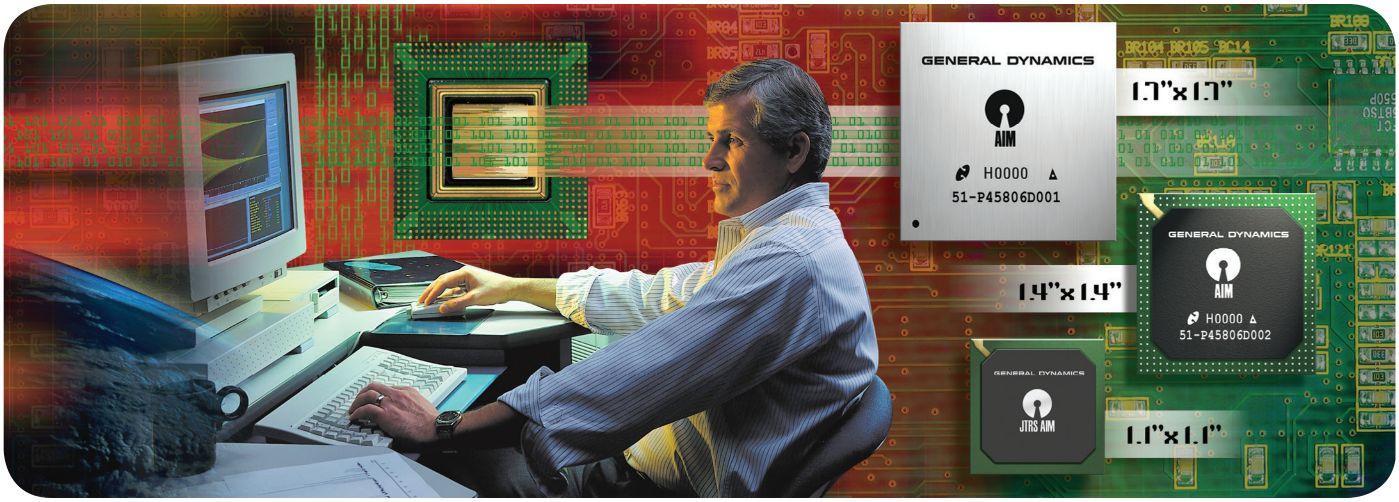
GENERAL DYNAMICS
Mission Systems

Advanced INFOSEC Machine (AIM)



Embeddable, high-grade cryptography

Totally programmable

Interoperable with future and legacy systems

AIM is a programmable, embeddable security engine for communications equipment requiring high-grade cryptographic processing. The state-of-the-art AIM chip provides a secure, certified hardware platform on which software emulations of cryptographic algorithms and higher-level crypto applications can execute. AIM is totally programmable and supports interoperability with legacy equipment as well as modern network-centric systems and enables the products in which AIM is embedded to be modified or upgraded in the future with a download of software. The AIM design includes three independent cryptographic processors (KMCE, PCE, CCE), which are tailored to efficiently execute key management and traffic encryption/decryption functions. Three package types of the AIM platform have been certified by the U.S. Government to protect information through Top Secret Codeword.

AIM Technology

The AIM architecure supports high-speed, multi-channel encryption/decryption and advanced key management devices. AIM's versatile design enables it to process data packets from many channels at the same time. AIM simultaneously supports cryptographic algorithm processing for both symmetric algorithms (block and streaming cipher) and non-symmetric (public key) algorithms.

Key Management

The KMCE is the master controller in the AIM. It contains a ROM-based Secure Operating System (SOS). The architecture contains a high-performance 32-bit RISC processor with a math co-processor designed for public key algorithm processing. This provides high-speed capability for outstanding performance for multiple- and single-channel secure processing embedment applications.

Secure Operating System

The SOS provides a multi-security level, multi-tasking environment for the development of user application software. This includes task and object separation, which allows programs to run from both internal and external RAM and ROM.

