Proteus Crypto Module
High Assurance Suite A/B Cryptographic Module for Embedded Applications

The Proteus Cryptographic Module (PCM) is ideal for programmable embedded applications that require minimal size, weight and power, while meeting the highest level of information security—NSA Type 1 Certification.

Advanced Cryptographic Technology
The PCM was designed to be crypto-modern; compatible with legacy algorithms yet programmable for future applications. The design features the NSA Certified MYK-185A processor, which incorporates fully redundant ARM processors with real-time alarm and integrity checking. The PCM offers a variety of hardware-assisted cryptographic algorithms for both Suite A and Suite B supporting U.S. Government, NATO and coalition operation.

Integrated Key Management
Key management is made simple by the integral secure, authenticated boot-loading process supported by internal battery-backed RAM (BRAM). In simple terms, this means that the engine is completely unclassified when the BRAM is zeroized, whether prior to programming or after zeroization, simplifying handling and other logistics.

When programmed, the module offers a Crypto Ignition Key (CIK) function to lock the system in which it is embedded.

The MYK-185A is the Type 1 certified key management processor and trusted cryptographic controller for the PCM’s security critical operations. It controls all key loading, storage, and transfer of multi-level traffic keys to the PCM’s traffic engines. The MYK-185A powers-up in a secure authenticated boot-up state where private information stored in a secure on-chip Battery-Backed RAM (BRAM) is accessed to bring-up the processor into a Type 1 operational state. When the BRAM is zeroized, the processor is completely unclassified, which simplifies handling and other logistics. The PCM is capable of supporting multiple, independent channels, operating at different classification levels, whereby keys and key material are managed by the MYK-185A.
High-grade, high-assurance protection of voice and data from unclassified up to Top Secret Sensitive Compartmented Information (TS-SCI)

Highly Scalable Performance

Minimal Footprint

Minimal External Logic

2.5" x 4.2" x 0.3"

Proven Low Risk Technology for Easy Integration

Proven MYK-185A core engine is NSA-Certified

Supports EKMS and KMI connectivity, including Red, Black, and Benign fill

Dedicated interfaces for CIK and DS-101/102

Low Power

<600 mW @ 40 MHz

Power scalable to performance

Key Specifications

Simplified Key Management for Easy Operation

<600 mW @ 40 MHz

Field upgradeable

Proven MYK-185A core engine is NSA-Certified

Field upgradeable

Dedicated interfaces for CIK and DS-101/102

Simplified Key Management for Easy Operation

Dedicated interfaces for CIK and DS-101/102

Supports EKMS and KMI connectivity, including Red, Black, and Benign fill

Separate Red and Black CPU host busses for system interfaces

Software field-upgradeable using authenticated process

Capable of running user-defined software to support system operations

Type 1 hardware randomizer ensures highest level of security

Number of independent channels is hardware and algorithm dependent

Multi-Level capable dependent on system application

Specifications subject to change.