



M.O.S.T. Family Microprocessor Card Security Features

Individual members of the CardLogix M.O.S.T. family contain many of the following features to thwart unauthorized access to the secure cards. Features are listed in alphabetical order.

- ◆ Bus scrambling
- ◆ Current scrambling
- ◆ Customizable operating system - can be modified for special customer requirements. Consult CardLogix for specifics, minimum quantities, etc.
- ◆ Documentation control, restricted access to data, NDA, wafer/die monitoring
- ◆ Dummy computations
- ◆ Error counter authentication
- ◆ File structure permanently fused into card at factory
- ◆ Full chip erase capability in case of fraudulent access
- ◆ Fuses and test structure protection
- ◆ Hardware MMU, acts as firewall
- ◆ Memory encryption
- ◆ Metal mask
- ◆ No back doors into card operating system
- ◆ No DIR command - user MUST know file addresses or risk lockout
- ◆ No regular layout structures
- ◆ No test mode for the I/O port. Test circuitry physically removed at die scribe
- ◆ On chip randomization of instructions - randomizes power consumption
- ◆ On-chip encryption of all information
- ◆ Random wait states
- ◆ Randomized encryption algorithms
- ◆ Self timed memories (not related to input clock)
- ◆ Transport code / Unique chip ID
- ◆ Use of lower physical layers for EEPROM
- ◆ Voltage / Frequency control

This list is not organized by part type; it is presented to show the extent of the security features employed.