Advanced INFOSEC Machine (AIM)

Benefits/Features

- U.S. Government certified — Top Secret/Codeword
- Three independent crypto processors
- Multiple channels (1024)
- 20 Mbps throughput (algorithm dependent)
- Library of certified algorithms and crypto equipments
- Applications (CEAs) interoperable with future and legacy systems
- Supports multiple security levels
- Flexible I/O ports:
- 2 full-dux serial
- 32-bit parallel
- CIK, DS-101* and DS-102 interface
- Active power management
- Type-1 randomizer
- Total programmability
- Three certified packages:
- 1.7” x 1.7” SBGA
- 1.4” x 1.4” TEPBGA
- 1.1” x 1.1” SBGA
- Rapid switching between channels, algorithms and keys

** DS-101 needs additional circuitry*

Unique Functionality

- A multi-core VLSI chip
- Totally programmable key management
- Totally programmable traffic encryption
- 1024 independent channels, Type 1 and non-Type 1
- Fast context switching
- Certified for TS Codeword operation, transmit & receive
- Certified MSLS capability
- Supports more algorithms and equipment modes than any other crypto engine

AIM-based Applications

AIM can be embedded virtually anywhere encryption is needed. It is currently used in the following programs/applications:

Radios

- Handheld and soldier
- Manpack
- Software-defined
- JEM radio
- Multi-band, multi-mode (WITS, DMR, JTRS)

Key Management

- Ground-based space comms

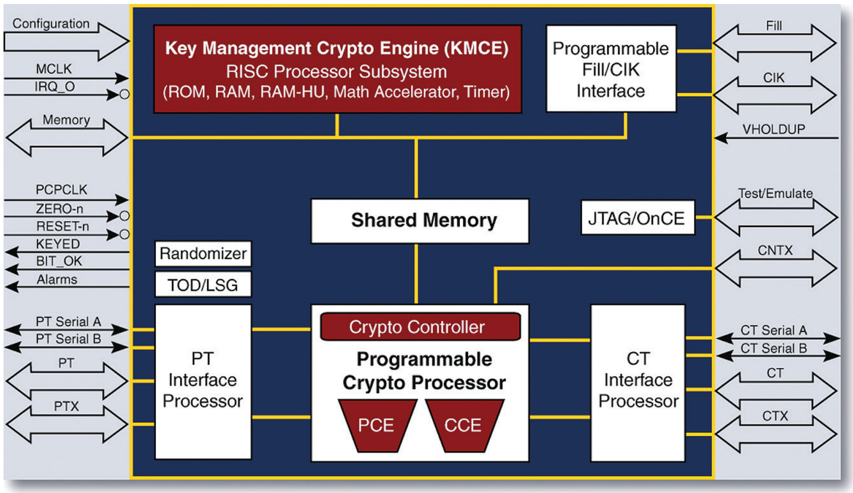
Crypto Modernization

- Trunk encryptors
- Link encryptors
- MLS workstation

Avionics

- F-22 enhancements
- Joint Strike Fighter
- IFF Mode 4 and Mode 5

Block Diagram



AIM Algorithm and Crypto Equipment Application (CEA) Software

The algorithms and CEAs shown in the table below have been developed to support AIM.

Algorithms

- Accordion 1.3, 3.0
- AES
- Baton
- Crayon
- DES, 3-DES
- DSA
- Firefly
- Jackknife
- Keesee
- Mark 12
- Medley
- Phalanx
- Saville
- SHA-1
- Vallor
- Walburn
- Weasel

CEAs

- APCO 25
- CCSA
- FED
- HAIPIS
- Havequick
- IFF Mode 4, Mode 5
- KG-84A/C (KIV-7)
- KG-235
- KGR-96
- KGV-8
- KGV-10
- KGV-11
- KWR-46
- KY-57/58
- KYV-5 (ANDVT)
- KY-99/100
- NES

GENERAL DYNAMICS
Mission Systems

gdmissionsystems.com/AIM • IASystems@gd-ms.com
Phone: 480-441-5448 • Toll-free: 866-400-0159