
NXP®
MIFARE® DESFire® EV3

# The foundation for a new era of secure, connected Smart City services

As the third evolution of NXP's proven contactless MIFARE DESFire portfolio, the MIFARE DESFire EV3 IC enables a new era of Smart City services, with next-generation performance, higher-level security features and seamless integration of mobile services.

## KEY FEATURES

- ISO/IEC 14443 A 1-4 and ISO/IEC 7816-4 compliant
- Common Criteria EAL5+ certified for IC hardware and software
- NFC Forum Tag Type 4 certified
- SUN message authentication for advanced data protection within standard NDEF read operation
- Flexible file structure for true multi-application operation
- Inter-application file sharing enables multiple applications with a common purse
- Wide choice of open DES/2K3DES/3K3DES/AES crypto algorithms
- Multiple key sets per application for post-issuance rolling application keys
- Proof of transaction with card generated MAC
- Transaction Timer defends against man-in-the-middle attacks
- Virtual Card architecture for privacy protection
- Proximity check to detect relay attacks

## TARGET APPLICATIONS

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

## KEY BENEFITS

- Services running on MIFARE DESFire EV3 can be deployed to NFC mobile phones using MIFARE 2GO
- Preloaded keys for delegated application management allow to add new services to already deployed cards
- Functional backward compatibility to MIFARE DESFire EV2 and MIFARE DESFire EV1 offers a seamless upgrade path
- Improved operating range and higher transaction speeds compared to its predecessors enhance both user experience and security

Targeting a broad range of Smart City services, including public transport and access management, the MIFARE DESFire EV3 IC offers enhanced security and convenience, and delivers significant benefits to operators and end users alike.

## TAILORED SUPPORT FOR SECURITY AND PRIVACY

Special features address the need for enhanced security and privacy in Smart City services. For example, a card generated MAC can help to ensure the authenticity of each transaction, so as to minimize fraud and identity theft. To help mitigate man-in-the-middle attacks, the new Transaction Timer feature makes it possible to set a maximum time per transaction, so it's harder for an attacker to interfere with the transaction.

The new Secure Unique NFC (SUN) messaging feature, also available on NXP's NTAG 424 DNA IC, offers a more secure way to maintain data confidentiality and integrity. Each time a card or ticket equipped with the MIFARE DESFire EV3 IC is tapped, the SUN messaging feature generates a unique authentication message based on a CMAC calculation. The tap-unique URL, with its crypto-secure SUN code, can then be sent to a server for verification. When operated in NDEF mode, the SUN messaging feature is compatible with NFC phones and other NFC-enabled devices, making secure authentication of tags and messages a convenient option on widely available, off-the-shelf devices.

## CONTACTLESS PERFORMANCE

For a truly convenient touch-and-go experience, the MIFARE DESFire EV3 IC offers an increase in operating distance and speed compared to previous versions. The 70 pF option can enable read range optimizations for form factors that require a small antenna. The transaction speed is up to 1.5 times faster compared to NXP's MIFARE DESFire EV1 IC, so operators can enhance system efficiency and improve the end-user experience without having to update the reader infrastructure.

## FOCUSED ON MOBILE

Smart City services that run on MIFARE DESFire EV3 can be deployed to NFC-enabled smartphones and wearables using NXP's MIFARE 2GO cloud service. MIFARE 2GO manages digitized MIFARE product-based credentials and can enable contactless payments or access features using the device.

## THE FOUNDATION FOR MULTIPLE SMART CITY APPLICATIONS

Each MIFARE DESFire EV3 IC is pre-configured with keys to enable delegated application management, which supports over-the-air updates to already-issued smart cards, making it easier to deploy additional services to existing users. The preloaded keys support personalization for each IC, without forcing card issuers to manage and deliver a new set of keys.

## FEATURES

| MIFARE DESFire EV3 | |
|---|---|
| **Memory** | |
| Non-Volatile (NV) size [kB] | 2/4/8 |
| Write endurance [cycles] | 1,000,000 |
| Data retention [yrs] | 25 |
| **RF Interface** | |
| According to ISO/IEC 14443A | Yes - up to layer 4 |
| Frequency [MHz] | 13.56 |
| Baud rate [kbits/s] | 106 … 848 |
| Operating distance [mm] | Up to 100 |
| **Security** | |
| Unique serial number [byte] | 7, cascaded |
| Access keys | 14 keys per application |
| Multiple key sets | Up to 16 per application |
| Access conditions | Up to 8 keys per access right |
| AES, 2K3DES & 3K3DES cryptography | MACing/Encipherment |
| On-chip anti-tear support | Yes |
| Common Criteria certification (HW+SW) | EAL5+ |
| **Special Features** | |
| Multi-application | As many as memory supports, Delegated Application Management |
| Number of files per app | 32 |
| Purse functionality | Value file |
| Inter-application file sharing | Yes |
| Transaction MAC | Per application |
| SUN (Secure Unique NFC Message) | Yes, compatible with NTAG DNA |

## ORDERING INFORMATION: MIFARE DESFire EV3

| | 2 kB | 4 kB | 8 kB |
|---|---|---|---|
| **17 pF** | **Part Type** | | |
| Wafer | MF3D2301DUD/00 | MF3D4301DUD/00 | MF3D8301DUD/00 |
| MOA4 | MF3D2300DA4/00 | MF3D4300DA4/00 | MF3D8300DA4/00 |
| MOA8 | MF3D2300DA8/00 | MF3D4300DA8/00 | MF3D8300DA8/00 |
| **70 pF** | **Part Type** | | |
| Wafer | MF3DH2301DUD/00 | MF3DH4301DUD/00 | MF3DH8301DUD/00 |
| MOA4 | MF3DH2300DA4/00 | MF3DH4300DA4/00 | MF3DH8300DA4/00 |
| MOA8 | MF3DH2300DA8/00 | MF3DH4300DA8/00 | MF3DH8300DA8/00 |

www.nxp.com



Date of Release: 19 May 2020
Document Number: MFDFLFEV3 REV0

Near Field Communication CERTIFIED

MIFARE

www.MIFARE.net