Migrate classic contactless smart card systems to the next security level

MIFARE Plus

MIFARE Plus brings benchmark security to mainstream contactless smart card applications. It is the only mainstream IC compatible with MIFARE Classic, offering a seamless upgrade path for existing infrastructure and services.

Key applications

- Public transportation
- Access management, e.g. employee, school, or campus cards
- Electronic toll collection
- Car parking
- Loyalty programs

Key features

- 2 or 4 KB EEPROM
- Simple fixed memory structure compatible with MIFARE Classic 1 K (MF1ICS50), MIFARE Classic 4 K (MF1ICS70)
- Migration path from MIFARE Classic to MIFARE Plus security level supported
- Open standard AES crypto for authentication, integrity, and encryption
- Common Criteria certification: EAL4+ for IC HW and SW
- Complies with ISO/IEC 14443-A
- 7-Byte Unique Identifier (UID) or 4-Byte Non Unique Identifier (NUID) and random IDs
- Multi-sector authentication, multi-block read and write
- Anti-tear function for writing AES keys
- Keys can be stored as MIFARE Classic CRYPTO1 keys (2 x 48 bit per sector) or as AES keys (2 x 128 bit sector)
- Supports virtual card concept
- High data rates up to 848 kbit/s
- Available in MOA4 modules or 8-inch sawn bumped wafer

NXP MIFARE Plus is based on open global standards both for air interface and cryptographic methods. It is available in two versions: MIFARE Plus S, the Slim version, for straightforward migration of MIFARE Classic systems, and MIFARE Plus X, the eXpert version, which offers more flexibility to optimize the command flow for speed, privacy, and confidentiality.
MIFARE Plus X offers a rich feature set, including proximity checks against relay attacks.
MIFARE Plus is fully functional backwards compatible with MIFARE Classic 1 K / 4 K. Interoperability with MIFARE Classic has been verified by the independent MIFARE Certification Institute. MIFARE Plus offers the possibility to issue cards seamlessly into existing MIFARE Classic applications, before the infrastructure is upgraded. Once the infrastructure security upgrades are in place, MIFARE Plus cards can be switched to a more secure mode in the field with no customer interaction necessary.

AES (advanced encryption standard) is then used for authentication, encryption, and data integrity. MIFARE Plus supports high-speed communication between the card and terminal at up to 848 kbps/s, for time critical services. The read range of up to 10 cm increases the convenience of the touch-and-go experience.

Security levels

MIFARE Plus cards support one pre-personalization level and three security levels. Cards operate in one security level at any given time and can only be switched to a higher level.
An automatic anti-tear mechanism is available for secure deployment of rolling keys. If a card is removed from the field during a key update, it either concludes the update or automatically falls back to the previous key.
NXP recommends 7-Byte UID, but offers 4-Byte UID versions of MIFARE Plus during migration. MIFARE Plus is available in the proven MOA4 module and as sawn bumped wafers; no changes for existing manufacturing processes are necessary.
For benchmark security on the reader side, the MIFARE SAM AV2 (secure application module) is available. It includes all MIFARE Plus commands, secure key storage and AES calculation for a reader device. To support the design-in process for reader manufacturers and solutions developers, NXP provides MIFARE Plus documentation, application notes, and software toolkits.

About MIFARE

MIFARE is NXP´s well-known brand for a wide range of contactless IC products used in more than 40 different applications worldwide. With more than 150 million reader core components and 5 billion smart card ICs sold, MIFARE products are proven and reliable more than any other interface technology in the market.
MIFARE products comply with the international standard ISO/IEC 14443 and are backwards compatible within the product families. This ensures that the existing infrastructure can be smoothly upgraded to higher security and feature levels such as payment systems, ticketing solutions, loyalty programs, access management and parking.
To further extend the reach of MIFARE products, the MIFARE4Mobile Industry Group brings MIFARE applications into NFC enabled mobile devices.

- Security Level 0
  MIFARE Plus cards are pre-personalized with configuration keys, level switching keys, MIFARE Classic CRYPTO1 and AES keys for the memory.
- Security Level 1
  In this level the cards are 100% functionally backwards compatible with MIFARE Classic 1 K / 4 K cards. Cards work seamlessly in existing MIFARE Classic infrastructure.
- Security Level 2
  (MIFARE Plus X only)
  Mandatory AES authentication. MIFARE Classic CRYPTO1 for data confidentiality.
- Security Level 3
  Mandatory AES for authentication, communication confidentiality and integrity.
  Optional proximity detection (MIFARE Plus X only)

Product Features	MIFARE Plus S 2K	MIFARE Plus S 4K	MIFARE Plus X 2K	MIFARE Plus X 4K
Memory				
EEPROM size [byte]	2 K	4 K	2 K	4 K
Write endurance [typical cycles]	200 000			
Data retention [years]	10			
Organization	32 sectors with 4 blocks	32 sectors with 4 blocks 8 sectors with 16 blocks	32 sectors with 4 blocks	32 sectors with 4 blocks 8 sectors with 16 blocks
RF-Interface				
Acc. To ISO 14443A	yes - up to layer 4			
Frequency [MHz]	13.56			
Baudrate [kbit /s]	106 … 848			
Anticollision	bit-wise			
Security				
Unique Serial Number [byte]	4 or 7			
4 byte Random ID	yes in SL3			
True Random Number Generator	yes			
Access keys	CRYPTO1 or AES keys per sector			
Access conditions	per sector			
AES security	CMACing		CMACing / Encipherment	
Anti-tearing	for AES keys, sector trailers and configuration			
Cryptography	AES (128 bit), CRYPTO 1			
Special Features				
Supported MF PLUS levels	SL1, SL3		SL1, SL2, SL3	
Multi-sector authentication	yes			
Virtual card support	yes, limited command set		yes, full command set	
Proximity check	no		yes	
Packaging				
Sawn Wafer (Au Bumped)				
7 Byte UID	MF1SPLUS6001DUD	MF1SPLUS8001DUD	MF1PLUS6001DUD	MF1PLUS8001DUD
4-Byte Non Unique (NUID)	MF1SPLUS6031DUD	MF1SPLUS8031DUD	MF1PLUS6031DUD	MF1PLUS8031DUD
MOA4 Module				
7 Byte UID	MF1SPLUS6001DA4	MF1SPLUS8001DA4	MF1PLUS6001DA4	MF1PLUS8001DA4
4-Byte Non Unique (NUID)	MF1SPLUS6031DA4	MF1SPLUS8031DA4	MF1PLUS6031DA4	MF1PLUS8031DA4
MOA8 Module				
7 Byte UID	MF1SPLUS6001D8	MF1SPLUS8001DA8	MF1PLUS6001DA8	MF1PLUS8001DA8
4-Byte Non Unique (NUID)	MF1SPLUS6031DA8	MF1SPLUS8031DA8	MF1PLUS6031DA8	MF1PLUS8031DA8

MIFARE, MIFARE Plus and MIFARE4Mobile are trademarks of NXP Semiconductors N.V.

www.MIFARE.net

www.nxp.com

2013 NXP Semiconductors N.V.
I rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The formation presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and ay be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof oes not convey nor imply any license under patent- or other industrial or intellectual property rights.

Date of release: September 2013