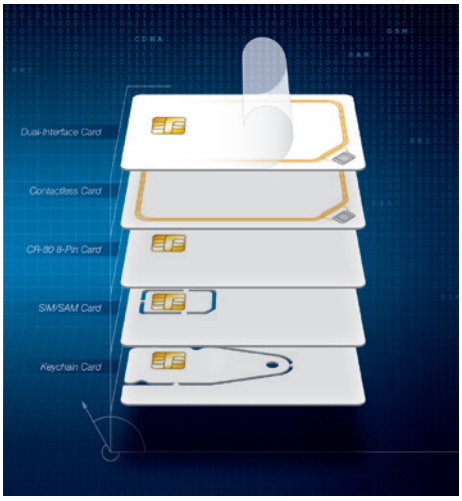
M.O.S.T. Card®

Low-Cost, High-Security Card Family



M.O.S.T. Cards® are a microprocessor-based smart card family designed for multi-function and/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 purse functions.

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 e-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-proofed, working on multiple silicon vendors' devices. So your projects are always 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
- Data retention > 10 years
- Endurance: maximum of 16.5 million programming cycles at 25° C

Electrostatic discharge protection > 6,000V

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)
- Rapid card development through M.O.S.T. Toolz
- Multiple reader and terminal choices
- ISO 7816 1-4 and ISO 14443A compliant

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

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
- SBumps

Windows

idblox

CardLogix
16 Hughes, Suite 100, Irvine, CA 92618 USA
Phone +1 949 380 1312 · Fax +1 949 380 1428 · www.cardlogix.com · sales@cardlogix.com

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.

Part Number	User Memory	Security Features	File Types Supported	Protocols
CLXSU032KC5/T=0ED	4k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse	T=0
CLXSU064KC5/T=0ED	8k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse	T=0
CLXSU128KC5/T=0ED	16k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse	T=0
CLXSU256KC5/T=0ED	32k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse	T=0
CLXSU544KC5/T=0ED	68k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Extended, Linear, Cyclical, APP, CHV, Purse	T=0
CLXSU064KC6/CAED	8k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse, GPF	14443 Contactless
CLXSU128KC6/CAED	16k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse, GPF	14443 Contactless
CLXSU256KC6/CAED	32k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse, GPF	14443 Contactless
CLXSU544KC6/CAED	68k bytes	SHA-1, DES, 3DES, AES-128	MF, DF, EF-Transparent, Extended, Linear, Cyclical, APP, CHV, Purse, GPF	14443 Contactless
CLXSU064KC7/AED	8k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1
CLXSU128KC7/AED	16k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1
CLXSU256KC7/AED	32k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1
CLXSU512KC7/AED	64k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Extended, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1
CLXSU640KC7/AED	80k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Extended, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1
CLXSU102MC7/AED	128k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Extended, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1
CLXSU115MC7/AED	144k bytes	SHA-1, SHA-256, HMAC, DES, 3DES, AES-128, -192, -256	MF, DF, EF-Transparent, Extended, Linear, Cyclical, APP, CHV, Purse, GPF	T=0, T=1

CardLogix