AN12753

MIFARE DESFire EV3 Quick start guide

Rev. 1.2 — 30 September 2020 Application note
575512 COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE, MIFARE DESFire EV3, ISO/IEC 14443, ISO/IEC 7816, NFC, NDEF, NFC Tag Type 4, SDM, Secure Messaging, Contactless
Abstract	This document gives a quick introduction to MIFARE DESFire EV3 and lists all supporting documents, software tools and further material that is available and offered from NXP for an easy product design-in. It summarizes all information required for somebody who wants to start solution development including MIFARE DESFire EV3.

Revision history

Revision history

Rev	Date	Description
1.2	20200930	DocStore number of MIFARE DESFire EV3 data sheet corrected in Section 3
1.1	20200527	Updated title of the document and removed specific sections. Security status changed to Company Public.
1.0	20200309	Initial version of this document

1 Introduction

1.1 Purpose of this document

This document introduces the MIFARE DESFire EV3 technical support items and documentation, and explains which deliverables can be retrieved from NXP to have a quick and smooth start with developing new MIFARE DESFire EV3 applications, solutions and infrastructures.

In this document, all the information that is necessary for somebody who is interested in MIFARE DESFire EV3 is gathered. This bundle of information and support items which is provided is called “Product Support Package” for the MIFARE DESFire EV3.

The Product Support Package is a full set of documentation and software deliverables, enabling system integrators, software engineers, card manufacturers, etc. to implement their new solution based on MIFARE DESFire EV3 very easy and convenient.

1.2 Document audience

This document is targeting technical as well as marketing and business-oriented people who want to gather first knowledge concerning MIFARE DESFire EV3. Everybody who is interested on a more detailed and more technical level will be redirected to the full set of material complementing the IC.

It also addresses developers, project leaders and system integrators who have a general technical understanding and overview of a specific smartcard technology or infrastructure. More in-depth details can be found in the complimentary application notes which are mentioned within this introductory document.

2 MIFARE DESFire EV3 Overview

2.1 Characteristics of MIFARE DESFire EV3

MIFARE DESFire EV3 is the latest addition to the MIFARE DESFire family, released in April 2020.

The MIFARE DESFire family is an evolving smartcard family, offering products which are based on a flexible, secure and scalable platform, serving continuous innovation and the important aspects security as well as privacy.

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

MIFARE DESFire EV3 is a Common Criteria EAL5+ security certified IC, which fully complies with the requirements for fast and highly secure data transmission and flexible application management. It introduces a set of new features and brings along enhanced performance for best user experience.

2.2 MIFARE DESFire EV3 key pillars

MIFARE DESFire EV3 is the fastest MIFARE DESFire product ever built, being the go-to product for multi-application systems.

It provides superior end-user experience and enables fast and easy solution development.

The three key pillars of MIFARE DESFire EV3 are:

1. **Multi-Application**
   - Seamless drop-in replacement for existing MIFARE DESFire infrastructures (due to full backwards compatibility)
   - Adding new applications Over-the-Air with the AppXplorer cloud service
   - Secure and efficient inter-application transaction and data management

2. **Security**
   - Secure and reliable key update in the field
   - Offline and online transaction verification using the card generated TMAC
   - Transaction Timer to mitigate Man-in-the-Middle attacks and interference by transaction "delaying"

3. **Performance**
   - The fastest MIFARE DESFire that was ever built (1.6x faster than MIFARE DESFire EV1)
   - More operating distance and range offered for better user experience (~15%)
   - Faster and more reliable tearing handling (3x faster than on MIFARE DESFire EV1)

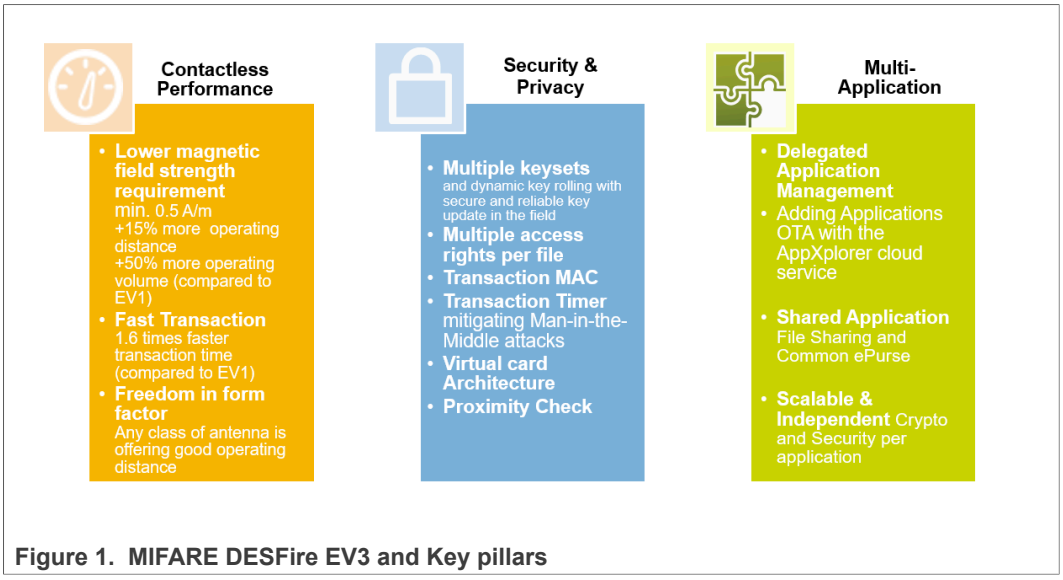

Figure 1. MIFARE DESFire EV3 and Key pillars

2.3 New innovative features and functionality

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

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

New features of MIFARE DESFire EV3 include:

- **Transaction Timer**
  This feature allows configuring the maximum time, a transaction can take. Setting the transaction timer mitigates attacks where a Man-in-the-Middle attacker would delay the execution of the CommitTransaction command and so avoid completing the transaction on the card. This could be done by keeping the card powered until, for example, being controlled by a control agent while riding the public transport.
  The Transaction Timer feature allows the card issuer to configure a maximum time a transaction can take. Once the threshold is exceeded, the card will automatically reset.

