



## **MIFARE DESFire EV1**

**Compatibility and Comparison with MIFARE DESFire (MF3ICD40)**

**Susanne Stern, Product Manager AFC**



## Functional backwards compatibility to MIFARE DESFire

- ▶ MIFARE DESFire EV1 can be operated in a functional backwards compatible way to the native command set of MIFARE DESFire (MF3ICD40)
- ▶ As the whole IC and Operating System (OS) is a new development including added security mechanisms, individual command timings may differ between MIFARE DESFire EV1 and MIFARE DESFire (MF3ICD40)
- ▶ There are optional new features of MIFARE DESFire EV1, which enhance the security of the new product

# General overview

MIFARE DESFire ↔ MIFARE DESFire EV1

## MIFARE DESFire

- ▶ 4 KB Memory
- ▶ Full ISO14443-4, basic ISO7816 support
- ▶ High data rate; up to 424 kbps
- ▶ 3DES in hardware

## MIFARE DESFire EV1

- ▶ Up to 8 KB Memory
- ▶ Full ISO14443-4, extended ISO7816 support
- ▶ High data rate; up to 848 kbps
- ▶ 3DES & AES in hardware, improved security concept
- ▶ Random UID
- ▶ Configurable ATS

# Benefits from new Features

MIFARE DESFire ↔ MIFARE DESFire EV1

## DESFire

- ▶ 4 KB Memory

## DESFire EV1

- ▶ Up to 8 KB Memory:  
2 KB, 4 KB, 8 KB
- ▶ BENEFIT:  
It covers applications from:
  - Access management (2 KB)
  - AFC (4 KB)
  - Biometric solutions (8 KB)

## DESFire

- ▶ Full ISO14443-4, basic ISO7816 support

## DESFire EV1

- ▶ Full ISO14443-4, extended ISO7816 support
- ▶ **BENEFIT:**  
It offers extended support for applications, which require ISO 7816 support, such as:
  - Logical Access (PC Login)
  - Old readers
  - Java based solutions

## DESFire

- ▶ High data rate; up to 424 kbps

## DESFire EV1

- ▶ High data rate; up to 848 kbps
- ▶ **BENEFIT:**  
Faster transaction especially on reading high volumes of data (e.g. biometric information)



# More Security on MIFARE DESFire EV1

MIFARE DESFire ↔ MIFARE DESFire EV1

## MIFARE DESFire

- ▶ 3DES in hardware

## MIFARE DESFire EV1

- ▶ 3DES & AES in hardware, improved security concept
- ▶ CC EAL 4+ Composite Certificate on the security concept.
- ▶ BENEFIT:
  - External, independent evaluation of the product ensures high level of security.

## MIFARE DESFire

- ▶ DES or TDES DESFire backwards compatible Mode: 16-byte

## MIFARE DESFire EV1

- ▶ DES or TDES DESFire backwards compatible Mode: 16-byte
- ▶ DES or TDES Standard Mode: 16-byte
- ▶ 3KTDES: 24-byte
- ▶ AES 128: 16 byte
- ▶ BENEFIT:
  - New application on secure mode
  - 'Old' application for backwards compatibility

## MIFARE DESFire

- ▶ 3-pass mutual authentication based on the crypto method used.
- ▶ En/Decryption based on MIFARE DESFire backwards compatible TDES
- ▶ CRC16, 4-byte MAC for every calculation
  
- ▶ Init Vector (IV) reset to “00”

## MIFARE DESFire EV1

- ▶ 3-pass mutual authentication based on the crypto method chosen
- ▶ En/Decryption based on crypto method chosen
- ▶ CRC16 and 4-byte MAC for DESFire backwards compatible TDES,
- ▶ CRC32 and 8-byte CMAC for TDES and AES.
- ▶ DESFire backwards compatible mode reset to ‘00’, new modes IV is continued in a session.

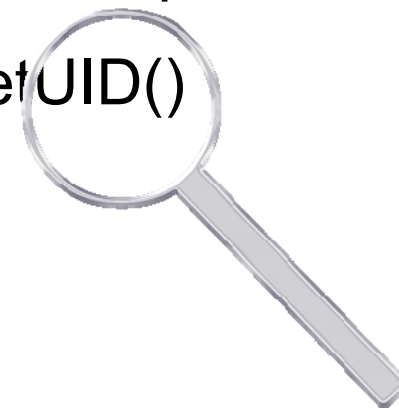


# New Features

MIFARE DESFire EV1

## Random UID vs. UID

- ▶ During card activation sequence, the UID will be retrieved from the card.
  - Random UIDs can be used during activation sequence
  - The UID can be read out encrypted with `GetUID()` command AFTER authentication



### **BENEFIT:**

Privacy friendly card activation for the end customer.

# ATS

- ▶ Historical bytes within the ATS are open
  - The entire ATS can be configured within MIFARE DESFire EV1 (Be aware, this is a real expert feature.)
  - This feature may be a privacy issue.

## **BENEFIT:**

Possibility to give important information of the PICC in a very early step during communication.

**In case that you have any further questions,  
please feel free to contact me at any time:**

Susanne Stern  
Product Manager AFC  
Market Sector AFC  
Business Line Identification  
NXP Semiconductors

---

Mikron-Weg 1  
8101 Gratkorn  
Austria  
Email: [susanne.stern@nxp.com](mailto:susanne.stern@nxp.com)

**HAVE A LOOK AT: [www.mifare.net](http://www.mifare.net)**