

POET ACM

Programmable Objective Encryption Technologies Advanced Cryptographic Module



A Next-generation High-speed, Multi-channel, Type 1 Encryptor

Concurrent, high-speed COMSEC and TRANSEC operation

Based on proven NSA certified technology

Modular Design support upgrades to existing and future satellite systems

Overview

General Dynamics C4 Systems has teamed with the Air Force, Army and Navy in developing the next-generation high-speed, high-capacity encryptor, the POET ACM. This module will perform numerous, concurrent, COMSEC and TRANSEC operations and is the ideal high grade cryptographic solution for communication terminals and transceivers.

The ACM is being developed and documented as an evolvable cryptographic platform and is the foundation for new cryptographic applications. The design provides flexibility, programmability and scalability enabling both software-only and software/hardware variants that are optimized for a specific terminal embedment. Reuse of the proven POET platform reduces risks to future development efforts and NSA certification. The POET ACM showcases General Dynamics' state-of-the-art technology and builds upon its 40 years of providing Type 1 cryptographic chips, modules, and communications products.

POET ACM

The POET ACM is a programmable, embedded security device that provides NSA Suite A/Suite B encryption and key management. It has four independent, high-speed channels each capable of up to 2 Gbps operation. It has the capability of running multiple modes/algorithms simultaneously with varying security levels and data rates. It is HAIPE®-compatible and provides HAIPE data encryption and net-centric remote management capability. The POET ACM supports legacy algorithms for MILSTAR interoperability and modern modes for AEHF and TSAT terminals. The ACM architecture readily scales to both single and dual channels, thus realizing lower speed variants and reduced size, weight and power. The POET ACM is Crypto Modernization Initiative (CMI) compliant and supports uploads of both algorithm and management software.

Embedment of the versatile POET ACM realizes numerous advantages over previous cryptographic products. A single POET ACM can simultaneously provide a communications terminal with TRANSEC bit stream, orderwire encryption, link and baseband encryption. Embedment of a single cryptographic module versus many various modules in the communications terminal reduces both terminal size and complexity.

POET ACM Features

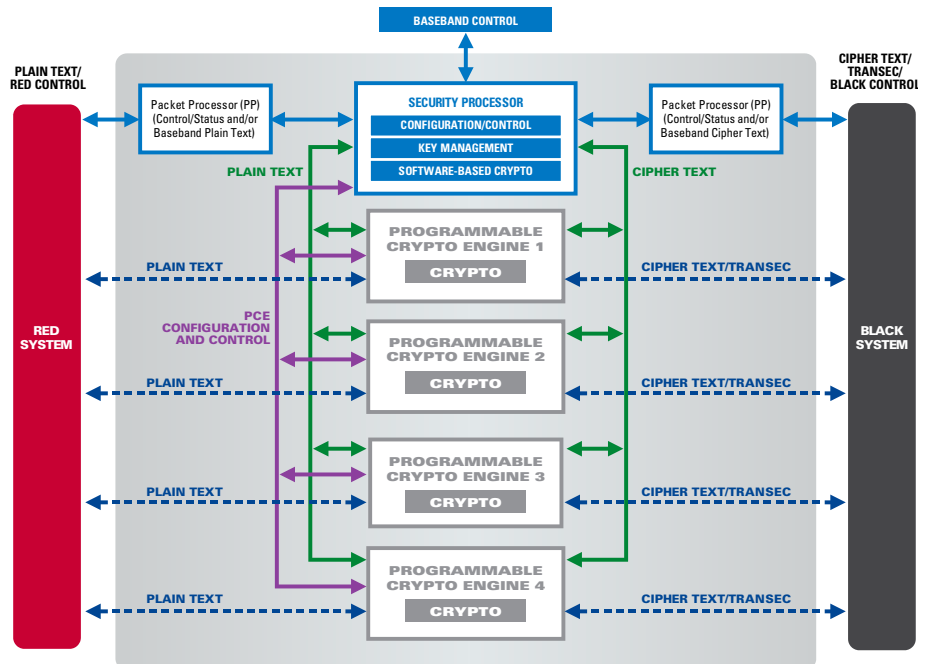
- Up to four independent cryptographic engines each capable of providing 2 Gbps throughput
- High speed transmission security (TRANSEC) key stream generation
- High speed communication security (COMSEC) encryption/decryption
- Simultaneous operation of numerous TRANSEC/COMSEC waveforms
- Legacy and modern algorithms, waveforms, and communications standards
- Multiple Single Levels of Security (MSLS)
- Programmable algorithm/Cryptographic Modernization Initiative (CMI) compliance
- Programmable key management for both legacy and new Key Management Infrastructure (KMI)
- Scalable throughput and power
- Design based on NSA Type 1 certified platform (POET ACM is currently undergoing NSA evaluation with certification anticipated 4Q 2009.)

Benefits

- The flexible and scalable design readily adapts to emerging terminal requirements thereby reducing long lead time and high risk aspect of terminal development
- Provides crypto capabilities for above 2 GHz terminals
- Scalable to both single and dual channels, thus realizing lower speed variants
- Variants will accommodate reduced size, weight and power

Cryptographic Standards and Interoperability

- HAIBE version 3.0.2
- Link Encryptor Family (LEF)
- IP Security (IPSec)
- KGV-11/MILSTAR
- AEHF TRANSEC key stream and cover



The flexible and scalable POET ACM readily adapts to the host terminal communication requirements.

- TSAT TRANSEC key stream and cover
- HNW TRANSEC key stream and cover
- EKMS 308D Red and Black key load

POET ACM Applications

- Navy Multi-band Terminal (NMT)
- Family of Beyond Line of Sight Terminal (FAB-T)
- High Capacity Communications Capability (HC3) terminals
- Software Defined Radios
- Communications Terminals

Algorithms

- ACCORDION
- AES
- BATON
- FIREFLY
- Enhanced FIREFLY

- KEESEE
- MEDLEY
- SHILLELAGH

Interfaces

- Red/Black Traffic and Control Interface – RGMII supporting Ethernet 1000Base-T
- Reprogramming Interface Ethernet 100 Base-T
- DS-101 key fill
- Cryptographic Ignition Key (CIK)
- Dedicated zeroize, tamper, reset inputs
- Dedicated health output
- 12 Volt Black Power

GENERAL DYNAMICS C4 Systems

8220 East Roosevelt Street, M/D R7229 • Scottsdale, Arizona 85257 • Website: www.gdc4s.com/poet
Phone: 480-441-5448 • Toll-free: 866-400-0195 • Email: IASystems@gdc4s.com

© 2009 General Dynamics. All trademarks indicated as such herein are trademarks of General Dynamics. HAIBE is a registered trademark of the National Security Agency. All other product and service names are the property of their respective owners. © Reg. U.S. Pat. and Tm. Off. All rights reserved. General Dynamics reserves the right to make changes in its products and specifications at anytime and without notice.