MIFARE DUOX®

Kombination von asymmetrischer & symmetrischer Kryptographie

Informationsblatt

Der **MIFARE DUOX®** ist der erste kontaktlose Smartcard-IC seiner Klasse, der asymmetrische und symmetrische Kryptographie in einem einzigen Chip vereint. Er vereinfacht die Schlüsselverwaltung und beschleunigt die asymmetrische Authentifizierung in sicherheitsrelevanten Zugangsmanagement-Anwendungen.

Anwendungsbereiche:

- Zutrittsmanagement
- Sicherer Zugang zum Auto
- Laden von Elektrofahrzeugen

MIFARE DUOX® bietet Flexibilität, eine dynamische Schlüsselbereitstellung und eine sehr hohe Sicherheit durch die Beschränkungen symmetrisch-basierter Installationen. Durch das Hinzufügen asymmetrischer Kryptographie und Zertifikatsmanagement-Fähigkeiten auf den Smartcard-IC reduziert MIFARE DUOX® die Komplexität der Schlüsselbereitstellung und -verwaltung und ermöglicht neue Designflexibilität, Schutz und Skalierbarkeit für sicherheitsabhängige Anwendungen.

Produktmerkmale:

IC-Merkmale für Speicher und RF-Schnittstelle	
Größe des nichtflüchtigen Benutzerspeichers	2/4/8/16 KB
Schreibbeständigkeit und Datenerhalt	1.000.000 Zyklen und 25 Jahre
Frequenz	13.56 MHz
Baudrate	106 bis zu 848 kbits/s (und Unterstützung von VHBR)
Normkonformität und Zertifizierung	
ISO/IEC 14443	Schicht 1-4
ISO/IEC 7816	Ja, ISO/IEC 7816-4-Befehle und Wrapped Command Format
ISO/SAE 21434	Ja
Gemeinsame Kriterien	Zertifizierung nach EAL 6+ AVA_VAN.5 (für HW und SW)
NFC-Forum	Tag Typ 4
Sicherheit	
Symmetrische Kryptographie	AES-128, AES-256
Asymmetrische Kryptographie	ECC mit ECDSA, ECDH und NIST P-256 oder brainpoolP256r1
Asymmetrische Authentifizierung	ECC-basierte gegenseitige, leser-unilaterale & karten-unilaterale Authentifizierung
Unterstützung von Post-Quantum-Crypto	Zukunftssicher für die Post-Quantum-Ära (über AES-256-Stärke & Schlüssellänge)
Datenvertraulichkeit, Authentizität, Integrität	AES-CMAC, AES-CBC-Verschlüsselung, sicherer Kanalaufbau über EV2 Secure Messaging, sichere dynamische Nachrichtenübermittlung (SUN-Funktion)
Erweiterte Merkmale und Funktionen	
Echte Multi-Applikations-Unterstützung	Unbegrenzte Anzahl von Anwendungen & Delegated Application Management-Funktion
Annäherungsprüfung	Mechanismus zur Erkennung von Relay-Angriffen
Transaktions-MAC und Transaktionssignatur	Generierung eines sicheren Nachweises für ausgeführte Transaktionen
Transaktions-Timer	Funktionalität zur Verhinderung von Man-in-the-Middle-Angriffen
Originalitätsprüfung	Überprüfung der Echtheit des ICs durch dynamische ECC-Authentifizierung
EV-Ladefunktionalität	EV-ladespezifischer Befehlssatz gemäß VDE-AR-E 2532-100
Temperaturbereich	-40 bis +105°C auf Siliziumebene

© MADA Marx Datentechnik GmbH
Hinterhofen 4
78052 Villingen-Schwenningen

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