NXP IC for next-generation multi-application smart cards

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, security and enhanced multi-application support.

KEY FEATURES

- ISO/IEC 14443 A 1–4 and ISO/IEC 7816 compliant
- 2/4/8 kB 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 Smart Card architecture for privacy protection
- Proximity check to protect againt 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 hardware and software

TARGET APPLICATIONS

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

KEY BENEFITS

- Functional backward compatible to MIFARE DESFire EV1
- Improved operating range and performance
- Enhanced security level with Common Criteria EAL5+ certification
- MIsmartApp enabling post–issuance of additional services in already deployed cards
- Multiple keysets with key rolling for simplified key migration in the field
- Transaction MAC ensuring the authenticity of each transaction

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 a significant increase in operating distance and speed 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 for the 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 Smart Card architecture anticipates future needs of privacy protection. Other 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. MIFARE DESFire EV2 offers an enhanced security level with Common Criteria EAL5+ certification.

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 consumerfriendly choice for system design, with heightened security and reliability.

FEATURES

Memory		Special Features	
EEPROM size	2/4/8 kB	Multi-application	Unlimited applications, MIsmartApp
Write endurance [cycles]	500,000	Number fo files per app	32
Data retention [yrs]	10	Purse functionality	Value file
Organization	Flexible file system	Inter-app file sharing	Yes
Security		Transaction MAC	Per application
Unique serial number [byte]	7, cascaded	Virtual smart card architecture	PICC and application level
Random number generator	Yes	Proximity check	Yes
Access keys	14 keys per application	**RF-Interface**	
Multiple key sets	Up to 16 per application	Acc. to ISO 14443A	Yes-up to layer 4
Access conditions	Per file	Frequency [MHz]	13.56
AES, 3DES & DES Security	MACing/Encipherment	Baud rate [kbit/s]	106 … 848
Anti-tear supported by chip	Yes	Anti-collision	Bit-wise
Common Criteria certification (HW+SW)	EAL5 +	Operating distance [mm]	Up to 100