AN13454

MIFARE Ultralight AES quick start guide

Rev. 1.1 — 18 February 2022

Application note
COMPANY PUBLIC

Document information

Information	Content
Keywords	MIFARE, MIFARE Ultralight AES, quick start guide, AES Authentication, counter, CMAC
Abstract	This document gives a quick introduction to MIFARE Ultralight AES 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 Ultralight AES.

Revision history

Revision history

Rev	Date	Description
1.1	20220218	Security status changed to "Company public"
1.0	20211202	Initial version of this document

1 Introduction

1.1 Purpose of this document

This document introduces the MIFARE Ultralight AES 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 Ultralight AES applications, solutions and infrastructures.

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

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 Ultralight AES 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 Ultralight AES. Everybody who is interested on a more detailed and more technical level will be redirected to the full set of material complementing the IC.

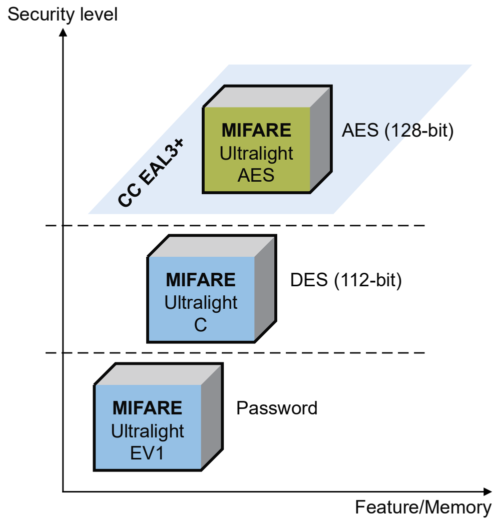
It also addresses developers, project leaders and system integrators who have a general technical understanding and overview of a specific smartcard technology or infrastructure. More in-depth details can be found in the complimentary application notes which are mentioned within this introductory document.

2 MIFARE Ultralight AES overview

2.1 Characteristics of MIFARE Ultralight AES

MIFARE Ultralight AES is the latest addition to the MIFARE Ultralight family, released in 2022.

The MIFARE Ultralight family has evolved since the first MIFARE Ultralight, and culminates with the MIFARE Ultralight AES being the first Common Criteria certified product in its family, providing AES-128 3-pass mutual authentication and memory access protection, and CMAC-based secure messaging for data integrity protection.



aaa-044600

Figure 1. MIFARE Ultralight Evolution

Table 1. MIFARE Ultralight AES feature comparison

Product features	MIFARE Ultralight			
	EV1		C	AES
RF Interface	ISO/IEC 14443-2, Type A 13.56 MHz			
Protocol	ISO/IEC 14443-3			
UID - unique identifier	7-byte UID			
Privacy				Random ID
Communication speed	106 kbps			
Memory size [Bytes]	48	128	144	144
Memory model				
Crypto			3KDES	AES
Key length			112-bit	128-bit
Authentication	Password		3-pass mutual	
Communication security				CMAC
Command Counter to limit negative authentication attempts	-			yes

Table 1. MIFARE Ultralight AES feature comparison*...continued*

3x independent one-way counter	yes	-	yes (AES optional)
Virtual card concept			VC Select Last
Originality check features	ECC signature	-	ECC signature programmable
CC Certification			CC EAL 3+
NFC compliance	NFC Forum Type 2 Tag compliant		
Input capacitance [pF]	17 / 50		

2.2 MIFARE Ultralight AES key pillars

MIFARE Ultralight AES is the first limited-use MIFARE product on the market using Advanced Encryption Standard (AES) with external Common Criteria EAL3+ (AVA_VAN.2) security certification. It is targeted as a cost-effective solution for single use public transport tickets, hospitality applications (such as hotel room access, parking garage access, spas, gyms etc.) and event ticketing.

Table 2. MIFARE Ultralight AES key features

Security	• Support of 3-pass mutual AES authentication based on a key length of 128-bit – Data protection in user memory – One-way counter with optional AES authentication protection • Secure messaging communication mode (CMAC) for data integrity protection over RF-Interface – Countermeasure against both replay attacks and man-in-middle attacks • Common Criteria (CC) EAL3+ (AVA_VAN.2) certification
Privacy and ownership	• Random ID (optional) addressing privacy concerns to prevent personal data tracking – Regulations do not allow to trace end user of a ticket outside authorized use case infrastructure – Retrieval of 7-byte UNIQUE ID requires authentication with a dedicated 128-bit AES key • Originality Check based on customizable ECC signature
Design-in and scalability	• AES support from ticket to card to phone – Allows security streamline from cost-effective single use ticket up to multi-application product • Silicon comes with DARK GREEN classification supporting eco-friendly paper tickets and cards

3 MIFARE Ultralight AES Product support package

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

1. **Data sheet – DS5379 MIFARE Ultralight AES MF0AES(H)20**
   Product data sheet, available in NXP DocStore document number 5379xx
2. **Data sheet – DS7036 MIFARE Ultralight AES MF0AES(H)30**
   Product data sheet, available in NXP DocStore document number 7036xx
3. **Application note – AN13454 MIFARE Ultralight AES quick start guide**
   available in NXP DocStore, document number 7108xx
4. **Application note – AN13452 MIFARE Ultralight AES features and hints**
   available in NXP DocStore, document number 7106xx
5. **Application note – AN13453 MIFARE Ultralight AES card coil design guide**
   available in NXP DocStore, document number 7107xx
6. **Product qualification package – PQP MIFARE Ultralight AES**
   available in NXP DocStore, document number 7172xx
7. **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/
8. **RFID Discover**
   A Windows-based software tool that can be used for NXP product-specific command exchange with the MIFARE Ultralight AES 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/
9. **NXP card test framework**
   A Windows-based software tool that can be used for NXP product-specific command exchange with the MIFARE Ultralight AES 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.
10. **Android applications – TagInfo and TagWriter**
    Android Apps offering the possibility to interact with the MIFARE Ultralight AES 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/

11. **MIFARE Ultralight AES sample cards**
    Sample cards can be requested directly at your NXP representative or contact person (sales, marketing, business development).

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 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.

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.

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

MIFARE — is a trademark of NXP B.V.

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

Tables

Tab. 1. MIFARE Ultralight AES feature comparison 4

Tab. 2. MIFARE Ultralight AES key features 5

Figures

Fig. 1. MIFARE Ultralight Evolution 4

Contents

1	**Introduction**	**3**
1.1	Purpose of this document	3
1.2	Document audience	3
2	**MIFARE Ultralight AES overview**	**4**
2.1	Characteristics of MIFARE Ultralight AES	4
2.2	MIFARE Ultralight AES key pillars	5
3	**MIFARE Ultralight AES Product support package**	**6**
4	**Legal information**	**8**

Date of release: 18 February 2022
Document identifier: AN13454