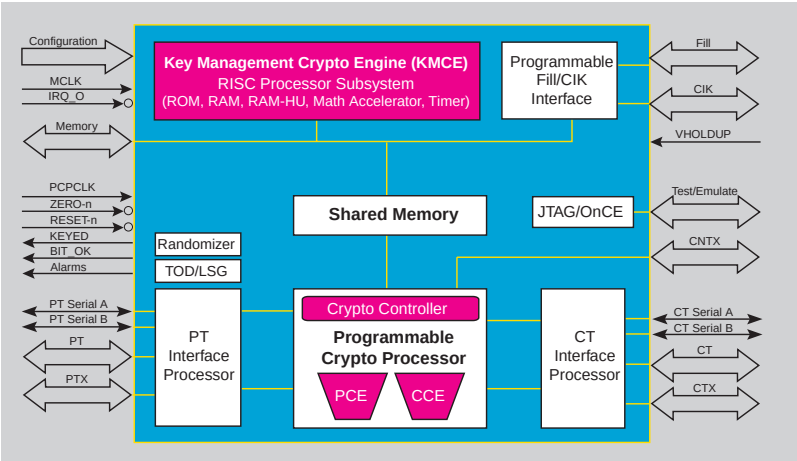
Advanced INFOSEC Machine

AIM



Target Applications

- ***Radios:***
  - ✓ *Handheld and Soldier*
  - ✓ *Manpack (LST-5D)*
  - ✓ *Multi-band, Multi-mode (SPEAKeasy, WITS, DMR, JTRS)*
- ***Avionics:***
  - ✓ *F-22 Enhancements*
- ***Networks:***
  - ✓ *NES (ATM, Performance)*
  - ✓ *ATM NIC*
- ***Key Management:***
  - ✓ *FASKMM*
  - ✓ *DTD2000*
- ***INFOSEC Equipment Upgrades:***
  - ✓ *Trunk Encryptors*
  - ✓ *Link Encryptors*
- ***Telephony:***
  - ✓ *STE*
  - ✓ *STU III Cellular*

AIM FEATURES

- Programmable INFOSEC processor for High-Grade Security
- Processor resources consist of 3 independent superscaler RISC architectures (PCE, CCE, KMCE)
- Multiple channels operating simultaneously
- High algorithm throughput
- Key & algorithm agile (Single clock Context Switch time)
- Interoperable with future and legacy systems
- Multi-Level Security (MLS) per packet
- Security Policy Enforcement of application information flow and data isolation requirements via:
  - Secure Operating System
  - PCP architecture
- Flexible PT and CT interfaces:
  - 2 full-duplex synchronous serial port
  - Configurable 8/16/32 bit parallel port
  - 3 data formats - APDU, Fixed, Variable
- Full CIK, DS-101 and DS-102 interface
- Power Management
  - Battery backed memory
  - Low-power design, static
  - Individual blocks powered only when used
- Randomizer
- Programmable TOD/LSG
- Development Tools
  - Operational performance model
  - Compilers, assemblers, & simulators
  - Real time emulator - OnCE & JTAG
  - AIM Development Platform (ADP)

AIM APPLICATIONS

AIM is designed to be the embedded cryptographic processing engine for communication equipment requiring high-grade cryptographic processing. AIM can be implemented in either a data flow-through architecture or in a co-processor architecture. The architecture's internal security mechanisms are used to assure object and task isolation of sensitive data (PT), variables, unclassified data, and the protected data (CT) in real-time task switching modes of operation. Cryptographic algorithm processing for both symmetric algorithms (typical codebook and serial feedback) and non-symmetric (public key class) algorithms are supported simultaneously. Target applications include high-speed, multi-channel en(de)cryption and advanced key management devices.

PERFORMANCE

The performance of certain algorithms is listed below. Because different versions of AIM run at different clock frequencies, performance specs (in bits/clock) are expressed here as a percentage of Input Clock rate. For example, if you are running Baton at 10 MHz, the encryption rate will be 12.9 Mbps. See our AIM web site at **http://aim.motorola.com** for specific numbers on the desired AIM device.

