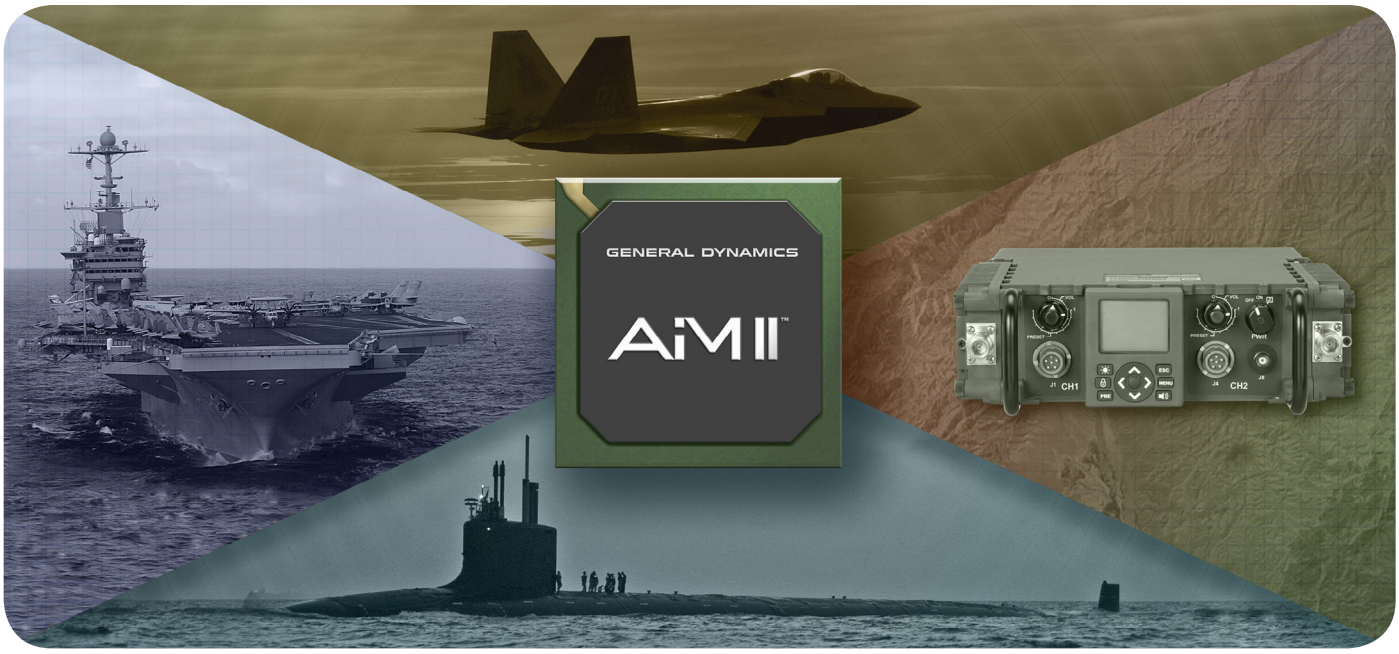
GENERAL DYNAMICS
Mission Systems

AIM II — Embeddable Programmable Security



A member of General Dynamics' Family of Advanced Core Cryptographic Technologies (FAC^{2}T)

NSA certified

Multi-security level architecture

Support for single and multi-channel embedments

Extensible design supports up to 500 Mbps

Low power, high performance, fully programmable

AIM II™

Overview

AIM II builds on 40 years of fielded Type 1 cryptographic chips, modules, and communication products. It is the next-generation successor to the Advanced INFOSEC Machine (AIM), which has seen wide use in General Dynamics products, and was specifically developed for Joint Tactical Radio Systems (JTRS). AIM II enhances many of AIM's proven features like total programmability and adds new capabilities to ease integration into new developments. Investments in current AIM-based platforms are leveraged since AIM II is code compatible with AIM. Like AIM, AIM II is a state-of-the-art INFOSEC device that serves as the core of a secure system.

AIM II

AIM II is a programmable, embeddable security engine for communications equipment requiring high-grade cryptographic processing. The state-of-the-art AIM II chip provides a secure hardware platform on which software-based cryptographic algorithms and higher-level crypto equipment applications (CEAs) can execute. AIM II is totally programmable and supports interoperability with legacy equipment as well as modern net-centric systems. It enables the products in which AIM II is embedded to be modified or upgraded in the future with a download of software. The AIM II design includes three independent cryptographic processors that are tailored to efficiently execute key management and traffic encryption/decryption functions. The National Security Agency (NSA) has certified the AIM II to protect information classified Top Secret and below.

AIM II — Embeddable Programmable Security

AIM II Features

- Faster context switching (time needed to change from one CEA to another)
- Enhanced traffic engines support one active and three shadow programs
- Single clock cycle context switching between four different CEAs (reduced latency)
- Efficiently meets new security requirements
- Enhanced algorithm performance
- Two parallel ports and two serial ports per Interface Processor (improved support for MLS systems)
- Support for multiple Red Processors
- New Command and Control Interface
- Supports new security requirements with fewer parts
- New programmable chip selects and general purpose I/O
- Reduces external support parts
- Supports legacy and future crypto modernization waveforms
- Backward compatibility with existing AIM software
- Improved power, size and environmental characteristics
- 0.13 micron processing technology
- 1.2 volt core
- –40°C to 85°C
- Remains non-CCI until Type 1 software has been added

AIM II Applications

- Software definable radios
- Single- and multi-channel radios
- Type 1 and non-Type 1 radios
- Multiple Level Security radios and Network Interface Cards (NIC) HAIPE
- Legacy crypto replacement
- Crypto Modernization programs
- Homeland security applications
- Avionic (manned and unattended) applications
- JTRS radio products (e.g., airborne, maritime, and fixed station, vehicle, and manpack, handheld and small form fit)
- Key management products and applications modules

AIM and AIM II Algorithm and Crypto Equipment Application (CEA) Software

The algorithms and CEAs shown below have been developed to support AIM and AIM II.

Algorithms

- Accordion
- Acme
- AES (AIM)
- Baton
- Benign Techniques
- Crayon
- DES, 3-DES
- Digital Signature Algorithm (DSA)
- Elliptic Curve Cryptographic (ECC)
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Firefly
- Jackknife
- Joseki
- Keesee
- Mark XII (Cadmus)
- Medley
- Phalanx
- Saville
- SHA-1/256/384/512
- Shillelagh
- Vallor
- Walburn
- Weasel

CEAs

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

** In development*

GENERAL DYNAMICS
Mission Systems

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

D-AIM2-04-0316