

Simplify security in smart city applications



As the first MIFARE® IC to combine asymmetric and symmetric cryptography on a single chip, MIFARE DUOX simplifies key management and accelerates asymmetric authentication in security demanding access-management applications.

Target applications

- Access management
- Secure car access
- Electric vehicle (EV) charging

MIFARE DUOX meets the needs of applications demanding flexibility, dynamic key provisioning and very high security by addressing the limitations of symmetric-based installations. By adding asymmetric cryptography and certificate management capabilities to the smartcard IC, MIFARE DUOX reduces the complexity of key provisioning and management, and enables new levels of design flexibility, protection and scalability for security-dependent applications.

Key features

- ISO/IEC 14443 A 1-4 & 7816-4 compliant
- CC EAL 6+ certified hardware and software
- NFC Forum Tag Type 4 certified
- ISO/SAE 21434 automotive cybersecurity requirements compliant
- Flexible file structure for true multi-application support on one IC
- Inter-application file and data sharing
- Support for symmetric cryptographic algorithms (AES-128, AES-256)
 - AES-256 cryptography for post-quantum-crypto capability
- Support for asymmetric cryptographic algorithms and key management (ECC with NIST P-256 and brainpoolP256r1 curves)
 - ECDH key agreement protocol
 - ECDSA signature generation

- Fast ECC-based mutual authentication and reader-unilateral authentication
- Simplified key management and key distribution via PKI features
- Extended operating temperature range for industrial & automotive applications on IC (silicon) level (-40 to +105°C)
- Enhanced feature set
 - Proximity Check to prevent relay attacks
 - Transaction Signature/MAC for proof of executed transactions
 - SUN feature for easy implementation of 2nd factor authentication
 - Delegated Application Management supports app installation from multiple issuers
 - Transaction Timer to prevent man-in-the-middle attacks

Key benefits

- ECC-based asymmetric cryptography for on-chip keypair generation, signature generation and verification as well as PKI based X.509 certificate handling
- Simplified key distribution based on private/public key scheme and certificate management, allowing easier key management and updates for NFC reader terminals
- Pre-personalization, via the NXP Trust Provisioning Service, enables secure injection of customer-specific keys and data
- Virtual cards, based on MIFARE DUOX, can soon be deployed to smartphones using NXP's MIFARE 2GO cloud service

ECC asymmetric authentication

The newly introduced support for Elliptic Curve Cryptography (ECC), including mutual, reader-unilateral and card-unilateral authentication methods, allows for various ECC-based authentication protocols that can be executed in NFC reader-terminal infrastructures. Depending on the required level of security for authentication and the follow-on transaction, lightweight implementations of the reader terminal are also possible. For card-unilateral authentications, where the reader is not required to authenticate itself to the smartcard, the reader terminal's BOM remains low, since there's no need for a secure access module (SAM) or other type of secure key storage.

Public Key Infrastructure (PKI) and simplification of key distribution

Instead of distributing sensitive symmetric keys to the NFC reader-terminal infrastructure, public keys and their related certificates can be shared easily and securely with other system integrators and the infrastructure. Public keys and certificates can also be shared via PKI systems without compromising confidentiality. This helps overcome existing issues with key distribution and security concerns related to symmetric keys. By avoiding the potential risks of leaking highly sensitive symmetric keys, this approach minimizes the risk landscape and reduces the potential for fraud.

The perfect fit for account-based systems

Account-based systems that put minimal data on the smartcard and store the rest of user-account information in a backend cloud system don't typically require mutual authentication between the smartcard and the reader terminal. As a result, a very simple, lightweight reader terminal can be deployed. Two MIFARE DUOX features – card-unilateral authentication and on-chip generation of a Transaction Signature – are ideally suited for this type of configuration.

Enhanced scalability and multi-platform availability

MIFARE DUOX leverages the file-system concept, already widely used in MIFARE DESFire® EV3 product, making it easy to realize applications and services for NFC-based infrastructures. Porting existing card and application structures from MIFARE DESFire EV3 to MIFARE DUOX is doable in an easy way, due to the same underlying file-system architecture.

