ENHANCED SECURITY FOR LIMITED-USE CONTACTLESS APPLICATIONS

With cryptographic authentication that's easy to integrate into existing infrastructures, the MIFARE Ultralight AES IC adds security, privacy, and scalability to a variety of limited-use contactless applications.

TARGET APPLICATIONS

- Single-trip and multi-use transit tickets
- Hospitality RFID basic guest key card
- Sporting-event tickets
- Exhibition passes
- Access passes, e.g. festival or leisure park entry
- Electronic vouchers
- Loyalty programs

The MIFARE Ultralight AES IC delivers a new level of trust for limited-use tickets and key cards by supporting AES cryptographic authentication. Designed as a secure, contactless replacement for traditional paper tickets, mag-stripe, barcode, and QR code-based systems, the IC gives solution providers a more convenient, more secure way to issue single-trip and multi-use transit tickets, event tickets, access passes, loyalty cards. Further, in hospitality it gives guests secure access to hotel rooms and other hotel facilities, including spas, gyms, and parking garages.

KEY BENEFITS

- AES cryptography for secure authentication and protected data access with 128-bit key length and optional Command Counter to limit negative authentication attempts resulting in strong guest protection, card clone prevention, and secure room access
- Chip-level security implementations to ensure privacy, including 7-byte UID with optional Random ID support
- Originality verification using pre-programmed, ECC-based originality signature, plus originality check back on 128-bit originality key that leverages AES authentication

- Proven secure performance with CC EAL 3+ certification and ISO/IEC 14443A-2/-3 compliance

CONTACTLESS SECURITY

- Using a single, standard-based encryption method, such as AES, simplifies the infrastructure and reduces the complexity of business processes. Service providers gain the benefit of reduced maintenance costs, with the reassurance of greater fraud prevention.
- With tickets, vouchers, and key cards based on MIFARE Ultralight AES, solution providers have a convenient, more secure way to issue single-trip and multi-use transit tickets, RFID event tickets, access passes, loyalty cards, and more.
- In hospitality MIFARE Ultralight AES gives hotel owners and brands a more secure contactless way to transition away from legacy access technologies, such as mechanical keys, mag-stripe cards, and previous generations of RFID key cards. The MIFARE Ultralight AES IC is suited for basic RFID guest cards and its enhanced security features can contribute to a secure RFID lock system, for increased privacy and safety during each guest's stay.

FASTER DEVELOPMENT

- Developers have a faster way to deliver enhanced security in limited-use ticketing applications because of using the same memory structure and command sets with MIFARE Ultralight. The MIFARE Ultralight AES IC also helps to enable scale for transport and access operators as well other service providers, since a single encryption standard supports multiple form factors, from paper tickets to smartcards and mobile devices.
- This means as well that door-lock operators have less effort to implement the MIFARE Ultralight AES IC in infrastructures that already support AES cryptography, by leveraging the AES support of readers.

KEY FEATURES

Security

- Protected data access based on AES authentication with 128-bit key length and optional Command Counter to limit negative authentication attempts
- CMAC protection for message integrity protection
- Optional AES authentication protection for 1x out of 3x 24-bit one-way-counter
- 7-byte UID with optional Random ID support for enhanced privacy
- ECC-based originality signature (pre-programmed)
- Originality check based on 128-bit originality key leveraging the AES authentication
- Common Criteria certification: EAL 3+

Contactless Performance

- ISO/IEC 14443 A -2 / -3 compliant
- Operating distance of up to 10 cm
- Data transfer of 106 kbit/s

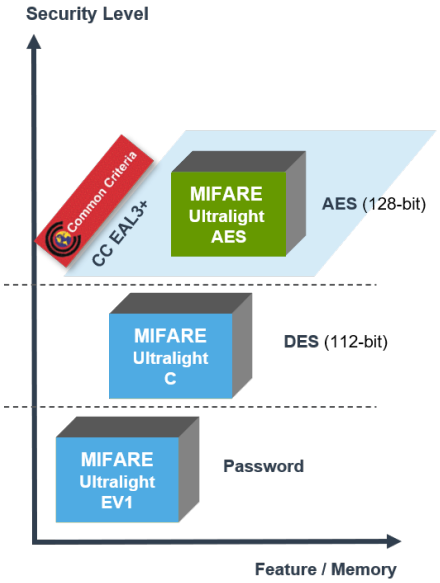
Memory

- 144-byte EEPROM user memory
- Number of single write operations: 100,000

www.MIFARE.net

MIFARE ULTRALIGHT IC FAMILY: COMPARISON TABLE

	MIFARE Ultralight AES	MIFARE Ultralight C	MIFARE Ultralight EV1
Memory (bytes)	144	144	48/128
OTP area (bits)	32	32	32
Counter (bits)	3 x 24 (AES protection optional)	1 x 16	3 x 24
Access protection (bits)	128-bit AES	112-bit 3DES	32-bit password (and password acknowledge)
Security certification	CC EAL3+		
Data integrity	CMAC		
Random ID	X		
Originality Signature	X		X



ORDERING INFORMATION

INPUT CAPACITANCE	PACKAGE FORMAT	MIFARE Ultralight AES
17 pF	Sawn wafer 120 µm on FFC (AU-bumped)	MF0AES2001DUD
	Sawn wafer 75 µm on FFC (AU-bumped)	MF0AES2001DUF
	MOA8 module	MF0AES2000DA8
50 pF	Sawn wafer 120 µm on FFC (AU-bumped)	MF0AESH2001DUD
	Sawn wafer 75 µm on FFC (AU-bumped)	MF0AESH2001DUF
	MOA8 module	MF0AESH2000DA8

www.nxp.com

Date of Release: February 2022

Document Number: MIFAREULAESFSA4 REV 0