- **Secure Dynamic Messaging**
  The Secure Dynamic Messaging (SDM) on MIFARE DESFire EV3 allows for confidential and integrity protected data exchange, without requiring a preceding authentication. This allows adding security to the data read, while still being able to access it with standard NDEF readers for NFC Forum Tag Type 4 cards. The typical use case is an NDEF message holing a URI and some meta-data, where SDM allows this meta-data to be communicated confidentiality and integrity protected towards the backend server.

- **NXP AppXplorer support with pre-configured NXP DAM Keys**
  MIFARE DESFire EV3 supports the delegated application management (DAM), which allows a card issuer to delegate the application creation to third parties (application providers) in the field. Details to the DAM feature can be found in the DESFire EV3 Datasheet.
  To ease delegated application management, NXP developed a webservice called AppXplorer. The AppXplorer cloud platform allows card issuers and application providers to connect to each other, and make the application provider's applications available for the card issuer's cards. Applications can then be loaded onto cards by the card holder through the AppXplorer platform using a mobile app. To further smoothen the process, an option is foreseen where the AppXplorer platform can make use of a set of NXP pre-configured DAM keys. This avoids a card pre-personalization effort for the card issuer, as NXP will already trust-provision the NXP DAM keys onto the IC during manufacturing.

MIFARE DESFire EV3 improvements and innovations:

- **Backwards compatibility**
  MIFARE DESFire EV3 can be used as a drop-in replacement for existing MIFARE DESFire reader installations.
  It can be used functionally as MIFARE DESFire EV1 or MIFARE DESFire EV2 in its default delivery configuration. Every new feature would require an activation and/or the use of new commands which is described in their respective sections in this document.

- **Increased frame size**
  A larger frame size of up to 256 bytes can be utilized for several data exchange commands. This allows the transfer of large amounts of data in fewer command-response pairs and so increases the overall transaction time.

- **Performance benefit - Up to 1.6 times speed improvement (compared to MIFARE DESFire EV1)**
  Faster transaction speed enhances the overall system efficiency and user experience without any required reader changes. (Measurement done at a 2 A/m field strength using an AES reference transaction).

- **Performance benefit - Up to 50 % more operating volume (compared to MIFARE DESFire EV1)**
  The transaction starts earlier, as the operating distance is enlarged and the overall transaction is more robust as the operating volume is higher. The minimum required field strength amounts 0.5 A/m.

3 MIFARE DESFire EV3 Product support package

The Product Support Package (PSP) for the MIFARE DESFire EV3 IC is composed of the following deliverables:

1. **Data sheet – DS4870 MIFARE DESFire EV3**
   Product Data sheet, available in NXP DocStore document number 4870xx

2. **Application note – AN12753 MIFARE DESFire EV3 Quick start guide**
   available in NXP DocStore, document number 5755xx

3. **Application note – AN12757 MIFARE DESFire EV3 Features and hints**
   available in NXP DocStore, document number 5881xx

4. **Application note – AN12752 MIFARE DESFire EV3 Feature and Functionality Comparison to other MIFARE DESFire products**
   available in NXP DocStore, document number 5756xx

5. **Application note – AN12755 MIFARE DESFire EV3 Card Coil Design Guide**
   available in NXP DocStore, document number 5758xx

6. **Product Qualification Package – PQP5962 MIFARE DESFire EV3**
   available in NXP DocStore, document number 5962xx

7. **Wafer Specification – WS5808 MF3D(H)x3 Wafer and Delivery Specification**
   available in NXP DocStore, document number 5808xx

8. **TapLinx**
   An Android SDK offering easy implementation of Android Apps interacting with any of the NXPs offered contactless NFC-based ICs. Available via the NXP website under the following weblink: https://www.mifare.net/en/products/tools/taplinx/

9. **RFID Discover**
   A Windows-based software tool that can be used for NXP product-specific command exchange with the MIFARE DESFire EV3 IC. Available in NXP DocStore and on the NXP website under the following weblinks:
   https://www.nxp.com/search?category=softwaretools&keyword=rfiddiscover
   https://www.mifare.net/en/products/tools/rfiddiscover/

10. **NXP Card Test Framework**
    A Windows-based software tool that can be used for NXP product-specific command exchange with the MIFARE DESFire EV3 IC. Especially suitable for generating transactions and scripts that can be used for chip configuration, personalization, transaction testing and much more. Available in NXP DocStore.

11. **Android Applications – TagInfo and TagWriter**
    Android Apps offering the possibility to interact with the MIFARE DESFire EV3 smartcards as well as any other of the NXPs offered contactless NFC-based ICs. Available via the NXP Website under the following weblinks:
    https://www.mifare.net/en/products/tools/nfc-taginfo-app/
    https://www.mifare.net/en/products/tools/nfc-tagwriter-app/

12. **MIFARE DESFire EV3 Sample Cards**
    Sample cards can be requested directly at your NXP representative or contact person (sales, marketing, business development) or ordered via the NXP website.

4 Legal information

4.1 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.

4.2 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.

4.3 Licenses

ICs with DPA Countermeasures functionality

LICENSED DPA COUNTERMEASURES™

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

Purchase of NXP ICs with NFC technology

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

4.4 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.

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

NTAG — is a trademark of NXP B.V.

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

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 30 September 2020
Document identifier: AN12753
Document number: 575512