

- Linear Record File
- Cyclic Record File
- Transaction MAC File

For the Standard Data File, which additionally supports the *Secure Dynamic Messaging (SDM)* feature on MIFARE DESFire EV3, all SDM relevant parameters and settings are returned.

The SDM parameters are listed in Table 8.

Table 8. SDM Options of the GetFileSettings command for the Standard Data File

SDM Options	Description
SDM Options	Bit settings for indicating whether SDM-specific options like the VCUID mirroring, SDMReadCtr, SDMReadCtrLimit, SDMEncFileData are enabled or disabled.
SDM Access Rights	Access rights for the SDM-specific data and the mirrored data (Meta Data Read access and SDM File Read access).
VCUID Offset	Mirror position for the VCUID (LSB first).
SDM Read Ctr Offset	Mirror position for the SDM Read Counter (LSB first).
PICC Data Offset	Mirror position for encrypted PICC Data (LSB first).
SDM MAC Input Offset	Offset in the file where the SDM MAC computation starts (LSB first)
SDM ENC Offset	Mirror position for the SDM ENC (LSB first).
SDM ENC Length	Length of the SDM ENC File Data (LSB first).
SDM MAC Offset	Mirror position for the SDM MAC.
SDM Read Ctr Limit	The limit of the SDMReadCtr. Limiting the number of reads that can be done with a single device applying Secure Dynamic Messaging. Main use case is to limit the number of usage from the card side.

For retrieving file counters from Standard Data Files on MIFARE DESFire EV3 that are related to the Secure Dynamic Messaging, the command **GetFileCounters** is available for execution.

This command returns the SDMReadCtr (LSB first) of the targeted file.

For changing all available file options and settings, the dedicated **ChangeFileSettings** command can be used.

Using this well-known command from MIFARE DESFire EV1 and EV2, all possible file settings can be changed. The available settings that can be modified are different between all available file types. For MIFARE DESFire EV3 the command is fully backward compatible and has been extended with the optional settings for configuring new IC features.

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 DESFire EV3, the same commands can be utilized.

For data exchange, MIFARE DESFire EV3 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.

MIFARE DESFire EV3 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 EV1 and EV2, the file access rights management is implemented in the same way for MIFARE DESFire EV3.

Every file can be associated with 4 basic access rights:

- Read
- Write
- ReadWrite
- ChangeConfiguration

These 4 access rights form one so called access condition set. Every file can be optionally equipped with up to 8 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 DESFire EV3 the described access rights and access condition sets are existing in the same way. But they have been extended with access conditions reflecting the access rights that are needed for Secure Dynamic Messaging (SDM).

Once SDM is enabled for a Standard Data File, additionally 3 access rights can be defined:

- SDM Meta Read
- SDM File Read
- 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 three mentioned access rights, an available application key number or the FREE (0xE) or NEVER (0xF) access right can be set.

The purpose / functionality of the three 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 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 DESFire EV3 product.

7.1 Virtual card

The virtual card feature and concept is unchanged in MIFARE DESFire EV3 and works in the same way as it is already known from MIFARE DESFire EV2.

Please refer to [1] for MIFARE DESFire EV3 virtual card architecture details.

7.2 Proximity check

The proximity check feature and concept is unchanged in MIFARE DESFire EV3 and works in the same way as it is already known from MIFARE DESFire EV2.

Please refer to [1] for MIFARE DESFire EV3 proximity check details.

As small extension to the existing three proximity check related commands, they have been extended with an optional parameter.

The three proximity check commands are:

- PreparePC
- ProximityCheck
- VerifyPC

The optional parameter *actBitRate* (activated bit rate) can be included as response parameter of the PreparePC command, which also means that the VerifyPC command needs to take this into consideration. However, this is only optional and there is no strong need to include the actBitRate, which guarantees complete backward compatibility of the proximity check protocol.

7.3 Originality check

The originality check feature and concept is unchanged in MIFARE DESFire EV3 and works in the same way as it is already known from MIFARE DESFire EV2.

There are two originality check procedures available on MIFARE DESFire EV3:

- Symmetric originality check concept using AES
- Asymmetric originality check concept based on signature checking and ECC

Please refer to [1] for MIFARE DESFire EV3 originality check details.

7.4 Transaction timer

The transaction timer is a new feature of MIFARE DESFire EV3 which was not existing on any of the prior MIFARE DESFire products.

To mitigate attacks where a Man-in-the-Middle (MitM) attacker would delay execution of the CommitTransaction command or a final write command to complete a transaction on the card, by keeping the card powered until, for example, he is being controlled by a

control agent during public transport, MIFARE DESFire EV3 supports a transaction timer feature.

This feature allows the card issuer to configure a maximum time a transaction can take. Once the threshold is exceeded, the card will automatically reset.

The transaction timer is by default turned off, and can be configured and activated by using the command SetConfiguration with Option 0x05, to configure the PDCap2.2.

Once enabled, the timer shall be activated on any subsequent transaction start via application selection with Cmd.SelectApplication or Cmd.ISOSelect / Cmd.ISOSelectFile.

If the timer expires, the card will be reset similar as with full power-off reset, i.e. moving the card into ISO/IEC 14443-3 IDLE state.

As long as the timer has not expired, regular command execution is not influenced by the feature. Once enabled, the transaction timer value shall be reflected via the PDCap2.2 as returned on a Cmd.AuthenticateEV2First.

Please refer to [1] for MIFARE DESFire EV3 transaction timer details.

7.5 Secure dynamic messaging

Secure dynamic messaging is a new feature that was introduced with MIFARE DESFire EV3. The Secure Dynamic Messaging (SDM) allows for confidential and integrity protected data exchange, without requiring a preceding authentication.

MIFARE DESFire EV3 supports SDM for reading from one or more Standard Data Files on the PICC. Secure Dynamic Messaging allows adding security to the data read, while still being able to access it with standard NDEF readers for NTAG Type 4 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.

Please refer to [1] for MIFARE DESFire EV3 secure dynamic messaging details.

8 References

[1] Product data sheet - MIFARE DESFire EV3 contactless multi-application IC, document number DS4870xx, available in NXP DocStore.

[2] Product data sheet - MIFARE DESFire EV2 contactless multi-application IC, document number DS2260xx, available in NXP DocStore.

9 Legal information

9.1 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.

9.2 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.

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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

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 — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. 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.

9.3 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

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: 30 September 2020
Document identifier: AN12752
Document number: 575612