



NXP IC solution for contactless multi-application, high speed and secure smart cards

MIFARE DESFire

MIFARE DESFire is ideal for service providers wanting to use multi-application smart cards in transport schemes, e-government or identity applications. It fully complies with the requirements for fast and secure data transmission, flexible memory organization and interoperability with existing infrastructure.

Key applications

- ▶ Advanced public transportation
- ▶ Access management
- ▶ Event ticketing
- ▶ e-Government
- ▶ Identity

Key features

- ▶ Fully ISO 14443A 1-4 compliant
- ▶ 2Kbytes, 4Kbytes and 8 Kbytes EEPROM with fast programming
- ▶ Secure, high speed command set
- ▶ Flexible file structure
- ▶ Anti-collision
- ▶ Unique 7-byte serial number (ISO cascade level 2)
- ▶ Data integrity: CRC and bit counting on physical layer
- ▶ Open DES/3DES crypto algorithm in hardware
- ▶ Open AES128 crypto algorithm in hardware
- ▶ Based on Philips advanced 0.14 μm NV-technology
- ▶ Available in MOA4 modules or 8" sawn bumped wafer

MIFARE DESFire is based on open global standards for both air interface and cryptographic methods. It is compliant to all 4 levels of ISO / IEC 14443A and uses optional ISO / IEC 7816-4 commands.

Featuring an on-chip backup management system and the mutual three pass authentication, a MIFARE DESFire card can hold up to 28 different applications and 32 files per application. The size of each file is defined at the moment of its creation, making MIFARE DESFire a truly flexible and convenient product.

Additionally, an automatic anti-tear mechanism is available for all file types, which guarantees transaction oriented data integrity. With MIFARE DESFire, data transfer rates up to 848 Kbit/s can be achieved, making fast data processing possible.

The chip's main characteristics are denoted by its name DESFire – DES indicates the high level of security MIFARE DESFire achieves using a 3DES hardware cryptographic engine for enciphering transmission data. Fire reflects its outstanding position as a **F**ast, **I**nnovative, **R**eliable and **sE**cure IC in the contactless proximity transaction market.

Hence, MIFARE DESFire brings many benefits to end-users. Cardholders can experience convenient contactless ticketing while also having the possibility to use the same

device for related applications such as payment at vending machines, access management or event ticketing. In other words, the MIFARE DESFire silicon solution offers enhanced consumer-friendly system design, in combination with security and reliability.

MIFARE DESFire delivers the perfect balance of speed, performance and cost efficiency. Its open concept allows future seamless integration of other ticketing 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. MIFARE DESFire is your ticket to contactless systems worldwide.

The MIFARE pedigree

NXP MIFARE interface platform is the industry standard for contactless ticketing solutions. With more than 7 million reader core components and more than 1 billion card ICs sold, MIFARE is a proven and reliable technology, which represents the largest installed base worldwide.

Compliant with the ISO 14443A international standard, MIFARE ensures that today's infrastructure can easily be upgraded. It enables service providers to expand their transportation networks and to integrate additional services such as payment systems for taxi fares, cinema and theatre tickets, loyalty programs, access management and parking. And all while reducing the total costs of operations.

Product Features	MIFARE DESFire 2k	MIFARE DESFire 4k	MIFARE DESFire 8k	MIFARE DESFire SAM-X
	MF3 IC D21	MF3 IC D41	MF3 IC D81	MF3 IC D81 SAM
Memory				
EEPROM size [byte]	2048	4096	8192	72k
Write Endurance [cycles]	500 000	500 000	500 000	100 000
Data Retention [yrs]	10	10	10	10
Organization	flexible file system	flexible file system	flexible file system	128 key entries
RF-Interface				
Acc. to ISO 14443A	yes - up to layer 4	yes - up to layer 4	yes - up to layer 4	ISO 7616, T=1
Frequency [MHz]	13.56	13.56	13.56	1 ... 10
Baudrate [kbit/s]	106 ... 848	106 ... 848	106 ... 848	9.6 ... 1500
Anticollision	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	7
Random Number Generator	yes	yes	yes	yes
Access Keys	14 keys per application	14 keys per application	14 keys per application	128 key entries
Access Conditions	per file	per file	per file	per key entry
DES & DES3 Security	MACing / Encipherment	MACing / Encipherment	MACing / Encipherment	MACing / Encipherment
AES Security	MACing / Encipherment	MACing / Encipherment	MACing / Encipherment	MACing / Encipherment
Anti-tear supported by chip	yes	yes	yes	-
Special Features				
Multi-application	28 applications, MAD3	28 applications, MAD3	28 applications, MAD3	-
Purse Functionality	Value file	Value file	Value file	-
Secure Transport Transaction	512 byte read 128 byte write	512 byte read 128 byte write	512 byte read 128 byte write	-
Transaction Time [ms]	89	89	89	-
Packaging				
Sawn Wafer (Au-Bumped)	MF3ICD2101DW/V110	MF3ICD4101DW/V110	MF3ICD8101DW/V110	P5DF072EW1/TOPD4090
MOA4 Module	MF3MOD2101DV/410	MF3MOD4101DV/410	MF3MOD8101DV/410	-
PDM1.1 Module	-	-	-	P5DF072EV2/TOPD4090

MIFARE.net

www.nxp.com



©2008 NXP B.V.

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

Date of release: April 2008
Document order number: 9397 750 16504
Printed in the Netherlands