NXP®
MIFARE Plus® EV2

Seamless deployment of security upgrades for contactless services

This second-generation MIFARE Plus IC, equipped with enhanced performance and security features, along with support for mobile services and over-the-air updates, is a quick, cost-effective way to upgrade existing contactless infrastructures to AES security, and also delivers better experiences, with greater convenience, in Smart City services.

KEY FEATURES

Contactless Performance

- ISO/IEC 14443 A 1-4 & ISO/IEC 7816-4 for mobile and wearable device acceptance
- Better transaction times and RF-performance
- MIFARE Classic backward compatibility mode for a seamless infrastructure migration

Migration

- User-programmable activation parameters (SAK & ATQA) for preliminary migration of all security levels (SL0, SL1 and SL3) in MIFARE Classic product-based infrastructures
- Flexible migration to secure AES-128 authentication and messaging at sector or chip level in SL1SL3MixMode

Security

- Banking-level protection with Common Criteria EAL5+ certification
- Access rights division between SL1 and SL3 to restrict update operations
- Online and offline proof of transaction towards card generated Transaction MAC
- Smart card proximity check to detect relay attacks
- Transaction Timer to combat man-in-the-middle attacks

TARGET APPLICATIONS

- Public transportation
- Access management
- Closed-loop micropayment
- Campus and student ID cards
- Loyalty programs
- Electronic toll collection
- Car parking

KEY BENEFITS

- Seamless migration of existing infrastructures, with backward compatibility to MIFARE Classic EV1 and MIFARE Plus products
- Next-level protection, with upgrades from Crypto1 to 128-bit AES security
- Secure end-to-end communication channel for over-the-air services such as mobile top-up of smart cards and deployment of MIFARE 2GO (mobile services) in SL3

As the next generation of NXP's MIFARE Plus product family, the MIFARE Plus EV2 IC is designed to be both a gateway for new Smart City applications and a compelling upgrade, in terms of security and connectivity, for existing deployments. The IC demonstrates longer read range capabilities and faster transaction times to its predecessor, so contactless services are more convenient to use, and offers backward compatibility to MIFARE Classic EV1 and MIFARE Plus products, for a cost-efficient way to upgrade the security features of in-place smart card applications – without the need for extensive upfront investments to kick-off migrations.

STRONG SUPPORT FOR EXISTING INFRASTRUCTURES

The MIFARE Plus EV2 IC uses an innovative Security Level (SL) concept to help create seamless step-by-step upgrades of legacy infrastructures to higher security. The IC allows for SL switching from low security (SL1) to high security (SL3), based on 128-bit AES security for authentication, data integrity and data protection. SL switching can be applied to the IC as a whole or to individual sectors. A special feature, called SL1SL3MixMode, makes it possible to enable AES-128 secure authentication on sectors based on MIFARE Classic EV1. This allows, in combination with the new SL1 Update Restrictions, to read data stored in a block with SL1 authentication, but updating data only works with secure AES-128 authentication. The block-based structure of MIFARE Plus EV2 uses a technology logic that is compatible with the block-based structure of Crypto1 applications, so deployments based on Crypto1 can retain their structural logic. This allows for cost-efficient migration paths from legacy MIFARE Classic EV1 and Crypto1 to high-level 128-bit AES security. As the IC supports legacy and new infrastructures at the same time, end users can conveniently continue using the same smart card while the system is being upgraded to higher security.

EXPANDED FEATURE SET FOR SECURE, CONTACTLESS SMART CITY SERVICES

Special features address the need for enhanced security and privacy in Smart City services. For example, the Transaction MAC (TMAC) can help to ensure the authenticity of each transaction, so as to minimize fraud and identify theft. To help mitigate man-in-the-middle attacks, the new Transaction Timer feature, which is also available on NXP's MIFARE DESFire EV3 IC, makes it possible to set a maximum time per transaction, so it's harder for an attacker to interfere with the transaction. Support for EEPROM sizes up to 4 Kbytes help address the growing memory requirements of system applications.

SUPPORT FOR MOBILE & OVER-THE-AIR SERVICES

With MIFARE Plus EV2, Smart City services such as mobile transport ticketing and mobile access can run on NFC-enabled smartphones and wearables. Operating MIFARE Plus EV2 in SL3 supports the use of NXP's MIFARE 2GO cloud service, which manages digitized MIFARE product-based credentials and enables features like contactless payments and mobile access using NFC-enabled devices. Using the secure, end-to-end communication channel (SL1SL3MixMode) provided by MIFARE Plus EV2, system operators can design additional revenue streams based on the introduction of over-the-air services, such as mobile top-ups, even with legacy Crypto1 applications.

FEATURE COMPARISON: MIFARE Plus EV2 and MIFARE Plus X

Memory	MIFARE Plus EV2	MIFARE Plus X
Memory configuration	Block/sector structure	Block/sector structure
Memory size	2 kB / 4 kB	2 kB / 4 kB
RF Interface		
ISO/IEC	ISO/IEC 14443 A 1-4 ISO/IEC 7816	ISO/IEC 14443 A 1-4 ISO/IEC 7816
UID/ONUID	7B UID or 4B ONUID	7B UID or 4B ONUID
Data rates	Up to 848 kbps, ISO/IEC 14443-4	Up to 848 kbps, ISO/IEC 14443-4
Security		
Algorithm	AES 128-bit, secure messaging, legacy Crypto1	AES 128-bit, secure messaging, legacy Crypto1
Security Level concept	Sector-by-Sector or card	Card only
SL1SL3MixMode	SL3 access into SL1 sectors	-
Transaction MAC (TMAC)	Secure validation of back-end transaction	-
Transaction Timer	Mitigate man-in-the-middle attacks	-
Common Criteria certification	EAL5+ for IC HW and SW	EAL4+ for IC HW and SW

ORDERING INFORMATION

MIFARE Plus EV2	Delivery Form	17 pF	12NC
MF1P4200DA8/00	MOA8 module	4 k	935404786118
MF1P4200DA4/00	MOA4 module	4 k	935399739118
MF1P4201DUD/00	Wafer 120 µm 12"	4 k	935405406045
MF1P2200DA8/00	MOA8 module	2 k	935387932118
MF1P2200DA4/00	MOA4 module	2 k	935404211118
MF1P2201DUD/00	Wafer 120 µm 12"	2 k	935405407045
MIFARE Plus EV2	**Delivery Form**	**70 pF**	**12NC**
MF1PH4200DA8/00	MOA8 module	4 k	935383644118
MF1PH4200DA4/00	MOA4 module	4 k	935383641118
MF1PH4201DUD/00	Wafer 120 µm 12"	4 k	935405499045
MF1PH2200DA8/00	MOA8 module	2 k	935405195118
MF1PH2200DA4/00	MOA4 module	2 k	935405183118
MF1PH2201DUD/00	Wafer 120 µm 12"	2 k	935405497045

Date of Release: 23 June 2020
Document Number: MFPLUSEV2LF REV0