MICROSD™ ENCRYPTION UNIT FOR MOBILE DEVICES

CRYPTR MICRO

Motorola's CRYPTR micro encryption unit is well-suited for use in mobile devices to provide reliable data encryption for FIPS 140 applications.

The Motorola CRYPTR micro is designed for low power mobile applications that demand high assurance key management and encryption capabilities.

The inclusion of AES and Elliptic Curve Ciphers makes the CRYPTR micro particularly well-suited for solutions that require Suite B support. Combined with the high assurance built-in physical security measures, the CRYPTR micro is ready to meet the needs of critical security applications.

The CRYPTR micro unit is fully compliant with the SDIO Revision 2.0 standards and is reprogrammable through the 8 pin interface. This maximizes flexibility and provides ease of use in upgrade operations.

The High Assurance Boot ensures that only approved software can execute on the CRYPTR micro unit and validates the integrity of the software upon each power up.

The SDIO interface utilizes a dual port RAM allowing fast transfer for large data blocks between the Host device and the CRYPTR micro application. This capability provides optimal performance for meeting critical operational needs.

CRYPTR micro's ability to support Suite B applications in a range of environments while providing a trusted platform with a continuous upgrade path makes it an excellent choice for secure communication.

- **Full Suite B Solution**
  AES, Elliptic Curve Cipher Suites
- **FIPS 140-2 Level 3 Compliant**
  FIPS 140 Certification #1801
- **Standard SDIO interface**
  Supports SDIO Rev 2.0 electrical and power characteristics
- **Standard microSD Form Factor**
  Useable in a standard microSD connection
- **Designed for Mobile Applications**
  Low Power Consumption
  Configurable Speed
  Smart Power Management
- **High Assurance Boot**
  Allows trusted code to execute
- **Robust Hardware**
  Fail Safe Design
  Hardware Random Number Generator
  Field Upgradable Software Support
  Internal Physical Security Mechanisms

SECURITY AND PERFORMANCE SPECIFICATIONS

Throughput	10 Mbps
Key Storage	512 Keys
Certificate Storage	32 Certificates
Active Crypto Streams	4 Crypto Streams
Security Monitors	Detection of operational violation for Temperature, Frequency, Voltage
HW RNG	Hardware Random Number Generator
Audit Logs	Logging for creation of Encryption Keys and other events

ELECTRICAL AND PHYSICAL SPECIFICATIONS

Power	1.8V to 3.6V (encompassing SDIO standard 2.7V to 3.6V)
Low Power	1.8mW sleep mode (typical)
Interfaces	1x 8-pin microSDIO Rev 2.0 interface
Dimensions	Standard microSD™ Format

ENVIRONMENTAL SPECIFICATIONS

Operating Temperature	−40°C to +85°C
Storage Temperature	−60°C to +150°C

PROTOCOLS AND ENCRYPTION ALGORITHM INTEROPERABILITY

AES256	Advanced Encryption Standard: FIPS 197
ECDSA-384	Elliptic Curve Digital Signature Algorithm
ECDH-384	Elliptic Curve Diffie-Hellman
PKCS	Supports Public-Key Cryptography Standards in host devices
IKEv2	Internet Key Exchange version 2
DTLS	Datagram Transport Layer Security
SRTP	Secure Real Time Protocol
Crypto Accelerators	AES/GCM, SHA384/512 accelerators
Crypto Lib	Cryptographic Library

ENCRYPTION KEY PROVISIONING, KEY LOADING AND KEY MANAGEMENT

X.509v3	Elliptic-Curve Certificate Generation

UNCLASSIFIED COMSEC STANDARDS COMPLIANCE

NIST FIPS 140-2 level 3	National Institute of Standards and Technology NIST FIPS 140-2 FIPS 140-2 "Security Requirements for Cryptographic Modules" Certification #1801

MOTOROLA