MYK-185A
NSA-Certified Root of Trust Cryptographic Processor for Embedded Applications

Advanced cryptographic technology ideal for embedded applications that require minimal size, weight, power, and cost.

Applications
- Handheld Radios
- Manpack Link Devices
- Unmanned Platforms
- Embedded Wireless
- Remote Sensing
- Key Management
- Personal Authentication

Hardware and Design Features
The MYK-185’s design features fully redundant ARM processors with real-time alarm and integrity checking.

Hardware-assisted cryptographic algorithms support U.S. Government, NATO, and coalition operations.

Benefits
- Minimal Footprint
  - 19 mm² 324-BGA
  - Minimal External Logic
- Exceptionally Low Power
  - <0.5mA Hold-Up
  - <700mW Peak Operation
- Proven Low Risk Technology for Easy Integration
  - Over 400,000 MYK-185/A units fielded
  - Field upgradeable
- Simplified Key Management for Easy Operation
  - Red and Black Fill
  - Interfaces for DS-101, DS-102, and RS-232

Integrated Key Management
To simplify key management, internal battery-backed RAM (BRAM) supports the MYK-185A’s integral, secure, and authenticated boot-loading process.

When programmed for Crypto Ignition Key (CIK) operation, the system can be locked when the CIK is not present.
Designed for...

**Features and Capabilities**

Voice and data protection Operation in Suite A or Suite B modes supports wide-ranging applications encompassing government, civil and foreign interoperable markets.

Usable as a coprocessor, I/O processor, key manager or a stand-alone application processor.

32-bit general purpose I/O with interrupt control.

Separate Red and Black CPU host busses for system interfaces.

32-bit general purpose I/O with interrupt control.

Separate Red and Black CPU host busses for system interfaces.

Dynamic RAM controller, both Red and Black memory bus, with 64 Mbyte space each.

Software field-upgradeable using an authenticated process.

Capable of running user-defined software to support system operations.

Specialized interface for loading external cryptographic assist processors embodied in FPGAs.

Hardware randomizer ensures random number generation.

Easy to embed; Minimal external circuitry required.

Software Developer's Kit (SDK) available with NSA-approved modules to accelerate development.

**Technical Details**

**Hardware Accelerated Suite A and Suite B Encryption/Decryption AES Algorithm**

DSA Modulus Bootloader Trust Anchor Program

Cache Software:

- ECDSA
- ECDH
- SHA-256, 384, 512

Symmetric Algorithms

- AES
- MEDLEY

Hardware Acceleration for Public Key Operations:

- SHA-1
- 256 bit Multiplier
- Randomizer

**Physical/Electrical**

- 0.18 micron design
- Voltage: I/O, 3.3V; Core, 1.8V
- 19 mm² 324-pin BGA package
- < 0.5uA BRAM current
- ~ 630 mw max at 80MHz
- 1Hz to 80 MHz

Specifications subject to change.

Sales/Support Inquiries:

(310) 616-1125
Chuck.McCown@raytheon.com

www.raytheon.com/capabilities/cybersecurity/sis

Customer Success Is Our Mission