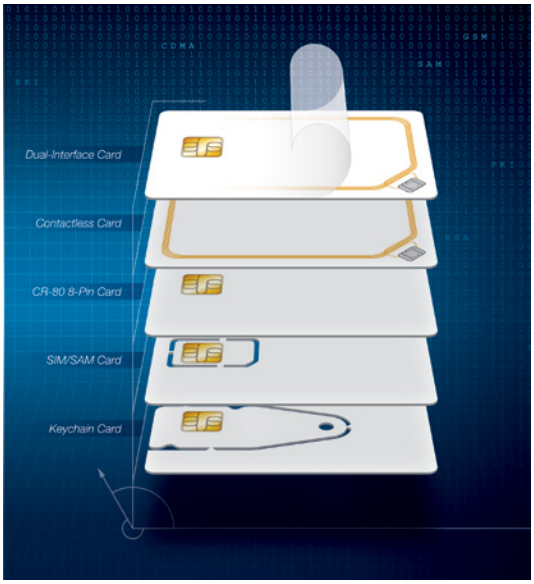
M.O.S.T. Card®

Low-Cost, High-Security Card Family



M.O.S.T. Card® is a microprocessor-based smart card family designed for multi-function or high-security applications. The M.O.S.T. card platform lets you design a smart card system that grows with your needs, supporting multiple functions, applications, and readers—all while maintaining high security. The family features up to 144k bytes of user memory that can be configured for high security and e-purse.

The cards contain the M.O.S.T Card Operating System which supports a variety of security measures, including SHA-1 and SHA-256 bi-directional/mutual authentication, AES, DES, 3DES and HMAC encryption, PIN/passwords, and internal random number generation for unique eSignatures, the SKI version of digital signatures, and transaction sessions.

The OS is built with error detection code and security self-tests. The EAL+ certified silicon provides continuous encryption of all data and the virtualization of the data across the non-volatile memory. The M.O.S.T. OS also features built-in anti-tearing mechanisms to support heavy transactional environments. M.O.S.T cards are future-proof and work on devices from multiple vendors, so your projects will always be supported.

Features

- Operating voltage range: 1.62V to 5.5V (ISO 7816 Class A, B, and C)
- CRC16 and CRC32 engines are compliant with ISO/IEC 3309
- Global unique card identifier system is compliant with ASN.1 Object Identifier components (ITU-T Rec. X.667 | ISO/IEC 9834-8, and with IETF RFC 4122)
- Conforms to FIPS 197
- Authentication mechanisms are fully compliant to Secure Hash Standard (SHS) FIPS PUB 180-4
- Conforms to (HDLC) procedures ISO/IEC 13239:2002
- Programmable passwords for all access modes: read, write, update, invalidate and rehabilitate
- eSignature functionality with vaulted and threshold key protection
- Data retention > 10 years
- Endurance: maximum of 16.5 million programming cycles at 25° C
- Electrostatic discharge protection > 6,000V

Dedicated Semiconductor and Operating System Countermeasures Guard Against:

- Side channel attacks
- Advanced fault attacks
- Velocity checking
- Voltage attacks
- Frequency attacks
- Temperature glitch attacks
- Optical attacks

High-Security Architecture

- A wide variety of user memory sizes
- T=0 or T=1 and contactless TLP protocols
- PC/SC compatible
- Negotiable communication speed (PTS)
- Hyper-Key diversification with GUID (16 bytes)
- Rapid card development through M.O.S.T. Toolz™
- Multiple reader and terminal choices
- ISO 7816 1-4 and ISO 14443A compliant

Card Security Options

- Laser engraving/indenting
- Guilloche and rosettes
- Microprinting
- Optically Variable Devices (OVDs) and holograms
- Hidden Card Validator™ graphics with lens viewer
- Ultraviolet (UV) ink
- Watermark
- CardLogix ReadyStart and Holofoil Cards
- SBumps

Development Tools

M.O.S.T. Cards are supported by the CardLogix M.O.S.T. Toolz® File Creation Utility, and the Smart Toolz® Development Kit, featuring the powerful Winplex® API. M.O.S.T. Toolz enables rapid creation and enabling of sophisticated files and applications that make your card unique. The cards are fully compliant with ISO 7816 1-4 and ISO 14443A standards and also work the PC/SC API.

CardLogix
16 Hughes, Irvine, CA 92618 USA
Phone +1 949 380 1312 || Fax +1 949 380 1428 || www.cardlogix.com || sales@cardlogix.com

M.O.S.T.® Card

Low-Cost, High-Security Card Family

M.O.S.T. CARD C-SERIES		C5	C6	C7	C8	C9	C10
INTERFACE	Contact	✓		✓		✓	✓
	Contactless		✓		✓	✓	✓
	MIFARE						✓
AUTHENTICATION	SHA-1	✓	✓	✓	✓	✓	✓
	SHA-256			✓	✓	✓	✓
DATA INTEGRITY	SHA-256 HMAC			✓	✓	✓	✓
	eSignature with Vaulted & Threshold Key Protection			✓	✓	✓	✓
ENCRYPTION	3DES	✓	✓	✓	✓	✓	✓
	AES-128	✓	✓	✓	✓	✓	✓
	AES-192			✓	✓	✓	✓
	AES-256			✓	✓	✓	✓
	Injectable AES Keys		✓	✓	✓	✓	✓
FILE SUPPORT	Long File Name APP ID			✓	✓	✓	✓
	MF	✓	✓	✓	✓	✓	✓
	DF	✓	✓	✓	✓	✓	✓
	EF (Transparent)	✓	✓	✓	✓	✓	✓
	EF (Large Size)	✓	✓	✓	✓	✓	✓
	EF (Cyclical & Linear)	✓	✓	✓	✓	✓	✓
	Purse	✓	✓	✓	✓	✓	✓
	APP	✓	✓	✓	✓	✓	✓
	CHV	✓	✓	✓	✓	✓	✓
CARD SECURITY	Global Password / PIN-PUK			✓	✓	✓	✓
	Admin Password		✓	✓	✓	✓	✓
	GUID	✓	✓	✓	✓	✓	✓
	Transport Key	✓	✓	✓	✓	✓	✓
	Forensic Data Logging	✓	✓	✓	✓	✓	✓
	Hyper-Key Diversification with GUID (16 bytes)			✓	✓	✓	✓
COMMUNICATION PROTOCOLS	T=0	✓		✓		✓	✓
	14443-A & 14443-B		✓		✓	✓	✓
	MIFARE Blocks						✓
EEPROM OPTIONS (USER MEMORY)	8k bytes	✓	✓	✓		✓	✓
	16k bytes	✓	✓	✓		✓	✓
	32k bytes	✓	✓	✓	✓	✓	✓
	64k bytes			✓			
	68k bytes	✓	✓			✓	✓
	76k bytes				✓		
	80k bytes			✓		✓	✓
	92k bytes		✓				
	128k bytes			✓		✓	✓
	144k bytes			✓	✓	✓	✓
	162k bytes				✓	✓	

Windows idblox®