

Cryptographic Solutions

ASM Programmable Cryptographic Module



ASM Discrete Form Factor Module

Key Features

Encryption/Decryption Modes:

- Suite A Algorithms
- Suite B Algorithms
- Legacy Algorithms
- BIP-32, SHA-1, SHA-384 Data Integrity
- Multiple Single Levels of Security (MSLS)
- Multiple Simultaneous Independent Crypto Channels

Key Management:

- DS-101, DS-102 Key Fill
- DS-100 Key Tagging
- Key Wrapping/Unwrapping and Updating
- Key Storage (1000+)
- Firefly Versions 9.1 and 17.1
- Enhanced Firefly
- Multiple Universal Key Sets (10+)
- CIK

Additional Security Functions:

- Unclassified Prior to Programming
- CCI After Activation
- Access Control Lists
- Password Verification
- High Speed Randomizer
- Real Time Clock
- Over/Under Voltage Detection
- Programmable Cryptographic Bypass
- Secure Authentication for Remote Management
- JOSEKI Decrypt
- Signature Verified Software Download
- Signature Verified Algorithm Download
- Embedding Equipment Unique Access Control, Bypass, and Audit Security Policies

Other Features:

- Red and Black 32 Bit PCI Data/Control I/F
- High Speed UART Control/Status I/F

Target Applications:

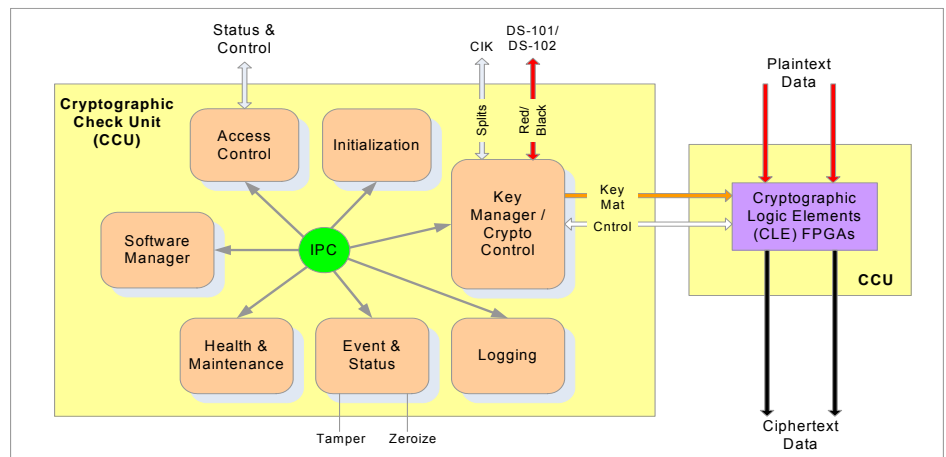
Government and Military Applications Requiring Type 1 Cryptography:

- HAIPIS In-Line Networks Encryptors
- JTRS Software Programmable Radios
- Media Encryptors
- Wireless Networks
- Airborne and Space Networks

ASM encryption products encompass a family of Type 1 fully programmable cryptographic modules designed for embedment in a wide range of equipment requiring a broad set of security features. ASM is designed to support the requirement sets of the Crypto Modernization Initiative, HAIPIS encryptor equipment, and the Joint Tactical Radio System (JTRS). ASM RadT Space products, suitable for embedment in a wide range of End Crypto Units (ECUs), address additional requirements necessary for operation in radiation environments.

ASM's innovative architecture permits straightforward evaluation and simplifies incorporation of design variants. Maximum use of COTS technology and components mitigates technology obsolescence risks. ASM supports 100% field re-programmability for all firmware, software, key management, and crypto control algorithms. One-time programmable capability is also supported.

ASM's flexibility and variety of configurations makes it an ideal choice for both low performance, low power equipment, and high performance, high throughput equipment.



ASM Programmable Cryptographic Engine Architecture

ASM Features	
Certification	Aeronix is actively seeking a Program of Record to carry into the certification process
Classification	Unclassified Prior to Module Activation, CCI After Activation
Cryptography	Reprogrammable - Suite A/B and Legacy Algorithms
Data Classification	System High Up To Top Secret, Multi-Channel MSLS Up To Secret
Data Channels/Rate	1-4 Full Duplex Channels TTL DC to 100+ Mbps/Channel (800 Mbps Aggregate Data Rate) or LVDS 1+ Gbps/Channel (8+ Gbps Aggregate Data Rate)
Bypass Channel(s)	Common Bypass and/or Channel/Algorithm/Waveform Specific Bypass
Key Management	CIK, Benign Key/Fill, Firefly, Enhanced Firefly, and OTAR
Security Policies	Embedding Equipment Unique Bypass, Access Control, and Audit Policies
100% Reprogrammable	All Firmware, Software, and Crypto Algorithms
Size	Multiple Form Factors as Small as 2" x 3" x 0.5"
Low Power	Less than 3.5 Watts at 100 Mbps



1775 West Hibiscus Boulevard ■ Suite 200 ■ Melbourne Florida 32901 ■ Tel.(321) 984-1671 ■ Fax.(321) 984-0366

www.aeronix.com