As an additional convenience, applications based on MIFARE DUOX can be deployed to other NFC-enabled platforms, such as smartphones and wearables, using NXP's MIFARE 2GO cloud service. Offering both a physical and a virtual form factor to end users allows for a seamless go-to-market experience and increased end-customer satisfaction.

Product features

MIFARE DUOX	
IC characteristics for memory and RF interface	
Non-volatile (NV) user memory size [KB]	2/4/8/16
Write endurance and data retention	1.000.000 cycles and 25 years
Frequency [MHz]	13.56
Baud rate [kbits/s]	106 up to 848 (and support of VHBR)
Standard compliance and certification	
ISO/IEC 14443	Layer 1-4
ISO/IEC 7816	Yes, ISO/IEC 7816-4 commands and wrapped command format
ISO/SAE 21434	Yes
Common Criteria	Certification on EAL 6+ AVA_VAN.5 (for HW and SW)
NFC Forum	Tag Type 4
Security	
Symmetric cryptography	AES-128, AES-256
Asymmetric cryptography	ECC with ECDSA, ECDH and NIST P-256 or brainpoolP256r1
Asymmetric authentication	ECC-based mutual, reader-unilateral and card-unilateral authentication
Support of post-quantum-crypto	Future-proof for post-quantum era (via AES-256 strength and key length)
Data confidentiality, authenticity, integrity	AES-CMAC, AES-CBC encryption, secure channel establishment via EV2 secure messaging, secure dynamic messaging (SUN feature)
Extended features and functionality	
True multi-application support	Unlimited number of application and Delegated Application Management feature
Proximity Check	Mechanism to detect relay attacks
Transaction MAC and Transaction Signature	Generating a secure proof of executed transactions
Transaction Timer	Functionality to prevent man-in-the-middle attacks
Originality Check	Verification of genuineness of the IC by dynamic ECC authentication
EV-charging functionality	EV-charging specific command set as defined in VDE-AR-E 2532-100
Temperature range	-40 to +105°C on silicon level

Ordering information

		2 KB	4 KB	8 KB	16 KB
MIFARE DUOX	17 pF	Part type			
	Wafer	MF3E23A1DUF/01	MF3E43A1DUF/01	MF3E83A1DUF/01	MF3E93A1DUF/01
	MOA8	MF3E23A0DA8/01	MF3E43A0DA8/01	MF3E83A0DA8/01	MF3E93A0DA8/01
	70 pF	Part type			
	Wafer	MF3EH23A1DUF/01	MF3EH43A1DUF/00	MF3EH83A1DUF/00	MF3EH93A1DUF/00
	MOA8	MF3EH23A0DA8/01	MF3EH43A0DA8/00	MF3EH83A0DA8/00	MF3EH93A0DA8/00

		2 KB	4 KB	8 KB	16 KB
MIFARE DUOX for EV-charging	17 pF	Part type			
	Wafer	MF3E23A1DUF/01EV	MF3E43A1DUF/01EV	MF3E83A1DUF/01EV	MF3E93A1DUF/01EV
	MOA8	MF3E23A0DA8/01EV	MF3E43A0DA8/01EV	MF3E83A0DA8/01EV	MF3E93A0DA8/01EV
	70 pF	Part type			
	Wafer	MF3EH23A1DUF/01EV	MF3EH43A1DUF/01EV	MF3EH83A1DUF/01EV	MF3EH93A1DUF/01EV
	MOA8	MF3EH23A0DA8/01EV	MF3EH43A0DA8/01EV	MF3EH83A0DA8/01EV	MF3EH93A0DA8/01EV

[nxp.com/MIFARE](https://www.nxp.com/MIFARE)

NXP, the NXP logo, MIFARE, MIFARE DESFire, MIFARE DUOX, MIFARE 2GO, and MIFARE logo are trademarks of NXP B.V. All other product or service names are the property of their respective owners. © 2024 NXP B.V.

Document Number: MIFAREDUOXFSA4 REV0