- Baton – 129%
- Phalanx – 139%
- DES (64-bit) – 76%
- Triple DES – 25%
- Accordion – 28%
- Saville – 4%
- Keesee – 100%

MOTOROLA

MULTIPLE ALGORITHMS

AIM's fully-programmable, superscaler architecture allows multiple algorithms to operate simultaneously. For example, a high-speed codebook encryption application can be running in the PCE, a high-speed serial feedback decryption operation can be running in the CCE, and a public key operation (e.g. Digital Signature) all can be executing in the KMCE at the same time. In addition to the algorithms themselves, the RISC portions of the crypto engines also can be used for general purpose data processing such as in-band signal processing error detection and correction (EDAC), or any other protocol or format processing required by the cryptography.

MULTIPLE CHANNELS

AIM's versatile design enables it to process data from many channels at the same time. This data is formatted into packets and loaded into the chip. As each packet comes in, its channel number is used to select the current key state and algorithm to execute. In the cases where the internal clock speed is significantly faster than the operating speed of the input device, AIM can perform the en(de)cryption for all channels.

SYSTEM ON A CHIP

The AIM VLSI is unclassified and is processed in commercial semiconductor foundries. The advantage is low-cost devices fabricated in the most advanced sub-micron processes available. The present 3.3 Volt, 0.35 sub-micron technology offers:

- Low Cost
- Low Power
- High Reliability
- Single VLSI Solution

CERTIFICATION

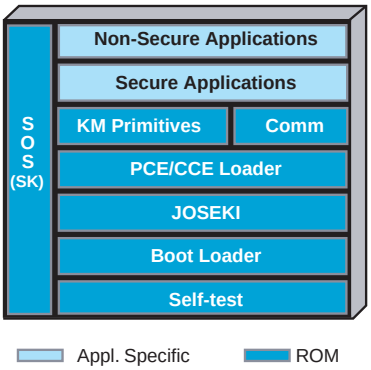
Motorola has worked hand in hand with the U.S. Government on the Certification of the AIM VLSI. Security Verification Testing has been successfully completed. Check our web site to see the latest status on full certification of the part.

KEY MANAGEMENT

The Key Management Cryptographic Engine 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.

SOS Services

- Task Management
  - Multi-Task (MLS)
  - Fast
  - Deterministic
- Communications
  - Device Drivers
  - Mailbox
  - Message Queues
  - I/O Control
- Program Manager
- JOSEKI Decryption



The figure above illustrates the type of services provided by the SOS and a typical software architecture of an application running on the SOS. The SOS provides a MLS multi-tasking environment for the development of user application software. It provides task and object separation which allows programs to run from both internal and external RAM and ROM. The SOS assures that only the unclassified program and data segments are executed externally to the chip. Post-processing tools, ACFM and JOSEKI encryptor, are used to create the seeds and the final program code.

EXPORTABILITY

The AIM VLSI is controlled as an EAR item, NOT as an ITAR item. Thus, the mere presence of the AIM VLSI in a system does not result in a high level of export control. The determining factor in classification of the host system, and its export control, is the type of algorithm ultimately used.

SIGNED SOFTWARE

All software running on AIM must have the proper digital signature. This assures that an unauthorized user cannot alter the software to be loaded, a further level of security.

AIM ALGORITHM DEVELOPMENT

Algorithms and total cryptographic functions are being developed to run on the AIM VLSI. Once verified, they will be able to be reused without alteration and without additional security evaluation. Check our web site to see the latest status of verified algorithms and functions.

All AIM development is performed using the AIM Development Platform, a suite of tools for the programming the AIM chip. These tools include a simulator, compilers, emulators, and assemblers working together to integrate the user's specific applications into a cohesive, functional program.

Motorola
8220 E. Roosevelt, M/D R1207
P.O. Box 9040, Scottsdale, AZ 85257-9040
Telephone: (480) 441-2814 Fax: (480) 441-0843
Web: http://aim.motorola.com
E-mail T. Craig Peacock at: AIM100@email.mot.com

R3-115-4002A

MOTOROLA