NXP IC for next-generation multi-application smart cards

MIFARE DESFire EV2

MIFARE DESFire EV2 is ideal for solution developers and system operators building reliable, interoperable and scalable smart card solutions. The second evolution of our industry-leading MIFARE DESFire open architecture platform for smart cards offers superior performance, state-of-the-art security and privacy and enhanced multi-application support to make new business models possible.

KEY FEATURES

▶ ISO/IEC 14443 A 1-4 and ISO/IEC 7816 compliant
▶ 2/4/8-Kbyte EEPROM with fast programming
▶ Flexible file structure
▶ NFC Tag Type 4 compliant
▶ Secure, high-speed command set
▶ MIsmartApp grants application space to third parties without sharing the master key
▶ Unlimited number of applications
▶ Transaction MAC to authenticate transactions
▶ Multiple key sets per application for key rolling
▶ Virtual Card architecture for privacy protection
▶ Proximity Check to protect against relay attacks
▶ High data rates according to ISO/IEC 14443-4: up to 848 Kbits/s
▶ Choice of open DES/2K3DES/3K3DES/AES crypto algorithms in hardware
▶ Unique 7-byte serial number (ISO Cascade Level 2)
▶ Common criteria certification: EAL5 + for IC HW and SW (certification in progress)

KEY APPLICATIONS

▶ Advanced public transportation
▶ Access management
▶ Closed-loop micropayment
▶ Campus and student ID cards
▶ Loyalty programs

Innovation in multi-application smart cards

MIFARE DESFire EV2 brings many benefits to end users. Cardholders can experience convenient contactless ticketing while also being able to use the same device for applications such as student ID, closed-loop payment at vending machines, access management, and loyalty programs. The innovative MIsmartApp feature enables new business models. System providers can offer or sell application space to third parties without having to share the master key. A MIFARE DESFire EV2 card can hold as many different applications as the memory will support, and new applications can be loaded after the product is in the field. It's like having an app store on a smart card. A purse can even be shared between applications, for greater interoperability.

Contactless performance

For a truly convenient touch-and-go experience, MIFARE DESFire EV2 offers an increase in operating distance compared to previous versions. The 70 pF option enables read range optimizations of small antenna form factors. MIFARE DESFire EV2 delivers the perfect balance of speed, performance, and cost efficiency. Its open concept allows future seamless integration of other media such as smart paper tickets, key fobs, and mobile ticketing based on Near Field Communication (NFC) technology. It is also fully compatible with the existing MIFARE reader hardware platform. With MIFARE DESFire EV2, data transfer rates up to 848 Kbit/s can be achieved, making fast data processing possible.

Security and privacy

MIFARE DESFire EV2 is based on open global standards for air interfaces and cryptographic methods. Proximity Check protects against relay attacks, while the Virtual Card Architecture anticipates future needs of privacy protection. Other security features include an on-chip backup management system and mutual three-pass authentication. Additionally, an automatic anti-tear mechanism is available for all file types, which guarantees transaction-oriented data integrity.

The DESFire name reflects NXP's continued commitment to best-in-class performance. The "DES" in the name refers to the use of DES, 2K3DES, 3K3DES and AES hardware cryptographic engine for securing transmission data, while "Fire" is an acronym for "Fast, Innovative, Reliable, and Enhanced" operation in contactless proximity applications. The MIFARE DESFire EV2 silicon solution is the consumer-friendly choice for system design, with heightened security and reliability.

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 more proven and more reliable than any other interface technology on the market. MIFARE products comply with the international standard ISO/IEC 14443 and are backward-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.

Selection guide MIFARE DESFire EV2 leaflet

Product Features	MIFARE DESFire EV2 2K MF3 D22	MIFARE DESFire EV2 4K MF3D42	MIFARE DESFire EV2 8K MF3 D82
Memory			
EEPROM size [byte]	2048	4096	8192
Write Endurance [cycles]	500 000	500 000	500 000
Data Retention [yrs]	25	25	25
Organization	Flexible file system	Flexible file system	Flexible file system
RF-Interface			
Acc. to ISO/IEC 14443A	Yes - up to layer 4	Yes - up to layer 4	Yes - up to layer 4
Frequency [MHz]	13.56	13.56	13.56
Baud rate [kbit/s]	106 … 848	106 … 848	106 … 848
Anti-collision	Bit-wise	Bit-wise	Bit-wise
Operating Distance [mm]	Up to 100	Up to 100	Up to 100
Security			
Unique Serial Number [byte]	7, cascaded	7, cascaded	7, cascaded
Random Number Generator	Yes	Yes	Yes
Access Keys	14 keys per application	14 keys per application	14 keys per application
Multiple Key Sets	Up to 16 per application	Up to 16 per application	Up to 16 per application
Access Conditions	Per file	Per file	Per file
AES, 3DES & DES Security	MACing / Encipherment	MACing / Encipherment	MACing / Encipherment
Anti-tear supported by chip	Yes	Yes	Yes
Proximity Check	Yes	Yes	Yes
Special Features			
Multi-application	Unlimited applications, MIsmartApp	Unlimited applications, MIsmartApp	Unlimited applications, MIsmartApp
Purse Functionality	Yes	Yes	Yes
Transaction MAC	Per application	Per application	Per application
Virtual Card Architecture	PICC & application level	PICC & application level	PICC & application level
Ordering information			
17 pF sawn wafer (bumped)	MF3D2201DUD	MF3D4201DUD/	MF3D8201DUD
17 pF MOA4 module	MF3D2200DA4	MF3D4200DA4/	MF3D8200DA4
70 pF sawn Wafer (bumped)	MF3DH2201DUD	MF3DH4201DUD	MF3DH8201DUD
70 pF MOA4 module	MF3DH2200DA4	MF3DH4200DA4	MF3DH8200DA4