



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

## MIFARE DESFire™ EV1

MIFARE DESFire EV1 is ideal for solution developers and providers wanting to combine and support multiple applications on one contactless smart card. 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
- ▶ E-Government incl. social services
- ▶ Closed loop micro-payment
- ▶ Loyalty programs

### Key features

- ▶ Fully ISO / IEC 14443 A 1-4 compliant
- ▶ 2/4/8-Kbyte EEPROM with fast programming
- ▶ Secure, high-speed command set
- ▶ High data rates according to ISO / IEC 14443-4: up to 848 Kbit/s
- ▶ Flexible file structure
- ▶ Choice of open DES/2K3DES/3K3DES/AES crypto algorithm in hardware
- ▶ Anti-collision
- ▶ Privacy protection
- ▶ Unique 7-byte serial number (ISO cascade level 2)
- ▶ Data integrity: CRC and bit counting on physical layer
- ▶ Available in MOA4 modules or 8" sawn bumped wafer
- ▶ Common Criteria certification: EAL4+ for IC HW and SW

MIFARE DESFire EV1 is based on open global standards for both air interfaces and cryptographic methods. It is compliant to all four levels of ISO / IEC 14443 A and uses optional ISO / IEC 7816-4 commands.

Featuring an on-chip backup management system and the mutual three pass authentication, a MIFARE DESFire EV1 card can hold up to 28 different applications and 32 files per application. The size and access conditions of each file are defined at the moment of its creation, making MIFARE DESFire EV1 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 EV1, 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 EV1, the first evolution of MIFARE DESFire: DES indicates the commitment for high levels of security - MIFARE DESFire EV1 uses a DES, 2K3DES, 3K3DES and AES hardware cryptographic engine for securing transmission data. Fire reflects its outstanding position as a Fast, Innovative, Reliable and Enhanced IC in the contactless proximity transaction market.



MIFARE DESFire EV1 brings many benefits to end users. Cardholders can experience convenient contactless ticketing while also having the possibility to use the same device for applications such as closed-loop payment at vending machines, access management, loyalty or social services. In other words, the MIFARE DESFire EV1 silicon solution offers enhanced, consumer-friendly system design, in combination with security and reliability. The 70 pF option enables read range optimizations of small antenna form factors.

MIFARE DESFire EV1 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.

### The MIFARE pedigree

NXP MIFARE™ is the leading open architecture technology platform for contactless ticket, card and reader solutions. With more than 50 million reader core components and 5 billion smart card ICs sold, MIFARE is a proven and reliable technology and represents the largest installed base worldwide.

Compliant with the ISO / IEC 14443 A 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. All while reducing the total costs of operations.

In addition, MIFARE4Mobile™ guides the successful extension of the MIFARE technology platform into NFC enabled devices.

| Product Features                     | MIFARE DESFire EV1 2 K          | MIFARE DESFire EV1 4 K          | MIFARE DESFire EV1 8 K          |
|--------------------------------------|---------------------------------|---------------------------------|---------------------------------|
|                                      | MF3 IC D21                      | MF3 IC D41                      | MF3 IC D81                      |
| <b>Memory</b>                        |                                 |                                 |                                 |
| EEPROM Size [byte]                   | 2048                            | 4096                            | 8192                            |
| Write Endurance [cycles]             | 500 000                         | 500 000                         | 500 000                         |
| Data Retention [yrs]                 | 10                              | 10                              | 10                              |
| Organization                         | flexible file system            | flexible file system            | flexible file system            |
| <b>RF-Interface</b>                  |                                 |                                 |                                 |
| Acc. to ISO 14443 A                  | yes - up to layer 4             | yes - up to layer 4             | yes - up to layer 4             |
| Frequency [MHz]                      | 13.56                           | 13.56                           | 13.56                           |
| Baudrate [kbit/s]                    | 106 ... 848                     | 106 ... 848                     | 106 ... 848                     |
| Anticollision                        | bit-wise                        | bit-wise                        | bit-wise                        |
| Operating Distance [mm]              | up to 100                       | up to 100                       | up to 100                       |
| <b>Security</b>                      |                                 |                                 |                                 |
| 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         |
| Access Conditions                    | per file                        | per file                        | per file                        |
| DES & 3DES Security                  | MACing / Encipherment           | MACing / Encipherment           | MACing / Encipherment           |
| AES Security                         | MACing / Encipherment           | MACing / Encipherment           | MACing / Encipherment           |
| Anti-tear supported by chip          | yes                             | yes                             | yes                             |
| <b>Special Features</b>              |                                 |                                 |                                 |
| Multi-application                    | 28 applications, MAD3           | 28 applications, MAD3           | 28 applications, MAD3           |
| Purse Functionality                  | value file                      | value file                      | value file                      |
| Transaction Logging Capability       | record file                     | record file                     | record file                     |
| Secure Transport Transaction example | 512 byte read<br>128 byte write | 512 byte read<br>128 byte write | 512 byte read<br>128 byte write |
| Related Transaction Time [ms]        | 89                              | 89                              | 89                              |
| <b>Packaging</b>                     |                                 |                                 |                                 |
| 17 pF                                |                                 |                                 |                                 |
| Sawn Wafer Type Description          | MF3ICD2101DUD/05                | MF3ICD4101DUD/05                | MF3ICD8101DUD/05                |
| MOA4 Module Type Description         | MF3MOD2101DA4/05                | MF3MOD4101DA4/05                | MF3MOD8101DA4/05                |
| MOA8 Module Type Description         | MF3MOD2101DA8/05                | MF3MOD4101DA8/05                | MF3MOD8101DA8/05                |
| 70 pF                                |                                 |                                 |                                 |
| Sawn Wafer Type description          | MF3ICDH2101DUD/05               | MF3ICDH4101DUD/05               | MF3ICDH8101DUD/05               |
| MOA4 Module Type Description         | MF3MODH2101DA4/05               | MF3MODH4101DA4/05               | MF3MODH8101DA4/05               |
| MOA8 Module Type Description         | MF3MODH2101DA8/05               | MF3MODH4101DA8/05               | MF3MODH8101DA8/05               |

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

**MIFARE.net**

[www.nxp.com](http://www.nxp.com)

© 2012 NXP Semiconductors N.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: October 2012