

AN14217

MIFARE DUOX Quick start guide

Rev. 1.0 — 20 November 2024

975210

Application note

Document information

Information	Content
Keywords	MIFARE, MIFARE DUOX, 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 DUOX 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 DUOX.



1 Introduction

1.1 Purpose of this document

This document introduces the MIFARE DUOX 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 DUOX applications, solutions and infrastructures.

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

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 DUOX 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 DUOX. 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 DUOX Overview

2.1 Characteristics of MIFARE DUOX

MIFARE DUOX was released in September 2024 as the first member of the MIFARE product family supporting asymmetric crypto. It can be seen as the logical successor of the MIFARE DESFire family.

The MIFARE DUOX is covering most well-known commands and features from previous MIFARE DESFire family ICs, plus adding some new features.

All **DES based crypto** an secure messaging variants earlier than the EV2 secure messaging are not supported anymore.

MIFARE DUOX is a Common Criteria EAL6+ 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 DUOX key pillars

MIFARE DUOX is the first product in the MIFARE family supporting asymmetric cryptography and authentication options. The basic functionality of MIFARE DUOX is closely related to MIFARE DESFire EV3, but its not to be seen as a successor of MIFARE DESFire EV3, but rather a completely new branch in the MIFARE product architecture. As asymmetric cryptography is able to offer an rather easy way for key distribution compared to symmetric cryptography, MIFARE DUOX is able to solve one of the most critical problems in many infrastructures: How to transfer keys from A to B. MIFARE DUOX follows the so called PKI (public key infrastructure) approach not only eliminates the need to exchange secret material between two entities, it also enables unilateral authentication schemes for card-unilateral and reader-unilateral authentications.

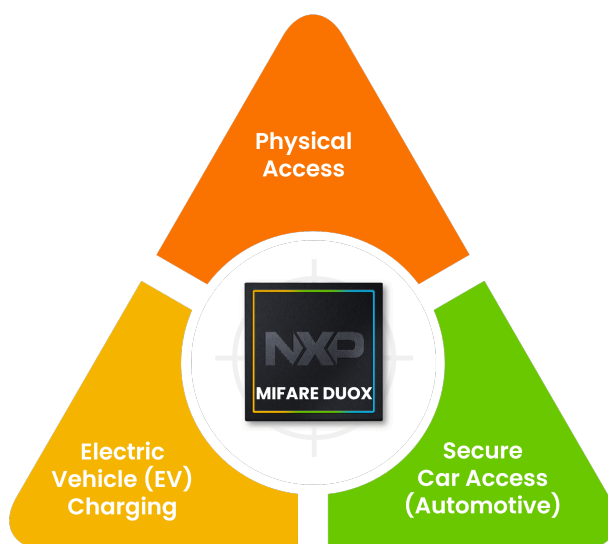


Figure 1. MIFARE DUOX key pillars

The MIFARE DUOX key pillars are:

- Asymmetric Cryptography and fast asymmetric authentication for simplified key management and key provisioning via the public key infrastructure and certificate distribution.
 - MIFARE DUOX offers key generation and certificate storage on the card
 - Reader deny-listing based on certificate revocation
 - 90 ms ECC based authentication
- Combining the best of 2 worlds, MIFARE DUOX is based on the field proven, flexible MIFARE DESFire architecture with asymmetric crypto on top
 - Combining flexible PKI based benefits with already well-known MIFARE DESFire file system
 - True multi-application support allowing implementations for many different use cases
 - Rich enhanced feature set including Proximity Check, Transaction Signature
- Performance and Security based on future proven hardware and software design
 - Fast and secure RF performance and transaction time
 - AES256 based cryptography support ensuring Post-Quantum-Crypto requirements readiness
 - Common Criteria EAL6+ certification

3 MIFARE DUOX Product support package

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

1. **Data sheet – DS9744 MIFARE DUOX**
Product Data sheet, available in NXP Secure Files document number DS9744xx
2. **Application note – AN14217 MIFARE DUOX Quick start guide**
available in NXP Secure Files, document number 9752xx
3. **Application note – AN14215 MIFARE DUOX Features and hints**
available in NXP Secure Files, document number 9750xx
4. **Application note – AN14218 MIFARE DUOX Feature and Functionality Comparison to MIFARE DESFire products**
available in NXP Secure Files, document number 9753xx
5. **Application note – AN14216 MIFARE DUOX Card Coil Design Guide**
available in NXP Secure Files, document number 9751xx
6. **Product Qualification Package – PQP9746 MIFARE DUOX**
available in NXP Secure Files, document number PQ9746
7. **Wafer Specification – AD9747 MF3E(H)x3 MIFARE ECC Wafer and Delivery Specification**
available in NXP Secure Files, document number AD9747xx
8. **UM9748 MF3E(H)x3 MIFARE ECC User Guidance Manual**
available in NXP Secure Files, document number AD9747xx
9. **TapLinx**
An Android SDK offering easy implementation of Android Apps interacting with any of the NXP's offered contactless NFC-based ICs. Available via the NXP website under the following weblink: <https://www.mifare.net/en/products/tools/taplinx/>
10. **RFID Discover**
A Windows-based software tool that can be used for NXP product-specific command exchange with the MIFARE DUOX IC. Available in NXP DocStore and on the NXP website under the following weblinks: <https://www.nxp.com/search?category=softwaretools&keyword=rfdiddiscover>
11. **NXP Card Test Framework**
A Windows-based software tool that can be used for NXP product-specific command exchange with the MIFARE DUOX 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.
available in NXP Secure Files, document number SW5434

12. Android Applications – TagInfo and TagWriter

Android Apps offering the possibility to interact with the MIFARE DUOX smartcards as well as any other of the NXPs offered contactless NFC-based ICs. Available via the NXP Website under the following weblinks:

<http://nxp.com/design/design-center/software/rfid-developer-resources/nfc-tagwriter-app-by-nxp:NFC-TAGWRITER>

<http://nxp.com/design/design-center/software/rfid-developer-resources/the-nfc-taginfo-app-by-nxp:NFC-TAGINFO>

13. MIFARE DUOX 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 Revision history

Table 1. Revision history

Document ID	Release date	Description
AN14217 v.1.0	20 November 2024	• Initial version

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) 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.

MIFARE — is a trademark of NXP B.V.

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

NTAG — is a trademark of NXP B.V.

Tables

Tab. 1. Revision history7

Figures

Fig. 1. MIFARE DUOX key pillars 3

Contents

1 Introduction2

1.1 Purpose of this document2

1.2 Document audience2

2 MIFARE DUOX Overview3

2.1 Characteristics of MIFARE DUOX3

2.2 MIFARE DUOX key pillars3

3 MIFARE DUOX Product support package5

4 Revision history7

Legal information8

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