MIFARE DUOX®

Combination of asymmetric & symmetric cryptography

Information sheet

MIFARE DUOX® is the first contactless smartcard IC in its class to combine asymmetric and symmetric cryptography in a single chip. It simplifies key management and key distribution and accelerates asymmetric authentication in security demanding access-management applications.

Anwendungsbereiche:

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

MIFARE DUOX® offers flexibility, dynamic key provisioning and a very high level of security due to 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.

Product features:

IC characteristics for memory and RF interface	
Non-volatile (NV) user memory size	2/4/8/16 KB
Write endurance and data retention	1.000.000 cycles and 25 years
Frequency	13.56 MHz
Baud rate	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

© MADA Marx Datentechnik GmbH
Hinterhofen 4
78052 Villingen-Schwenningen

+49 (0)7721 / 8848 - 0
info@mada.de
www.mada.de